



Using Vanguard Security Solutions to Complete  
DISA STIG SRR Review Procedures

**z/OS HEALTH CHECKER for RACF**  
**Analysis Process and Checklist**

*Modeled After:*  
*SRR REVIEW PROCEDURES*  
*z/OS HEALTH CHECKER Checklist for RACF*  
*Developed by Vanguard Integrity Professionals*  
*Version 6 Release 2*  
*January 2015*

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

DISA Version 6.28

Document Number HCK\_STIG-08012016-110000-628A

August, 2016

## 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: ZHCKR001.....	5
___STIG ID: ZHCKR030.....	7
___STIG ID: ZHCKR032.....	9

## UNCLASSIFIED

### z/OS HEALTH CHECKER for RACF Analysis Process and Checklist Version 6 Release 2

\_\_\_STIG ID: ZHCKR001

**Default Severity: Category II**

- a) Consult with your systems programmer to identify the name of the IBM Health Checker STC dataset(s) - very likely called 'SYS3.\*.HZSPDATA'. The STC dataset names can also be found on the HZSPDATA DD statement in proc HZSPROC (the Health Checker STC proc).
- b) Ensure the following data set controls are in effect for the IBM Health Checker STC data sets:
- READ access to the IBM Health Checker STC data sets can be given to auditors
  - UPDATE access to the IBM Health Checker STC data sets is restricted to domain level security administrators
  - UPDATE or higher access to the IBM Health Checker STC data sets is restricted to systems programming personnel, the Health Checker STC and authorized batch users
  - UACC (None) and NOWARNING are specified for the IBM Health Checker STC data sets
  - the RACF data set rules for the IBM Health Checker STC 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 row, type LV next to the dataset profile for the IBM Health Checker STC data sets.
  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' and 'Audit Failures' columns on the dataset profile General Information screen . They should specify 'Successes Write' and 'Failures Write' respectively.
  6. Repeat steps 1-5 above for any other IBM Health Checker dataset profiles.
- d) If UPDATE and ALLOCATE (e.g. ALTER) access to the IBM Health Checker STC data sets are specified as in b. above, there is NO FINDING.

**UNCLASSIFIED**

z/OS HEALTH CHECKER for RACF Analysis Process and Checklist

*Version 6 Release 2*

- e) If UPDATE and ALLOCATE (ALTER) access to the IBM Health Checker STC data sets is not restricted as in b. above there is a FINDING.
- f) If UACC = None and Warning = No there is NO FINDING
- g) If UACC is not None or Warning is not No, this is a FINDING.
- h) If logging is as specified in b. above there is NO FINDING.
- i) If logging is not as specified in b. above, there is a FINDING.

**CCI:** CCI-001499

## UNCLASSIFIED

### z/OS HEALTH CHECKER for RACF Analysis Process and Checklist Version 6 Release 2

\_\_\_STIG ID: ZHCKR030

Default Severity: Category II

- a) From the Administrator main menu, select 3;4 (Security Server Reports - General Resource Reports) and press ENTER.
- b) Type 1 for General Resource Profile Summary and tab down to CLASS and enter 'STARTED' for class name.
- c) Find the Health Checker General Resource profile and enter 'LR' next to it and hit ENTER. If not found go to step k. below.
- d) Find the userid associated with the Health Checker started task under the STDATA segment information of the Health Checker general resource profile.
- e) Go back to Administrator main menu, select 3;1 (Security Server Reports User Profile) and press Enter.
- f) Enter 2 (for User Attributes) and tab down to User ID and enter the User ID found in Step d) above and hit Enter.
- g) If the last column on the screen (PROT) is set to "PT", the Userid has the PROTECTED attribute set. If the last column is blank, the Userid does not have the PROTECTED attribute set.
- h) If PROTECTED = Yes, there is no FINDING.
- i) If PROTECTED = No, there is a FINDING.
- j). End Check
- k) If Health Checker is NOT found as a General Resource profile under the STARTED class in c.above, then check if is defined in the Started Procedures Table (ICHRIN03) as follows:
  1. From Analyzer main Menu, go to 3;4 (Online Displays Started Procedures Analysis) and Press Enter.
  2. Look for STARTED in the Source column and HZSPROC in the Procname column.
  3. If the Health Checker started procedure does not have an R in the M column there is NO FINDING (an R in the M column indicates that either the STARTED TASK USER ID does not have the protected attribute or is not defined (these are both findings) ).

**UNCLASSIFIED**

**z/OS HEALTH CHECKER for RACF Analysis Process and Checklist**  
*Version 6 Release 2*

4. If there is an R in the M column, there is a FINDING.

**CCI:** CCI-000764



**UNCLASSIFIED**

**z/OS HEALTH CHECKER for RACF Analysis Process and Checklist**  
*Version 6 Release 2*

**\_\_\_STIG ID: ZHCKR032**

**Default Severity: Category II**

- a) From the Administrator main menu, select 3;4 (Security Server Reports - General Resource Reports) and press ENTER.
- b) Type 1 for General Resource Profile Summary and tab down to CLASS and enter 'STARTED' for class name.
- c) Find the Health Checker General Resource profile (HZSPROC)..
- d). If found, there is NO FINDING.
- e) If not found, then check if is defined in the Started Procedures Table (ICHRIN03) as follows:
  - 1. From Analyzer main Menu, go to 3;4 (Online Displays Started Procedures Analysis) and Press Enter.
  - 2. Look for STARTED in the Source column and HZSPROC in the Procname Column.
  - 3. If found, there is NO FINDING.
  - 4. If it is not found, there is a FINDING.

**CCI:** CCI-000764