



Using Vanguard Security Solutions to Complete DISA STIG SRR Review Procedures

z/OS BMC IOA for RACF Analysis Process and Checklist

Modeled After:
SRR REVIEW PROCEDURES
z/OS BMC IOA for RACF Checklist
Developed by DISA for the DOD
Version 6 Release 7
October 2018

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

DISA Version 6.28

Document Number IOA_STIG-08012016-115700-628A

October, 2018

Copyright

© 1989-2012 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: ZIOA0060.....	4
___STIG ID: ZIOAR000.....	5
___STIG ID: ZIOAR001.....	7
___STIG ID: ZIOAR002.....	8
___STIG ID: ZIOAR020.....	9
___STIG ID: ZIOAR030.....	10
___STIG ID: ZIOAR032.....	11
___STIG ID: ZIOA0040.....	12

UNCLASSIFIED
z/OS BMC IOA for RACF Analysis and Checklist
Version 6 Release 6

___ **STIG ID: ZIOA0060**

Default Severity: Category II

- a) Interview the systems programmer responsible for the BMC IOA. Determine if the site has modified the following security exit(s):

IOASE06
IOASE07
IOASE09
IOASE12
IOASE16
IOASE32
IOASE40
IOASE42

Ensure the above security exit(s) has (have) not been modified.

If the above security exit(s) has (have) been modified, ensure that the security exit(s) has (have) been approved by the site systems programmer and the approval is on file for examination.

- b) If there have been no modifications to the security exits, or if modifications have been approved by Field Security Operations and the approval is on file for examination, there is NO FINDING.
- c) If there have been site modifications to the security exits and these modifications have not been approved by Field Security Operations, this is a FINDING.

CCI: CCI-000035

UNCLASSIFIED
z/OS BMC IOA for RACF Analysis and Checklist
Version 6 Release 6

___STIG ID: ZIOAR000

Default Severity: Category II

1. Check with your IOA or Systems Programming personnel and compile the list of BMC IOA Installation Datasets, Most likely similar to:
 SYS2.IOA.*.IOA*.* - /* All SYS2's */.
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?
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. Verify Read access is given, if applicable, to:
 Auditors
 BMC Users
 BMC STCs
 Batch Users
 Operations, Production Control and Scheduling 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. Verify Read access is given, if applicable, to:
 Auditors
 BMC Users
 BMC STCs
 Batch Users
 Operations, Production Control and Scheduling Personnel.
11. Repeat steps 2 through 10 for all datasets in option 1. above.
12. If 7, 8, 9 and 10 are all true, there is NO FINDING.

UNCLASSIFIED
z/OS BMC IOA for RACF Analysis and Checklist
Version 6 Release 6

13. If 7, 8, 9 and 10 are not true, this is a FINDING.

CCI: CCI-000213

CCI: CCI-002234

UNCLASSIFIED
z/OS BMC IOA for RACF Analysis and Checklist
Version 6 Release 6

___ **STIG ID: ZIOAR001**

Default Severity: Category II

- 1) Check with your IOA or Systems Programming personnel and compile the list of BMC IOA STCs. Most likely similar to:
 SYS3.IOA.*.IOAO.**.
- 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?
- 7) Verify that the UACC is NONE.
- 8) Tab down to Standard Access Permits and place an E next to it (hit enter).
 - a. Verify that UPDATE or higher access is limited to Systems Programming personnel.
 - b. Verify that Update access is permitted to BMC STCs, BMC Administrators, and batch users.
 - c. Verify Read access is limited to Auditors and BMC Users.
- 9) If Conditional Access Permits: _ (E to edit data) has *data is present* next to it, place an E next to it and hit enter.
 - a. Verify that UPDATE or higher access is limited to Systems Programming personnel.
 - b. Verify that Update access is permitted to BMC STCs, BMC Administrators, and batch users.
 - c. Verify Read access is limited to Auditors and BMC Users.
- 10) Repeat steps 2 through 9 for all datasets in option 1. above.
- 11) If 7, 8, and 9 are all true, there is NO FINDING.
- 12) If 7, 8, and 9 are not true, this is a FINDING.

CCI: CCI-001499

UNCLASSIFIED
z/OS BMC IOA for RACF Analysis and Checklist
Version 6 Release 6

___**STIG ID: ZIOAR002**

Default Severity: Category II

1. Check with your IOA or Systems Programming personnel and compile the list of BMC IOA User data sets. Most likely similar to:
 SYS3.IOA.*.IOAC.**.
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 1. above into: "Enter fully qualified (without quotes) data set or profile name: ".
5. Hit enter.
6. Enter Y for Display covering profile?
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, BMC STCs and/or batch users. Verify UPDATE access is limited to BMC Users. Verify Read access is given to Auditors.
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 access is limited to Systems Programming personnel, BMC STCs and/or batch users. Verify UPDATE access is limited to BMC Users and Production Control and/or Scheduling Personnel. Verify Read access is given to Auditors.
11. Repeat steps 2 through 10 for all datasets in option 1. above.
12. If 7, 8, 9 and 10 are all true, there is NO FINDING.
13. If 7, 8, 9 and 10 are not true, this is a FINDING.

CCI: CCI-001499

UNCLASSIFIED
z/OS BMC IOA for RACF Analysis and Checklist
Version 6 Release 6

___STIG ID: ZIOAR020

Default Severity: Category II

Verify that the accesses to resources in the BMC CONTROL-O Resources table in the z/OS STIG Addendum are properly restricted.

Note: To determine what resource class is used review the IOACCLASS setting in SECPARM to determine the resource class to use. Refer to ZIOA0040 for this setting.

a) Verify the resources identified in the BMC CONTROL-O Resources table in the z/OS STIG Addendum are properly defined and access is restricted to the appropriate personnel.

For all the PROFILES found in BMC BMC IOA Resources table in the z/OS STIG Addendum:

1. From the Administrator Main Menu Choose Option 3 Security Server Reports
2. then choose Option: 4 General Resource Profile
3. On the command line choose option 4 AND then Put (* or \$\$*)
next to PROFILE: and (class name from ZIOA0040) next to CLASS:

Profile: from table (or specify \$\$* as all profile start with a \$\$)

Class: from ZIOA0040

4. Hit enter.

5. Verify that the UACC for all profiles listed is NONE

6. Place an S next to the profile and validate that the access list is appropriate (as defined or more restrictive than the BMC IOA Resources table in the z/OS STIG Addendum.

If TYPE is GROUP, place an S in the CMD line
and hit enter to explode the GROUP.

7. For all resources with logging requirements place an LR next to the profile (hit enter and review the output) and validate that it specifies ALL(READ).

b) If all profiles, access lists, and Auditing are defined like or more restrictive than the BMC IOA Resources table in the z/OS STIG Addendum, then there is NO FINDING.

c) If any Profile, Access list or Auditing is more permissive than the BMC IOA Resources table in the z/OS STIG Addendum,
then there is a FINDING.

CCI: CCI-000035

CCI: CCI-002234

UNCLASSIFIED
z/OS BMC IOA for RACF Analysis and Checklist
Version 6 Release 6

___**STIG ID: ZIOAR030**

Default Severity: Category II

- a) From Analyzer main Menu, go to 3;4; Press ENTER
- b) Key in SORT PROCNAME; Press ENTER
- c) Key in L IOAGATE; Press ENTER
- d) If not found then IOAGATE; is not defined to RACF as a STC user.
- e) If found then use the U line command to determine if the userid is defined to RACF.
- f) The userid is defined to RACF if a userid display appears. If not defined you should see the message No data to display
- g) now press f3 to go back to the previous display. If no R is next to the entry then the user is protected.
- h) If an R is next to the entry, place an M on the command line and validate the following is NOT displayed:
VSA346R The user ID does not have the protected attribute.
- i) If the userid for the BMC IOA started task is defined to the security database and is protected, there is NO FINDING.
- j) If the userid for the BMC IOA started task is not defined to the security database, or is defined but does not have the protected attribute, this is a FINDING.

CCI: CCI-000764

UNCLASSIFIED
z/OS BMC IOA for RACF Analysis and Checklist
Version 6 Release 6

___**STIG ID: ZIOAR032**

Default Severity: Category II

a) Use Vanguard's Analyzer product to look at the Started Procedures Analysis report:

1. From Analyzer main Menu, go to 3;4; Press ENTER
2. Key in SORT PROCNAME; Press ENTER
3. Key in L IOAGATE; Press ENTER
4. Look at the source column. It will indicate STARTED class profile or ICHRIN03 entry.
5. If not found then IOAGATE is not defined to RACF as a STC user.

b) If a STARTED resource class profile exists for the IOAGATE STC, there is NO FINDING.

c) If neither a STARTED resource class profile or an ICHRIN03 entry exists for the IOAGATE STC, this is a FINDING.

CCI: CCI-000764

UNCLASSIFIED
z/OS BMC IOA for RACF Analysis and Checklist
Version 6 Release 6

___**STIG ID: ZIOAR040**

Default Severity: Category II

- a) The following keywords will have the specified values in the BMC IOA security parameter member:

Keyword	Value
DEFMCHKI	\$IOAEDM
SECTOLI	NO
DFMI06	EXTEND
DFMI07	EXTEND
DFMI09	EXTEND
DFMI12	EXTEND
DFMI16	EXTEND
DFMI32	EXTEND
DFMI40	EXTEND
DFMI42	EXTEND
IOACCLASS	\$IOA
RACSCLAS	SURROGAT
IOATCBS	YES

- b) If the above Keywords and Values are as specified, there is NO FINDING.
- c) If the above Keywords and Values are not as specified, there is a FINDING.

CCI: CCI-000035