VANGUARD
Integrity Professionals, Inc.
Enterprise Security Software

Using Vanguard Security Solutions to Complete DISA STIG SRR Review Procedures

Integrated Crypto Service Facility for RACF Analysis Process and Checklist

Modeled After:
SRR REVIEW PROCEDURES
z/OS ICSF 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 6.22

Document Number VSS_STIG-04222015-103700-622A

April, 2015

Copyright

© 1989-2010 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: ZICSR000 5
___STIG ID: ZICSR001 6
___STIG ID: ZICSR030 7
___STIG ID: ZICSR032 8

___STIG ID: ZICSR000 **Default Severity:** Category II

a) Check with your IOA or Systems Programming personnel and compile the list of IBM Integrated Crypto Service Facility (ICSF) install data sets, Likely:
1. SYS1.CSF.**
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 that READ access is limited to Systems Programming Personnel and Auditors and any other users that have a valid requirement to utilize these data sets. Press F3 to return to previous screen.
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 that READ access is limited to Systems Programming Personnel and Auditors and any other users that have a valid requirement to utilize these data sets. Press F3 to return to previous screen.
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

___STIG ID: ZICSR001 **Default Severity:** Category II

a) Check with your IOA or Systems Programming personnel and compile the list of IBM Integrated Crypto Service Facility (ICSF) datasets referenced in the CSFPARM DD statement of the ICSF started task(s) and/or batch job(s), the entries for CKDSN and PKDSN specify the data sets. They are Likely:
1. SYS3.CSF.CKDS and SYS3.CSF.PKDS.
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, ICSF STC and/or batch jobs only. Verify that READ access is limited to Systems Programming Personnel, ICSF STC, batch jobs and 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, ICSF STC and/or batch jobs only. Verify that READ access is limited to Systems Programming Personnel, ICSF STC, batch jobs and Auditors.
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-001499

___STIG ID: ZICSR030 **Default Severity:** Category II

1. From the Vanguard Security Solutions choose Administrator Option 1.
   2. Choose 3 Security Server Reports
   3. Choose option 1 User Profiles. Make sure you are in Live mode by typing LIVE on command line.
   4. Tab down to USERID and type in CSFSTART. (CSFSTART is the userid that must be associated with the started task profile.)
   5. Choose option 1, User Summary and hit enter.
   6. If the report displays NO USERIDS TO REPORT, this is a finding.
   7. If the report displays the User CSFSTART, place a UA next to the userid. If the display does not show PT under the PROT column or shows No USERIDS to Report, then there is a FINDING.
   8. If the USERID exists and PT is specified in the PROT column, then there is NO FINDING.

CCI: CCI-000764

___STIG ID: ZICSR032 **Default Severity:** Category II

1. From the Vanguard Security Solutions choose option 3 Analyzer.
2. Choose Option 3 Online Displays
3. Choose Option 4 Started Procedures Analysis
4. Do a SORT on PROCNAME and then L CSFSTART.
5. If CSFSTART exists and does not have any Messages associated with it, there is NO FINDING.
6. If CSFSTART does not exist or has Messages associated with it, there is a FINDING.

CCI: CCI-000764