



Using Vanguard Security Solutions to Complete DISA STIG SRR Review Procedures

z/OS CA Auditor for RACF Analysis Process and Checklist

Modeled After:
SRR REVIEW PROCEDURES
z/OS CA Auditor 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 ADT_STIG-08012016-105100-628A

August, 2016

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: ZADTR000 5

___STIG ID: ZADTR002 6

___STIG ID: ZADTR020 7

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

___STIG ID: ZADTR000

Default Severity: Category II

a) Check with your IOA or Systems Programming personnel and compile the list of CA-Auditor Installation Datasets, Likely:

1. SYS2.IOA.*.CTD*.**

SYS3.IOA.*.CTDI.**

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. Verify Read access is restricted to auditors, security administrators, and/or CA
Auditor's STCs and batch users.

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 restricted to auditors, security administrators, and/or CA Auditor's
STCs and batch users.

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 CA Auditor for RACF Analysis and Checklist
Version 6 Release 3

___**STIG ID: ZADTR002**

Default Severity: Category II

a) Check with your IOA or Systems Programming personnel and compile the list of CA-Auditor user data sets, Likely:

1. SYS3.EXAMINE

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, and/or ALTER access to systems programming personnel, security personnel and auditors.

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, and/or ALTER access to systems programming personnel, security personnel and auditors.

10. Repeat steps 2 through 10 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 CA Auditor for RACF Analysis and Checklist
Version 6 Release 3

___STIG ID: ZADTR020

Default Severity: Category II

Validate the following for the PROFILE LTDMMAIN resource in the PROGRAM resource

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 (LTDMMAIN)
next to PROFILE: and (PROGRAM) next to CLASS:
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 limited to systems
programmers, auditors and security personnel
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).

CCI: CCI-000035

CCI: CCI-002234