



Using Vanguard Security Solutions to Complete DISA STIG SRR Review Procedures

z/OS TDMF for RACF Analysis Process and Checklist

*Modeled After:
SRR REVIEW PROCEDURES
z/OS TDMF for RACF Checklist
Developed by DISA for the DOD
Version 6 Release 4
January 2015*

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

DISA Version 6.22

Document Number VSS_STIG-04222015-145200-622A

April, 2015

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: ZTDM0040	5
__STIG ID: ZTDMR000	6

UNCLASSIFIED

z/OS TDMF for RACF Analysis and Checklist

Version 6 Release 4

__STIG ID: ZTDM0040

Default Severity: Category II

a) Have the products system programmer display the configuration/parameters control statements used in the current running product to define or enable security for TDMF.

b) Verify the following specifications:

Parameter Options:

VOLUME SECURITY = YES

CHECK TARGET EMPTY = YES

Session Options:

Volume Security is not available.

CHECKTarget|CHKTarget

c) If (b) above is true, there is NO FINDING.

d) If (b) above is untrue, this is a FINDING

CCI: CCI-000035

UNCLASSIFIED

z/OS TDMF for RACF Analysis and Checklist

Version 6 Release 4

__STIG ID: ZTDMR000

Default Severity: Category II

- a) Check with your IOA or Systems Programming personnel and compile the list of Transparent Data Migration Facility (TDMF) Install data sets, Likely:
1. hlq.TDMF.**
 2. From the Administrator Main Menu Choose Option 2;3 (Security Server Commands, Data Sets)
 3. Type the resource names collected in option a.1 above at the prompt for “Enter fully qualified (without quotes) data set or profile name:”.
 4. Hit enter.
 5. Enter Y for Display covering profile? Y
 6. Verify that the UACC is NONE
 7. Verify that Audit Successes and Failures specifies UPDATE.
 8. Tab down to Standard Access Permits and place an ‘E’ next to the phrase and hit ENTER.
 9. Verify that the data set rules for the product install data sets
 - a. Permit READ access to all authorized users
 - b. Restrict UPDATE or higher access to systems programming personnel.
 10. Tab down to Conditional Access Permits line on the screen. If the phrase ‘*data is present*’ is found, enter an ‘E’ and hit ENTER.
 11. Verify that any additional data set rules for the product install data sets
 - a. Permit READ access only to authorized users
 - b. Restrict UPDATE or higher access to systems programming personnel
 12. Repeat steps 2 through 10 for all datasets in option a.1
- b) If 10a, 10b, 12a, and 12b are all true, there is NO FINDING.
- c) If 10a, 10b, 12a, and 12b are not true, this is a FINDING.

CCI: CCI-000213

CCI: CCI-002234