



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

### **z/OS ABEND AID for RACF Analysis Process and Checklist**

*Modeled After:*  
*SRR REVIEW PROCEDURES*  
*z/OS ABEND AID Checklist for RACF*  
*Developed by Vanguard Integrity Professionals*  
*Version 6 Release 4*  
*January 2015*

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

DISA Version 6.22

Document Number ABAID\_STIG-04222015-082200-622A

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: ZAID0040 ..... 5

\_\_\_STIG ID: ZAIDR000 ..... 6

\_\_\_STIG ID: ZAIDR001 ..... 8

\_\_\_STIG ID: ZAIDR020 ..... 10

\_\_\_STIG ID: ZAIDR030 ..... 12

\_\_\_STIG ID: ZAIDR032 ..... 14

**UNCLASSIFIED**

z/OS Abend Aid for RACF Analysis Process and Checklist

*Version 6 Release 4*

**\_\_\_STIG ID: ZAID0040**

**Default Severity:** Category II

- a) Use TSO option 3.4 to find the name of the Contents Dataset specified in the FDBDPARM DD statement in the Abend Aid started task procedure.
- b) Check the Contents Dataset for the setting of the parameter "External\_Security\_Enabled".
- c). If the setting of this parameter is "YES", there is NO FINDING.
- d) If the setting of this parameter is "NO", there is a FINDING.

**CCI:** CCI-000035

## UNCLASSIFIED

z/OS Abend Aid for RACF Analysis Process and Checklist

Version 6 Release 4

\_\_\_STIG ID: ZAIDR000

Default Severity: Category II

- a) Consult with your systems programmer to identify the names of the Compuware Abend-Aid product installation datasets (they may likely be called or begin with SYS2.ABENDAID, SYS2A.ABENDAID or SYS3A.ABENDAID).
- b) Ensure the following data set controls are in effect for the Compuware Abend-Aid installation data sets:
- READ access to the Compuware Abend-Aid installation data sets is restricted to authorized users.
  - UPDATE or higher access to the Compuware Abend-Aid installation data sets is restricted to systems programming personnel.
  - UACC (None) and NOWARNING are specified for the Compuware Abend-Aid installation data sets.
  - The RACF data set rules for the Compuware Abend-Aid 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 rows and type LV next to the dataset profile for the Compuware Abend-Aid 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' column on the dataset profile General Information screen. Underneath it should be found 'Successes Write' which means that all successful WRITE access is logged as specified in b.above.
  6. Verify the 'Audit Failures' column on the dataset profile General Information screen. Underneath it should be found 'Failures Write' which means that all failed WRITE access is logged as specified in b. above.
  7. Repeat steps 1-6 above for any other Compuware Abend-Aid dataset profiles.
- d) If UPDATE and ALLOCATE (e.g. ALTER) access to the Compuware Abend-Aid installation data sets are restricted to systems programming personnel, there is NO FINDING.

**UNCLASSIFIED**

**z/OS Abend Aid for RACF Analysis Process and Checklist**

*Version 6 Release 4*

- e) If UPDATE and ALLOCATE (ALTER) access to the Compuware Abend-Aid installation sets is not restricted to systems programming personnel 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, there is a FINDING.
- h) If all accesses of UPDATE or higher are logged there is NO FINDING.
- i) If all accesses of UPDATE or higher are not logged, there is a FINDING.

**CCI:** CCI-000213

**CCI:** CCI-002234

## UNCLASSIFIED

### z/OS Abend Aid for RACF Analysis Process and Checklist Version 6 Release 4

\_\_\_**STIG ID: ZAIDR001**

Default Severity: Category II

- a) Consult with your systems programmer to identify the names of the Compuware Abend-Aid product STC datasets (they may likely be called or begin with SYS3.ABENDAID).
- b) Ensure the following data set controls are in effect for the Compuware Abend-Aid STC data sets:
  - READ access to the Compuware Abend-Aid product STC data sets can be given to auditors.
  - UPDATE or higher access to the Compuware Abend-Aid product STC data sets is restricted to selected systems programming personnel and/or Abend Aid STCs and/or batch users.
  - UACC (None) and NOWARNING are specified for the Compuware Abend-Aid product STC data sets.
  - The RACF data set rules for the Compuware Abend-Aid STC 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 Compuware Abend-Aid 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 areas 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' column 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 Compuware Abend-Aid STC dataset profiles.
- d) If UPDATE and ALLOCATE (e.g. ALTER) access to the Compuware Abend-Aid STC data sets are specified as in b. above, there is NO FINDING.
- e) If UPDATE and ALLOCATE (ALTER) access to the Compuware Abend-Aid sets is not restricted as in b. above there is a FINDING.
- f) If UACC = None and Warning = No there is NO FINDING



**UNCLASSIFIED**

**z/OS Abend Aid for RACF Analysis Process and Checklist**  
*Version 6 Release 4*

- 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 Abend Aid for RACF Analysis Process and Checklist Version 6 Release 4

\_\_\_STIG ID: ZAIDR020

Default Severity: Category II

- a) From the Administrator main menu, select 3;4 (Security Server Reports, General Resource Profiles) and press ENTER.
- b) Tab down to "CLASS: ", and enter the Abend-Aid resource class name and press ENTER.  
(The Abend-Aid resource class name can be found in the Abend Aid STC JCL. It is the value specified for the EXTERNAL\_SECURITY\_RESOURCE\_CLASS parameter in the configuration file referenced on the FDBPARM DD statement)
- c) Check the profiles that are displayed on the General Resource Profile Summary screen. For any profiles on the display that are found in the Compuware Abend Aid Resources table in the z/OS STIG addendum:
  1. Verify that they are defined with a UACC=NONE.
  2. Type **LR** in the CMD column of each resource name and check that:
    - Warning is set to NO
    - The list of users and conditional access users only include users that belong to the groups specified in the COMPUWARE Abend-Aid resources table\*\*.
    - The access level for each user is ALTER or less.

\*\* (To check if a user belongs to one of the groups in the COMPUWARE Abend-Aid resources table:

  - Select Option 3;2 from the Administrator Main Menu (Security Server Reports, Group Profiles)
  - On the Group Reports Menu, enter 1 at the Command line (for Group Profile Summary)
  - Then tab down to Group and enter the Group Name from the resources table and hit enter.
  - On the next panel enter '**LV**' next to the group name and hit enter.
  - The 'General Information Screen' that comes up will have the list of Connected Users
- d) If
  - WARNING is not set to NO or
  - UACC is not NONE or
  - any users are granted access who are not in the Compuware Abend Aid Resources table
  - or Access is greater than ALTER for any Abend Aid Resource, there is a FINDING.

**UNCLASSIFIED**

**z/OS Abend Aid for RACF Analysis Process and Checklist**  
*Version 6 Release 4*

e) If none of the conditions in d) above are true, then there is NO FINDING..

**CCI:** CCI-000035

**CCI:** CCI-002234

## UNCLASSIFIED

### z/OS Abend Aid for RACF Analysis Process and Checklist Version 6 Release 4

\_\_\_**STIG ID: ZAIDR030**

**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, type STARTED for class name and hit Enter.
- c) Find the Abend Aid 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 Abend Aid started task under the STDATA segment information of the Abend Aid 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 Abend Aid 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 the Abend Aid started task Procname in the Procname column.
  3. If the Abend Aid 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 Abend Aid for RACF Analysis Process and Checklist

*Version 6 Release 4*

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

**CCI:** CCI-000764

**UNCLASSIFIED**

**z/OS Abend Aid for RACF Analysis Process and Checklist**  
*Version 6 Release 4*

**\_\_\_STIG ID: ZAIDR032**

**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 Abend Aid started task procname..
- 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 the ABEND AID started task proc name in the Procname column
  - 3. If found, there is NO FINDING.
  - 4. If it is not found, there is a FINDING.

**CCI:** CCI-000764