



Using Vanguard Security Solutions to Complete DISA STIG SRR Review Procedures

z/OS CA MICS FOR RACF Analysis Process and Checklist

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

UNCLASSIFIED

z/OS CA MICS for RACF Analysis and Checklist

Version 6 Release 3

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

DISA Version 6.22

Document Number VTA_STIG-04222015-093000-622A

April, 2015

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 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.

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

Table of Contents

__STIG ID: ZMICR000..... 4
__STIG ID: ZMICR002..... 5

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

__STIG ID: ZMICR000

Default Severity: Category II

a) Consult with your systems programmer to identify the names of the CA MICS resource management installation datasets (they may possibly be called or begin with SYS2.MICS).

b) Ensure the following data set controls are in effect for the CA-MICS resource management installation data sets:

- READ access to the CA MICS installation data sets is restricted to authorized users (i.e. auditors, security administrators, and MICS end users).

- UPDATE or higher access to the CA MICS installation data sets is restricted to systems programming personnel and MICS administrators.

- UACC (None) and NOWARNING are specified for the CA MICS installation data sets.

- The RACF data set rules for the CA MICS 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 MICS 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 Update' 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 Update' which means that all failed UPDATE access is logged as specified in b. above.
7. Repeat steps 1-6 above for any other CA MICS dataset profiles.

d) If UPDATE access or higher to the CA MICS installation data sets are restricted to systems programming personnel and MICS administrators, there is NO FINDING.

e) If UPDATE access or higher to the CA MICS installation data sets are not restricted to systems programming personnel and MICS administrators ,there is a FINDING.

f) If UACC = None and Warning = No for all the CA MICS installation data sets there is NO FINDING.

g) If UACC is not None or Warning is not No for all the CA MICS installation data sets, there is a FINDING.

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

- h) If all accesses of UPDATE or higher are logged for all the CA MICS installation data sets there is NO FINDING.
- i) If all accesses of UPDATE or higher are not logged for all the CA MICS installation data sets, there is a FINDING.

CCI: CCI-000213

CCI: CCI-002234

UNCLASSIFIED

z/OS CA MICS for RACF Analysis and Checklist
Version 6 Release 3

STIG ID: ZMICR002

Default Severity: Category II

- a) Consult with your systems programmer to identify the names of the CA MICS resource management user datasets (they may possibly be called or begin with SYS2.MICS.DATA).
- b) Ensure the following data set controls are in effect for the CA-MICS resource management user data sets:
- READ access to the CA MICS user data sets is restricted to authorized users (i.e. auditors, security administrators, MICS end users).
 - WRITE or higher access to the CA MICS user data sets is restricted to systems programming personnel, SMF Batch user(s) and MICS Administrators.
 - UACC (None) and NOWARNING are specified for the CA MICS user data sets.
 - The RACF data set rules for the CA MICS user data sets specify that all accesses of WRITE 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 MICS 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 WRITE 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 WRITE access is logged as specified in b. above.
 7. Repeat steps 1-6 above for any other CA MICS dataset profiles.
- d) If WRITE access or higher to the CA MICS user data sets are restricted to systems programming personnel, there is NO FINDING.
- e) If WRITE access or higher to the CA MICS user data sets are not restricted to systems programming personnel there is a FINDING.

UNCLASSIFIED

z/OS CA MICS for RACF Analysis and Checklist

Version 6 Release 3

- f) If UACC = None and Warning = No for all the CA MICS user data sets there is NO FINDING.
- g) If UACC is not None or Warning is not No for all the CA MICS user data sets, there is a FINDING.
- h) If all accesses of WRITE or higher are logged for all the CA MICS user data sets there is NO FINDING.
- i) If all accesses of UPDATE or higher are not logged for all the CA MICS user data sets, there is a FINDING.

CCI: CCI-001499