



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

### **z/OS Quest NC-PASS for RACF Analysis Process and Checklist**

*Modeled After:*  
*SRR REVIEW PROCEDURES*  
*z/OS NC-PASS for RACF Checklist*  
*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 RACF\_STIG-08012016-103200-628A

November, 2019

## 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: ZNCPR000 ..... 5
- \_\_STIG ID: ZNCPR001 ..... 6
- \_\_STIG ID: ZNCPR020 ..... 7
- \_\_STIG ID: ZNCPR030 ..... 8
- \_\_STIG ID: ZNCPR032 ..... 9

**UNCLASSIFIED**  
z/OS Quest NC-Pass for RACF Analysis and Checklist  
*Version 6 Release 2*

**\_\_STIG ID: ZNCPR000**

**Default Severity: Category II**

- a) Consult with your systems programmer to identify the names of the QUEST NC-PASS product datasets. (They may begin with SYS2.CCS, SYS2A.CS., or SYS3.CCS).
- b) Ensure the following data set controls are in effect for the QUEST NC-PASS product data sets:
  - UPDATE or higher access to the QUEST NC-PASS product data sets is restricted to systems programming personnel.
  - UACC (None) and NOWARNING are specified for the QUEST NC-PASS product data sets..
  - The RACF data set rules for the QUEST NC-PASS data sets specify that all accesses of UPDATE or higher (i.e., failures and successes) will be logged.
- c) Verify as follows:
  - 1. From the Administrator main menu, select 3.3 (Dataset Profile Reports) and press <ENTER>.
  - 2. Tab down to “Data Set” row, type LV next to the dataset profile for the QUEST NC-PASS data sets.
  - 3. Check that UACC = None and Warning = No on the dataset profile General Information Screen.
  - 4. Review the Universal Access and Access List on the dataset profile General Information Screen..
  - 5. Repeat steps 1-3 above for any other QUEST NC-PASS dataset profiles.
- d) If UPDATE and ALLOCATE (e.g. ALTER) access to the QUEST NC-PASS product data sets are restricted to systems programming personnel, there is NO FINDING.
- e) If UPDATE and ALLOCATE (ALTER) access to the CA -1 product data sets is **not** restricted to systems programming personnel, this 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..

**CCI: CCI-000213**

**CCI: CCI-002234**

**UNCLASSIFIED**  
z/OS Quest NC-Pass for RACF Analysis and Checklist  
Version 6 Release 2

**\_\_STIG ID: ZNCPR001**

**Default Severity: Category II**

- a) Create a dataset (DSORG: FB LRECL: 80) with a list of the NC-PASS data sets referenced in Section 6.3.2, NC-PASS for RACF, in the Z/OS STIG. Enter each dataset on its own line and starting in column 1.

*Note: Use ISPF 3.4 with the high-level qualifiers for the NC-PASS datasets to assist in generating the list of datasets.*

- b) From Analyzer main Menu, go to 3;B; Press ENTER
- c) Place an S next to “User defined list”. Key in the name of the dataset created in step (a) in the “Fully qualified (without quotes) name of data set containing list:” field. Press <ENTER>
- d) Place an R next one of the entries in the report. Press ENTER
1. If the RACF data set rules restrict UPDATE and/or ALTER access to Z/OS systems programming personnel and/or security personnel, there is NO FINDING.
  2. If the RACF data set rules restrict UPDATE access to the NC-PASS started task user ID, there is NO FINDING.
- e) If (d1) or (d2) is untrue, there is a FINDING.
- f) Repeat steps (d) (d1) and (d2) for each dataset in the list.

**CCI: CCI-001499**

**UNCLASSIFIED**  
z/OS Quest NC-Pass for RACF Analysis and Checklist  
*Version 6 Release 2*

**\_\_STIG ID: ZNCPR020**

**Default Severity: Category II**

- a) From Administrator main Menu, go to 3;15; Press ENTER
- b) Key in SECURID in the Group field. Press ENTER.
- c) If their report contains only the line NO CONNECTS TO REPORT, then SECURID is not defined as a group and there is a FINDING.
- d) If there is a SECURID group, then key in CS next the SECURID entry and press <ENTER>.
- e) Examine the list of user IDs in the Connect Summary report and ensure that Sensitive users (see note below) that require NC-PASS validation are connected to the SECURID group. If not, there is a FINDING.

Note: Sensitive users include systems programming personnel, security personnel, and other staff (e.g., DASD management, operations, auditors, technical support, etc.) with access to sensitive resources (e.g., operator commands, ACP privileges, etc.) that can modify the operating system and system software, and review/modify the security environment.

**CCI: CCI-000035**

**CCI: CCI-002234**

**UNCLASSIFIED**

z/OS Quest NC-Pass for RACF Analysis and Checklist  
*Version 6 Release 2*

**\_\_STIG ID: ZNCPR030**

**Default Severity:** Category II

- a) From Analyzer main Menu, go to 3;4 (Online Displays – Started Procedures Analysis) and Press ENTER
- b) Look for STARTED in the Source column, NCPASS in the Procname column and \* in the Jobname column.
- c) If the NC-PASS started task 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)
- d) If there is an R in the “M” column, there is a FINDING

**CCI:** CCI-000764



**UNCLASSIFIED**

z/OS Quest NC-Pass for RACF Analysis and Checklist  
*Version 6 Release 2*

**\_\_STIG ID: ZNCPR032**

**Default Severity:** Category II

- a) From Analyzer main Menu, go to 3;4; Press <ENTER>
- b) Look for STARTED in the Source column, NCPASS in the Procname column and \* in the Jobname column. If the entry exists, there is NO FINDING.
- c) If the entry looked for in step (b) above is not found, this is a FINDING.

**CCI:** CCI-000764