



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

### **z/OS RACF Analysis Process and Checklist**

*Modeled After:  
SRR REVIEW PROCEDURES  
z/OS RACF Checklist  
Developed by Vanguard Integrity Professionals  
Version 6 Release 39*

*January 2019*



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

### **z/OS CA-1 for RACF Analysis Process and Checklist**

*Modeled After:*  
*SRR REVIEW PROCEDURES*  
*z/OS CA-1 for RACF Checklist*  
*Developed by Vanguard Integrity Professionals*  
*Version 6 Release 7*  
*May 2019*

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

DISA Version 6.28

Document Number CA1-STIG-08012016-131800-628A

April, 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: ZCA10041 .....	6
__STIG ID: ZCA10060 .....	9
__STIG ID: ZCA1R000.....	10
__STIG ID: ZCA1R003.....	11
__STIG ID: ZCA1R020.....	13
__STIG ID: ZCA1R021.....	14
__STIG ID: ZCA1R030.....	16
__STIG ID: ZCA1R032.....	17
__STIG ID: ZCA1R038.....	18
__STIG ID: ZCA1R040.....	19

**UNCLASSIFIED**  
z/OS CA-1 for RACF Analysis and Checklist  
Version 6 Release 7

**\_\_STIG ID: ZCA10041**

**Default Severity: Category II**

- a) Determine if the CA-1 default system password 'CA1(TMS)' is being utilized.
- b) If the installed release of CA-1 is 11.5 or below do the following:
  - 1. From Analyzer Main Menu, go to 3;B Sensitive and Critical Datasets Analysis and place an S next to Authorized Program Facility (APF) Table, then ENTER.
  - 2. Locate the CA-1 LINKLIB dataset and enter an H in the Opt column for that dataset to search for a character string in the TMSTMVT module .
  - 3. On the next panel, enter TMSTMVT in the Member list field and C'CA1(TMS)' in the Search text field.
  - 4. If the Count column of the next display is zero (0), there is NO FINDING (meaning the default CA-1 system password is not being used).
  - 5. If the Count column of the next display is not zero, there is a FINDING as the default CA-1 system password has been found..
- c) If the installed release of CA-1 is 12.0 or above do the following:
  - 1. Check the 'SHUTDOWN' option for the presence of the CA\_! default password.
  - 2. To examine the SHUTDOWN option
    - a. Find the TMSINIT STC proc.
    - b. Find the TMSPARM DD statement which points to a PDS.
    - c. Look at the member TMOSYSxx in this dataset
    - d. Member TMOSYSxx will point to member TMOOPTxx which specifies the SHUTDOWN option.
    - e. If the CA\_1 password is specified in the SHUTDOWN option, this is a FINDING.
    - f. If the CA \_1 password is not specified in the SHUTDOWN option, there is no FINDING.

Note re c: above – needs verification as to what data is actually present on the SHUTDOWN option statement and also clarification as to where 'member' TMOOPTxx and TMOSYSxx actually are . Are they both PDS members and if so of which PDS's exactly?

**CCI: CCI-000035**

**UNCLASSIFIED**  
z/OS CA-1 for RACF Analysis and Checklist  
*Version 6 Release 7*

**\_\_STIG ID: ZCA1R001**

**Default Severity: Category II**

Ensure that WRITE and/or greater access to CA1 Tape management STC data sets is limited to System Programmers and/or CA1 Tape management STC(s) and/or batch user(s) only. READ access can be given to auditors.

- a) Check with your IOA or Systems Programming personnel and compile the list of CA CA-1 product installation data sets. Likely these data set names will start with CA1.TMS
- b). Do the following:
  1. From the Administrator Main Menu Choose Option 2 - Security Server Commands
  2. Then choose Option 3 - Data Set
  3. Tab to Enter fully qualified (without quotes) data set or profile name: and enter the name of the first CA CA-1 product installation data set found in a. above.
  4. Hit Enter.
  5. For the resulting pop-up, select Y when prompted with Display covering profile?
  6. On the next screen,
    - a. Verify that the UACC is NONE
    - b. Verify that all accesses of UPDATE or higher (i.e., failures and successes) will be logged. Look at the section of the screen under Audit: Next to Successes and Failures you should see Update.
  - c. Tab down to; Standard Access Permits and type an E and hit Enter.
  - d. On the next screen verify that UPDATE, and/or ALTER access is permitted to systems programming personnel, tape management personnel (tape librarians and any other users that perform control, initialization, and maintenance of the systems tape library) and CA CA-1 STCs and/or CA CA-1 batch userids..
  - e. Check if the Conditional Access Permits: section on the screen has the phrase \*data is present\* next to it.  
If so, enter an E on the line and hit Enter to get a list of who has Conditional Access Permits.
  - f. Verify that Conditional Access Permits of UPDATE, and/or ALTER access are restricted to systems programming personnel, tape management personnel (tape librarians and any other users that perform control initialization and maintenance of the systems tape library) and CA CA-1 STCs and/ or CA CA-1 batch userids.
7. Repeat steps 3 through 6 for all the CA CA-1 datasets found in a. above.
- c) If 6a, 6b, 6d and 6f above are all true, there is NO FINDING.

**UNCLASSIFIED**  
z/OS CA-1 for RACF Analysis and Checklist  
*Version 6 Release 7*

d) If 6a, 6b, 6d and 6f above are NOT all true, there is a FINDING..

**CCI:** CCI-001499



**UNCLASSIFIED**  
z/OS CA-1 for RACF Analysis and Checklist  
*Version 6 Release 7*

**\_\_STIG ID: ZCA10060**

**Default Severity: Category II**

1. If the installed release of CA-1 is 11.5 or below do the following:
  - a) Determine if either of the CA-1 security exits TMSUXnA and/or TMSUXnS is active.
  - b) From whatever tool is being used to view JES output, select any CA\_1 startup JES spool output data.
    1. Find all occurrences of TMSUX.
    2. For any exit that indicates ACTIVATED, determine if the name of the exit matches the TMSUXnA or TMSUXnS security exit criteria.
  - c) If there is an active TMSUXnA or TMSUXnS security exit ensure that it meets the following requirements:
    1. The usage and function of any active exit is fully documented,
    2. The exit code has been reviewed by a qualified security analyst,
    3. The use of the any active exit is approved by Security Management,
    4. All associated documentation is filed in the appropriate location.
  - d) If all of the items in (c) above are satisfied, there is no FINDING.
  - e) If any of the items in (c) above are not satisfied, there is a FINDING.
2. If the installed release of CA-1 is 12.0 or above do steps 1.a to 1. e above, but search for exit names TSMXITA and TSMXITS instead of TMSUXnA and TMSUXnS.

**CCI: CCI-000035**

**UNCLASSIFIED**  
z/OS CA-1 for RACF Analysis and Checklist  
*Version 6 Release 7*

**\_\_STIG ID: ZCA1R000**

**Default Severity: Category II**

- a) Consult with your systems programmer to identify the names of the CA-1 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 CA-1 product data sets:
  - UPDATE or higher access to the CA-1 product data sets is restricted to systems programming personnel.
  - UACC (None) and NOWARNING are specified for the CA-1 product data sets..
  - The RACF data set rules for the CA-1 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 CA-1 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 CA-1 dataset profiles.
- d) If UPDATE and ALLOCATE (e.g. ALTER) access to the CA-1 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 CA-1 for RACF Analysis and Checklist  
*Version 6 Release 7*

**\_\_STIG ID: ZCA1R003**

**Default Severity: Category II**

- a) Ensure that the CA-1 TMC and Audit data sets are properly protected and optional RDS and VPD data sets are properly protected. The RACF data set rule for the above data sets restrict READ access to application support personnel, production control and scheduling personnel.
- b) Based on Dataset Naming Conventions, identify effective masks to use to report on the TMC and Audit data sets. The low level qualifier of the data set names will probably be TMC and AUDIT respectively.
- c) Once the masks are identified, from Administrator Main Menu, go to 3;3 Data Set Reports.
  - 1. Select option 4 Access Lists, option B for Batch, and option Y for Enhanced Masking, then ENTER
  - 2. On the next panel enter the enhanced masking values separated by the OR logic operand. E.g.

**DATASET EQ SYS3.CA1.\*TMC OR  
DATASET EQ SYS3.CA1.\*AUDIT**

- 3. On the next panel enter a Y in the “Explode RACF groups access list at end of report” field enter an N in all other fields, then ENTER .
  - 4. Submit the Batch Job.
  - 5. Review the output in the PRNT JES data set for the report.
- d) The data set profiles listed above should restrict READ access to users with justification.
- e) Only z/OS systems programmer and tape management personnel should have UPDATE or higher access through these data set profiles.
- f) In addition to z/OS systems programmers, Tape Librarians, CA 1 batch production batch jobs and CA 1 started tasks are allowed UPDATE access through these data set profiles.
- g) From Administrator Main Menu, once again go to 3;3 Data Set Reports.
  - 1. Select option 2 Audit Flags, option B for Batch, and option Y for Enhanced Masking, then ENTER .
  - 2. On the next panel enter the enhanced masking values separated by the OR logic operand. E.g.

**DATASET EQ SYS3.CA1.\*TMC OR  
DATASET EQ SYS3.CA1.\*AUDIT**

- 3. Submit the Batch Job.

**UNCLASSIFIED**  
z/OS CA-1 for RACF Analysis and Checklist  
*Version 6 Release 7*

- 4 . Review the output in the PRNT JES dataset for the report.
- f) The data set profiles should specify successful ALTER access and all FAIL access attempts are logged.
  - g) If all of the items above are true, there are NO FINDINGS.
  - h) If any of the items above is untrue, there is one or more FINDINGS.

**CCI:** CCI-000035

**UNCLASSIFIED**  
z/OS CA-1 for RACF Analysis and Checklist  
*Version 6 Release 7*

**\_\_STIG ID: ZCA1R020**

**Default Severity: Category II**

- a) Ensure that all CA-1 command resources are properly protected.
- b) The CA-1 command resources RACF General Resource Class should be CA@MD. Once this has been verified, from Administrator Main Menu, go to 3;4 General Resource Reports.
  - 1. Select option 4 Access Lists, option B for Batch, and set the CLASS masking field to CA@MD, then <ENTER>.
  - 2. On the next panel enter a Y in the “Explode RACF groups access list at end of report” field, enter an N in all other fields, then <ENTER>.
  - 3. Submit the Batch Job.
  - 4. Review the output in the PRNT JES data set for the report.

- c) Only the Tape Librarian should have READ access to the following profiles:

**L0ADD, L0CLEAN, LOCHECKI, LOCHECKO, L0DELETE,  
L0ERASE, L0EXPIRE, L0RETAIN, L0SCRATC**

- d) Only the Tape Librarian and users requiring the functionality of extending retention dates for tape data sets should have READ access to the following profile:

**L0EXTEND**

- e) The tape Librarian and systems programmers only have READ access to the following profile:

**L0UPDTE**

- f) If all of the CA-1 command resources are protected at the appropriate levels, there is NO FINDING.
- g) If any CA-1 command resource is not protected properly, there is a FINDING.

**CCI: CCI-000035**

**CCI: CCI-002234**

**UNCLASSIFIED**  
z/OS CA-1 for RACF Analysis and Checklist  
Version 6 Release 7

\_\_**STIG ID: ZCA1R021**

**Default Severity:** Category II

- a) Ensure that all CA-1 command resources are properly protected.
- b) The CA-1 command resources RACF General Resource Class should be CA@MD.  
Once this has been verified, from Administrator Main Menu, go to 3;4 General Resource Reports.
  - 1. Select option 4 Access Lists, option B for Batch, and set the CLASS masking field to CA@MD, then <ENTER>.
  - 2. On the next panel enter a Y in the “Explode RACF groups access list at end of report” field, enter an N in all other fields, then <ENTER>.
  - 3. Submit the Batch Job.
  - 4. Review the output in the PRNT JES data set for the report..
- c) Only the Tape Librarian and Technical Support Personnel should have READ and UPDATE access to the following profiles:

**NLRES, NLNORES, NSLRES**

- d) Only the Tape Librarian and Systems Programmers should have READ and UPDATE access to the following profiles:

**NSLNORES, BLPRES, BLPNORES**

- e) The Tape Librarian only should have READ and UPDATE access to the following profiles:  
FORRES, YSVCUNCD
- f) Systems Programmers should have READ access to the following profile:  
YSVCUNCD
- g) Systems Programmers and Operators would have access to the following profiles:  
REINIT, BATCH, DEACT
- h) Users requiring access to CA-1 on-line applications for tape data set processing would have access through passwords. There are different passwords for different levels of functionality from general user to tape librarian..
- i) If all of the CA-1 command resources are protected at the appropriate levels, there is NO FINDING.
- j) If any CA-1 command resource is not protected properly, there is a FINDING.

**\*\*Note:** Tape librarian includes tape personnel, as well as STCs and Batch Users that perform CA 1 maintenance.

**UNCLASSIFIED**  
z/OS CA-1 for RACF Analysis and Checklist  
*Version 6 Release 7*

**CCI:** CCI-000035

**CCI:** CCI-002234

**UNCLASSIFIED**  
z/OS CA-1 for RACF Analysis and Checklist  
*Version 6 Release 7*

**\_\_STIG ID: ZCA1R030**

**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.
- c).Find CA-1 started class General Resource profile usually named TMSINIT.
- d). Find the Userid associated with CA-1 started task under the STDATA segment information of the general resource profile.
- e). Go back to Administrator main menu, select 3;1 (Security Server Reports – User Profile) and press ENTER .
- f) Tab down to User ID and enter the User ID found in Step d) above and hit enter.
- g). Page down till the Attributes section of the user profile.
- h) Verify that “Protected = Yes”.
- i) If “Protected = Yes”, there is no FINDING.
- j). If “Protected = No”, there is a FINDING.
- k) If TMSINIT 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 TMSINIT in the Procname column..
  3. If the TMSINIT 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)
  - 4..If there is an R in the “M” column, there is a FINDING.

**CCI: CCI-000764**



**UNCLASSIFIED**  
z/OS CA-1 for RACF Analysis and Checklist  
*Version 6 Release 7*

**\_\_STIG ID: ZCA1R032**

**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.
- c). Find the general resources profile for the CA 1 started task, usually named TMSINIT.
- d). If the General Resource profile for the CA 1 started task is found as a General under the STARTED class, there is no FINDING. .
- e) If the General Resource profile for the CA 1 started task is not found in the STARTED class, check if it is defined instead in the Started Procedures Table (ICHRIN03) by running DSMON as a batch job or invoking it under TSO.
- f). If the General Resource profile for the CA 1 started task IS found in the Started Procedures Table (ICHRIN03) , there is NO FINDING.
- g) If the General Resource profile for the CA 1 started task is NOT found in the Started Procedures Table (ICHRIN03) either, this is a FINDING.
- h) If TMSINIT is NOT found as a General Resource profile under the STARTED class in d. 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 SDSF in the Procname column..
  - 3. If SDSF is not found either as a General Resource Profile under STARTED class in e. above AND not found in the Started Procedures Table, this is a FINDING.

**CCI: CCI-000764**

**UNCLASSIFIED**  
z/OS CA-1 for RACF Analysis and Checklist  
*Version 6 Release 7*

**\_\_STIG ID: ZCA1R038**

**Default Severity:** Category II

- a) Find out from the users if they have defined their own RACF *classes* for CA 1 resources.
- b) Then verify if either the CA 1 RACF resource classes defined by the installation or the default CA 1 resource classes are active as follows:
  - 1) From the Administrator main menu, select 3;4 (Security Server Reports - General Resource Reports) and press ENTER .
  - 2) Type 1 for General Resource Profile Summary and Tab down to “CLASS: “, And enter either the installation-defined class names for CA 1 resources found in step a. above or the default CA 1 resource class names (CA@CMD or CA@APE)
  - 3). If the CLASS is found, there is no FINDING.
  - 4). If the CLASS is not found, there is a FINDING. .

**CCI:** CCI-000336

**CCI:** CCI-002358

**UNCLASSIFIED**  
z/OS CA-1 for RACF Analysis and Checklist  
Version 6 Release 7

\_\_STIG ID: ZCA1R040

**Default Severity:** Category II

- a) Ensure that all CA 1 parameters meet the following requirements as specified in in the U\_zOS\_STIG\_Addendum. Note: You do not need to reassemble or execute the steps in these sections, just ensure that when CA-1 was installed the following conventions were observd.
- b) Identify the CA-1 started procedure (STC) usually named TMSINIT.
- c) Identify the two-character suffix for the TMOSYSxx member of the dataset referenced in the TMSPARM DD statement of the TMSINIT started procedure JCL (BY DEFAULT THE SUFFIX IS '00').
- d) Identify the current TMSOPTxx member by browsing member TMOSYSxx of the dataset referenced in the TMSPARM DD statement of the TMSINIT started procedure JCL.
- e) Identify the CA-1 PPOPTION dataset currently in use.
- f) Browse member TMSOPTxx in the PPOPTION dataset currently in use.

1. Verify that the following parameters are set as follows:

BATCH	YES	(applicable only to CA-1 Version 11.5 or below)
CATSEC	NO	(applicable only to CA-1 Versions 5.3 to 11.5 (inclusive))
CMD	YES	
CREATE	UPDATE	
DSNB	YES	
FUNC	YES	
OCEOV	NO	

***NOTE – This requires the RACF System-wide TAPEDSN to be active.***

PMASK	Do not specify or change	
PSWD	YES	
SCRTCH	NO	
SECWTO	YES	(applicable only to CA-1 Version 5.2 and above)
UNDEF	FAIL	
UX0AUPD	NO	(applicable only to CA-1 Version 5.3 and above)
YSVC	YES	

***The systems programmer/IAO is responsible to ensure that the CA-1 external security options are specified in accordance with the above requirements.***

**UNCLASSIFIED**  
z/OS CA-1 for RACF Analysis and Checklist  
*Version 6 Release 7*

**UNCLASSIFIED**  
z/OS CA-1 for RACF Analysis and Checklist  
*Version 6 Release 7*

- g) If the above settings are as specified above, there is NO FINDING.
- h) If the above settings are NOT specified as above, this is a FINDING.

**CCI:** CCI-000035