Are Your Auditors and NIST Security Configuration Controls Driving You Crazy? Configuration Manager Implementation

Session 16910

Monday, March 2, 2015: 11:15 AM - 12:15 PM

Brian Marshall(Vanguard Integrity Professionals)
Tim Bougeault(US Bank)

#SHAREorg

SHARE in Seattle 2015

Agenda

- Introduction
- Audit Requirements
- DISA STIGs and NIST
- VCM Usage at US Bank
- Systems Programmer Point of View
- Install and Configuration
- Using VCM

usbancorp.

2014 3rd Quarter Stats:

- Ranking U.S. Bank is 5th largest
- U.S. commercial bank
- Period-end assets $391 billion
- Period-end deposits $273 billion
- Period-end loans $246 billion
- Customers 17.9 million
- Bank branches 3,177
- ATMs 5,026

Hardware Configuration

- 6 Sysplexes Running z/OS V2.1
- 3 Z196's, 1 Z13, and
- 3 ZEC12's
- 27 lpars, 20 of them are RACF and 7 are ACF2

RACF DB Stats

- Each RACF DB is 2K Cyls
- 83,713 USER profiles
- 29,794 DATASET profiles
- 35,406 GENERAL RESOURCE profile
- 6,845,719 USER-GROUP CONNECT profile

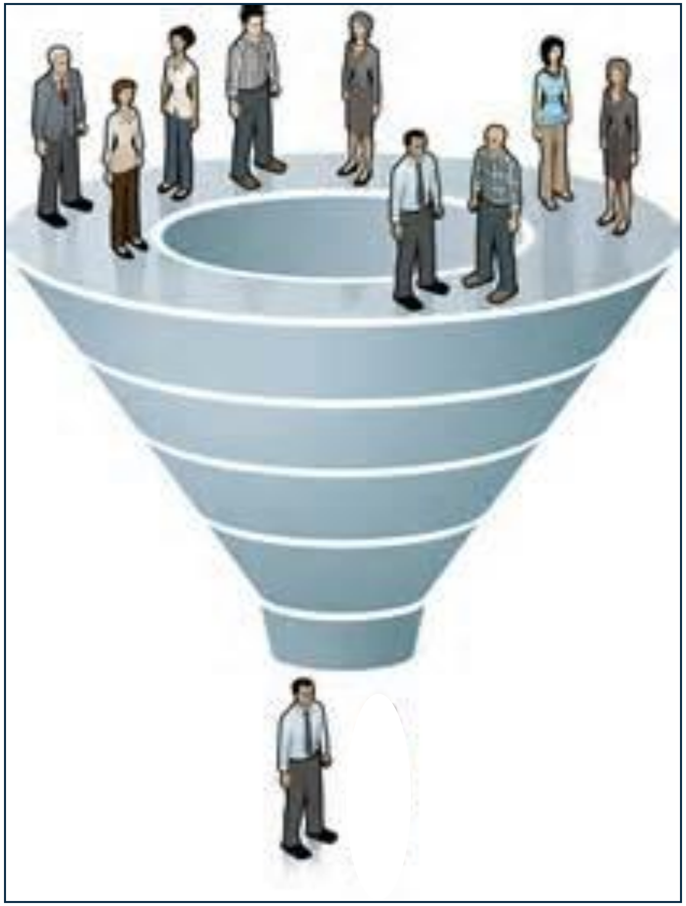
Why VCM for US Bank?

- Multiple Audits from different groups - internal & external
- Many auditors with different knowledge/skill sets
- Goal: Produce one report for distribution to each auditing group

The reports from VCM help us show compliance for internal and external audits.
Sox, PCI, OCC Requirements, □□□□□□□□

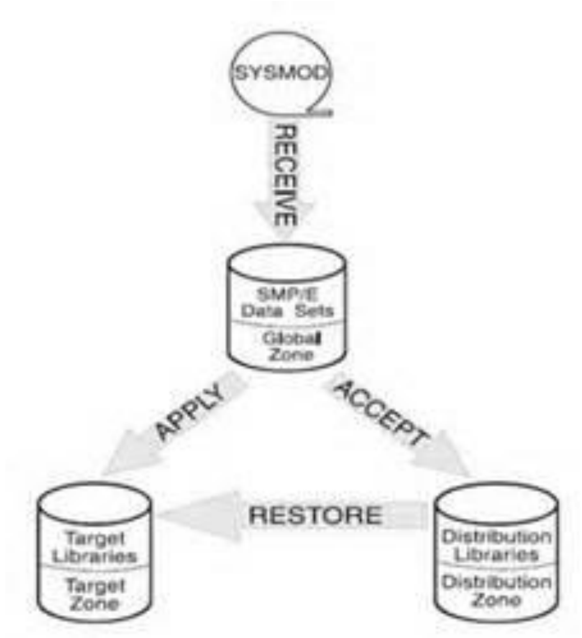
VCM Helps Reduce Time Impacts to Staff

Before VCM, information for an audit had to be requested from several IT staff members.



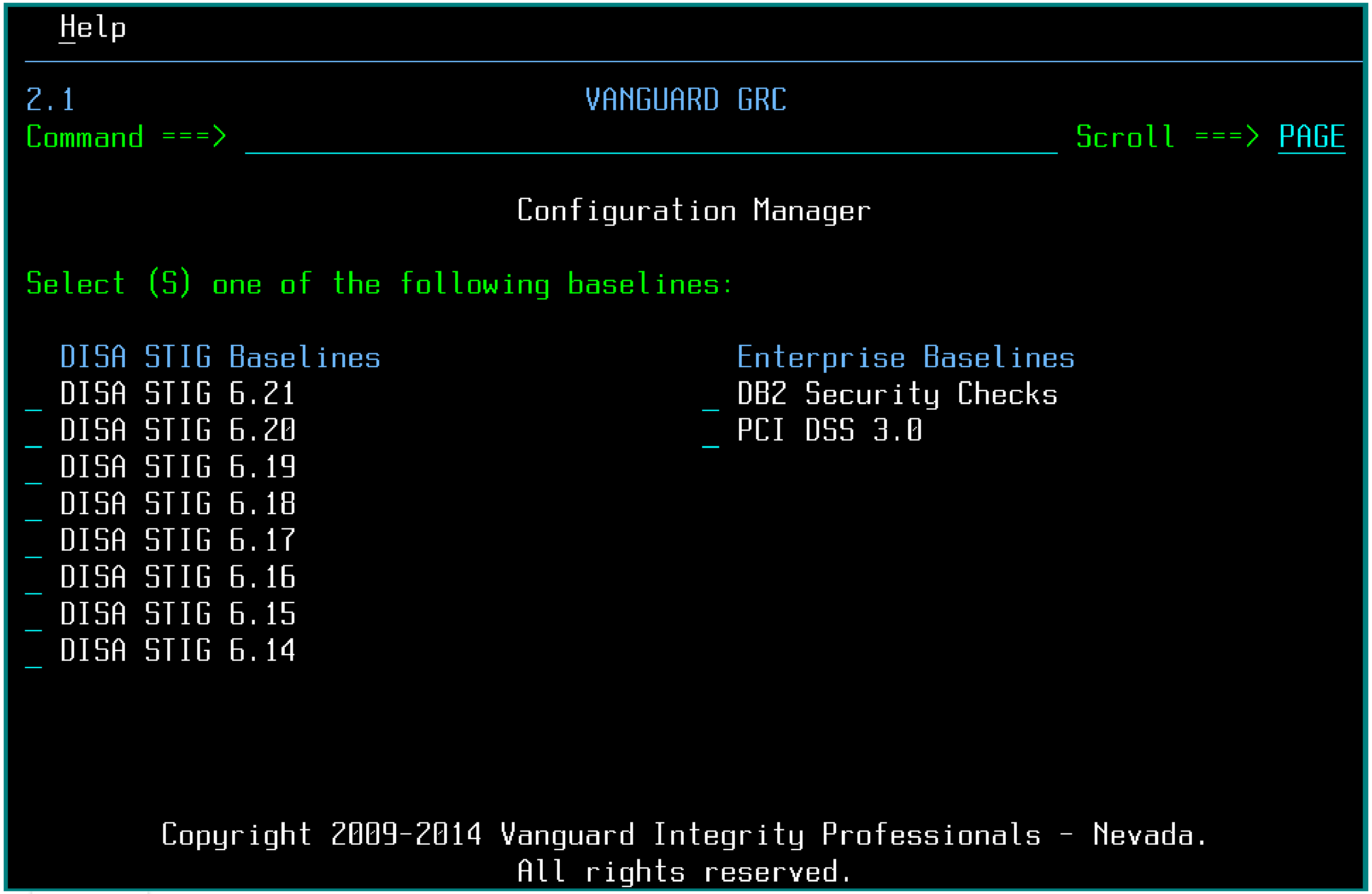
With VCM, audit information requests are quickly handled by one person.

VCM Install



- At US Bank VCM is smp/e installed as part of our Vanguard product set
- Usage requires a Vanguard product code (datecode).

VCM Opening panel



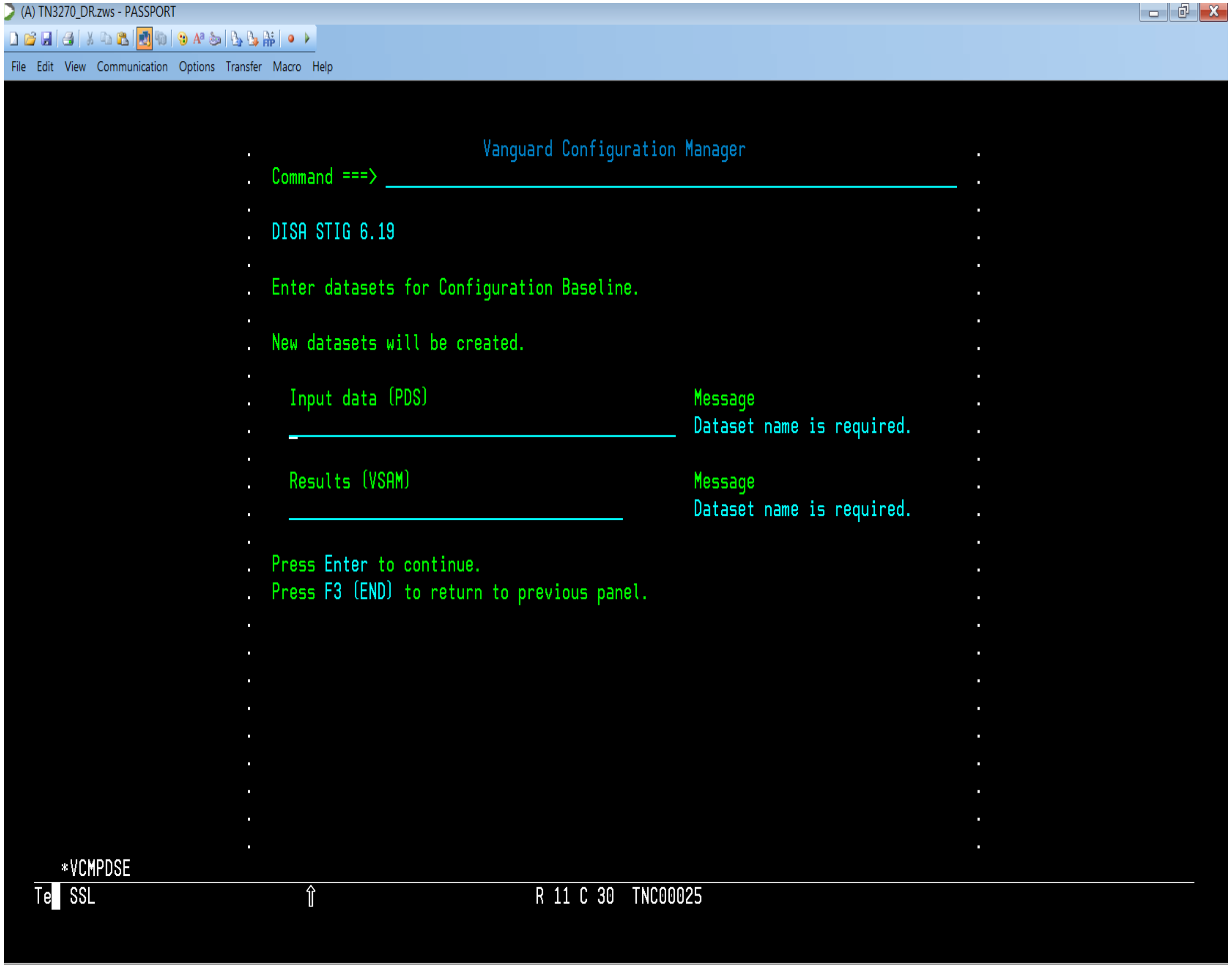
```
  Help
------------------------------------------------------------------------------
2.1                              VANGUARD GRC
Command ===> ________________________________________________ Scroll ===> PAGE

                              Configuration Manager

Select (S) one of the following baselines:

  DISA STIG Baselines                       Enterprise Baselines
_ DISA STIG 6.21                          _ DB2 Security Checks
_ DISA STIG 6.20                          _ PCI DSS 3.0
_ DISA STIG 6.19
_ DISA STIG 6.18
_ DISA STIG 6.17
_ DISA STIG 6.16
_ DISA STIG 6.15
_ DISA STIG 6.14



        Copyright 2009-2014 Vanguard Integrity Professionals - Nevada.
                              All rights reserved.
```

Pick your STIG or DB2 or PCI DSS 3.0

VCM Supported Compliance Checks

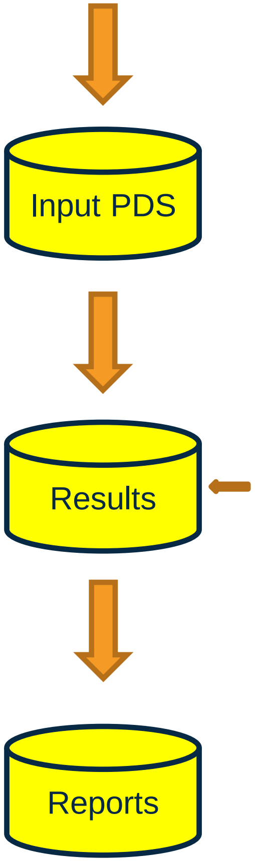
- VCM Currently Supports
  - DISA STIG levels 6.14 to Current 6.21 (completely)
  - Unlike other vendors, Vanguard Configuration Manager supports every single check in the DISA STIGs at the current level and back over 2 years.
  - DB2 Checks – VCM has built in DB2 checks that are posted on the NIST NVD.
  - PCI DSS 3.0 – VCM supports the checking of PCI DSS 3.0 requirements on the mainframe.
- VCM Future Support (Later 2015)
  - Health Checker Exploitation
  - 300+ additional Vanguard Checks

Input and Results Dataset Name Panel


(A) TN3270_DR.zws - PASSPORT
File Edit View Communication Options Transfer Macro Help

```
                     Vanguard Configuration Manager
 Command ===> ________________________________________________

 DISA STIG 6.19

 Enter datasets for Configuration Baseline.

 New datasets will be created.

   Input data (PDS)                          Message
   _________________________________         Dataset name is required.

   Results (VSAM)                            Message
   ____________________________              Dataset name is required.

 Press Enter to continue.
 Press F3 (END) to return to previous panel.

*VCMPDSE
Te SSL                        R 11 C 30  TNC00025
```

VCM Required Data Files



Data Collection PDS ← Data from Interviews

Execute Checks, Writes to Results VSAM File, Size does matter!

MAX_GENERATIONS(x)
Can be encrypted

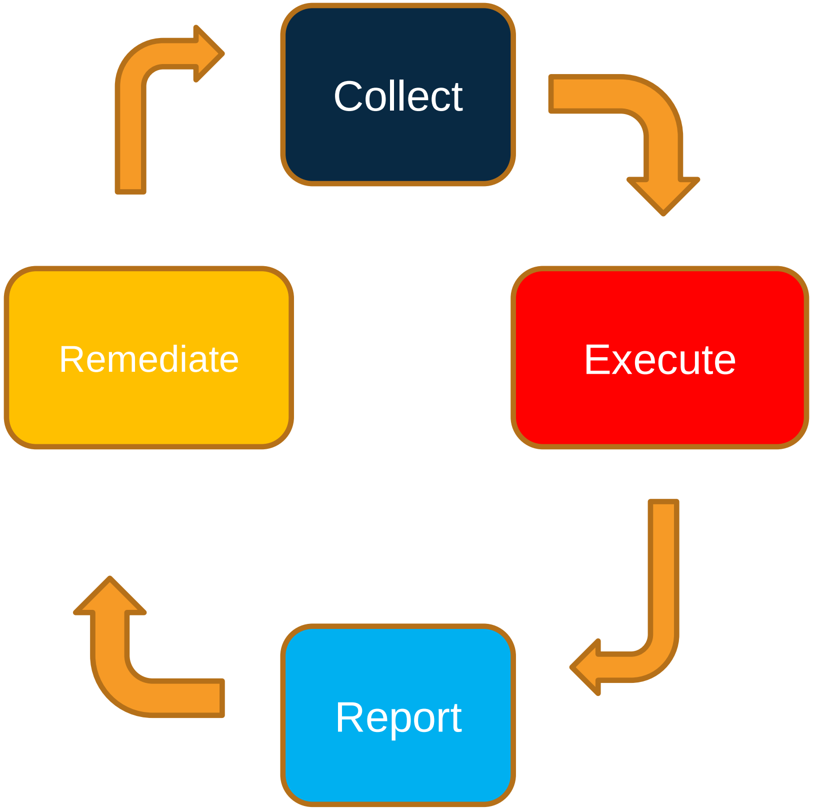
Produce Reports

At US Bank

VCM.INPUT.STIG620	PDS/e 10 cyls
VCM.RESULTS.STIG620	VSAM 1K cyls
VCM.REPORTS.STIG620	PDS 1500 cyls

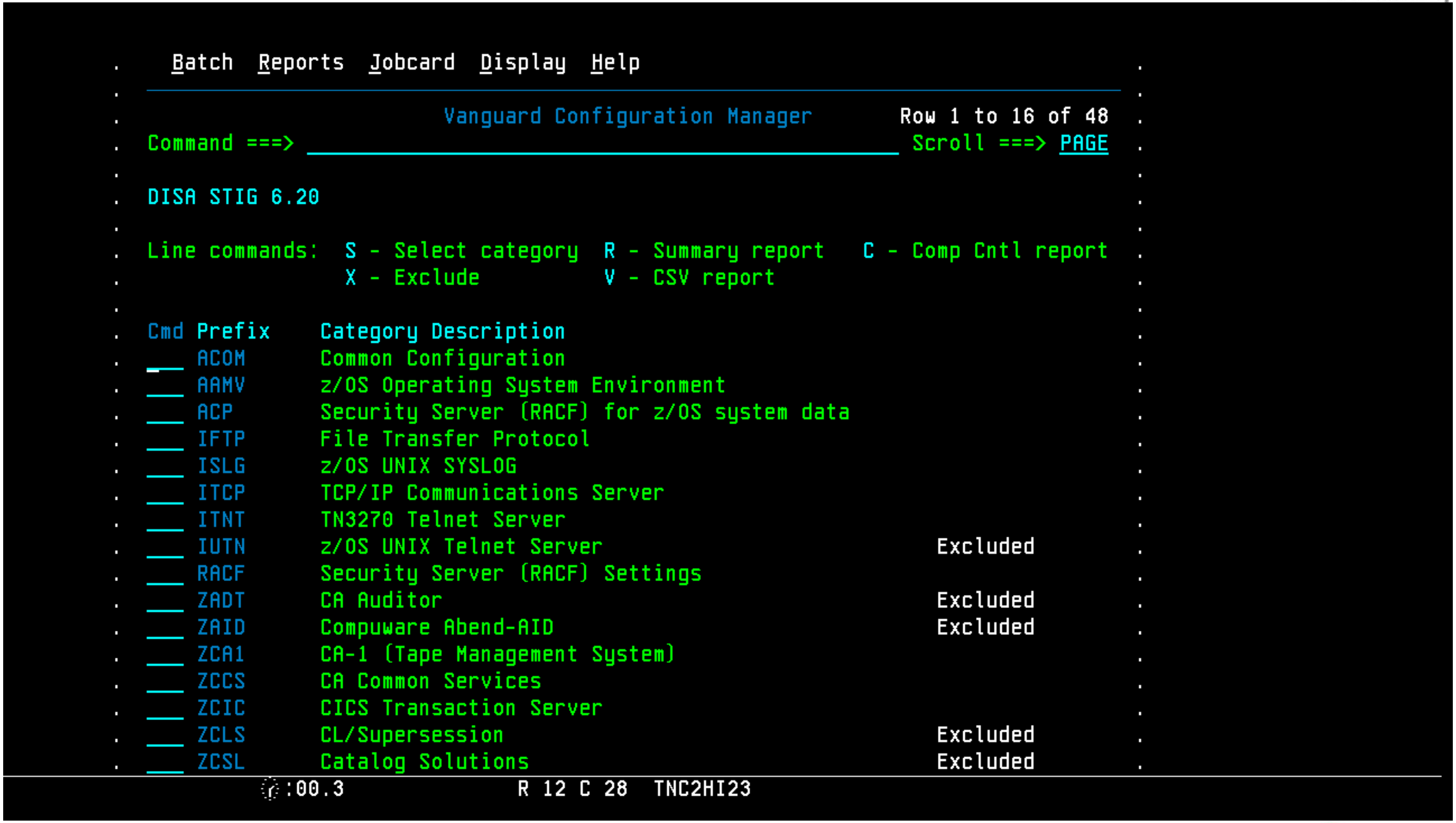
Organize files by STIG level
Each year we pick one STIG level to work with

The Flow



- Common Configuration
- Interview Process
- Execute the checks
- Report and Remediate
- Audit Deliverables
- Repeat

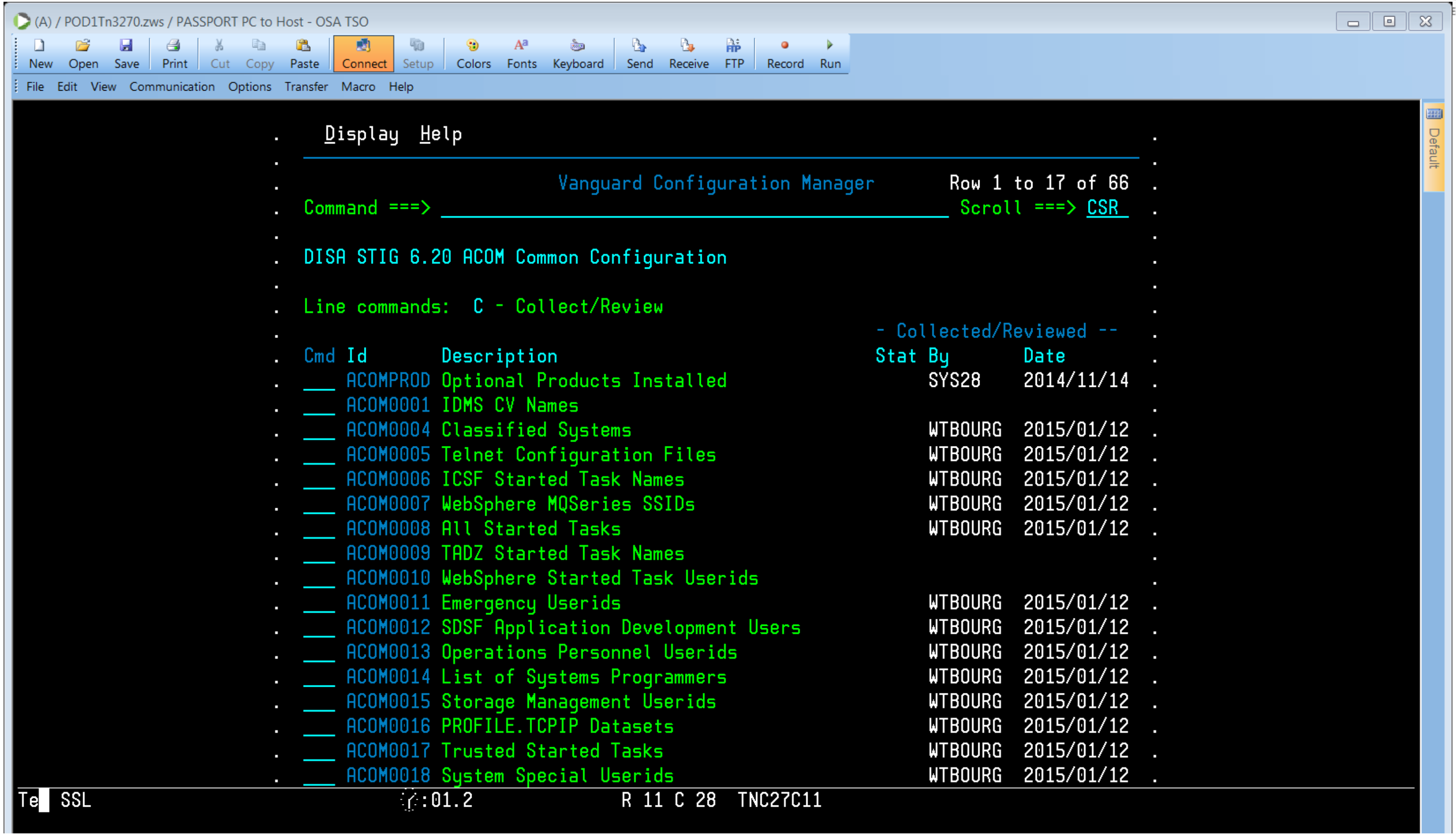
VCM Main Panel



```
   Batch  Reports  Jobcard  Display  Help
 ------------------------------------------------------------------------------
                       Vanguard Configuration Manager       Row 1 to 16 of 48
 Command ===> ________________________________________________ Scroll ===> PAGE

 DISA STIG 6.20

 Line commands:  S - Select category  R - Summary report   C - Comp Cntl report
                 X - Exclude          V - CSV report

 Cmd Prefix    Category Description
 ___ ACOM      Common Configuration
 ___ AAMV      z/OS Operating System Environment
 ___ ACP       Security Server (RACF) for z/OS system data
 ___ IFTP      File Transfer Protocol
 ___ ISLG      z/OS UNIX SYSLOG
 ___ ITCP      TCP/IP Communications Server
 ___ ITNT      TN3270 Telnet Server
 ___ IUTN      z/OS UNIX Telnet Server                            Excluded
 ___ RACF      Security Server (RACF) Settings
 ___ ZADT      CA Auditor                                         Excluded
 ___ ZAID      Compuware Abend-AID                                Excluded
 ___ ZCA1      CA-1 (Tape Management System)
 ___ ZCCS      CA Common Services
 ___ ZCIC      CICS Transaction Server
 ___ ZCLS      CL/Supersession                                    Excluded
 ___ ZCSL      Catalog Solutions                                  Excluded
          :00.3              R 12 C 28   TNC2HI23
```

STIG 6.20 has 48 Categories

Collect

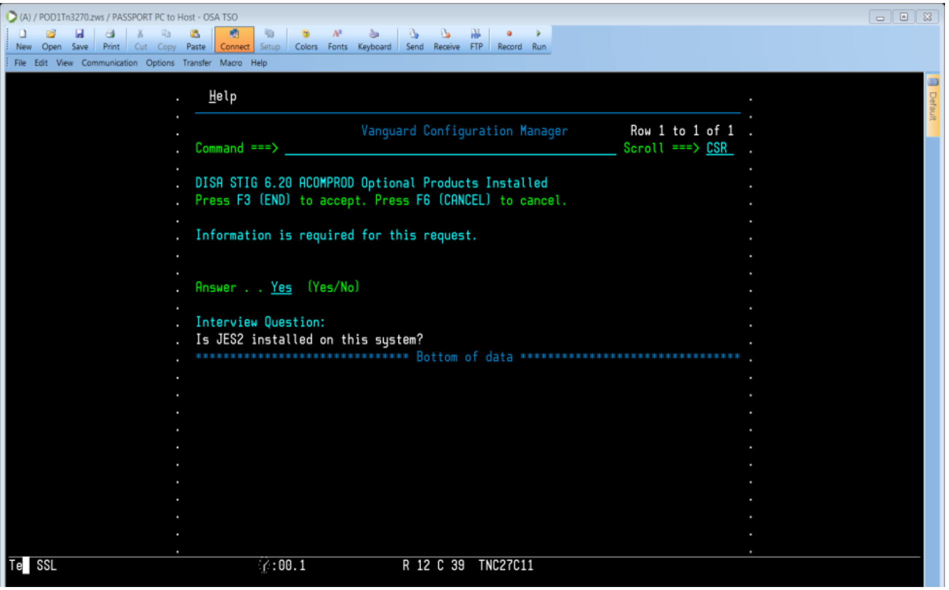


(A) / POD1Tn3270.zws / PASSPORT PC to Host - OSA TSO
New Open Save Print Cut Copy Paste Connect Setup Colors Fonts Keyboard Send Receive FTP Record Run
File Edit View Communication Options Transfer Macro Help
Default

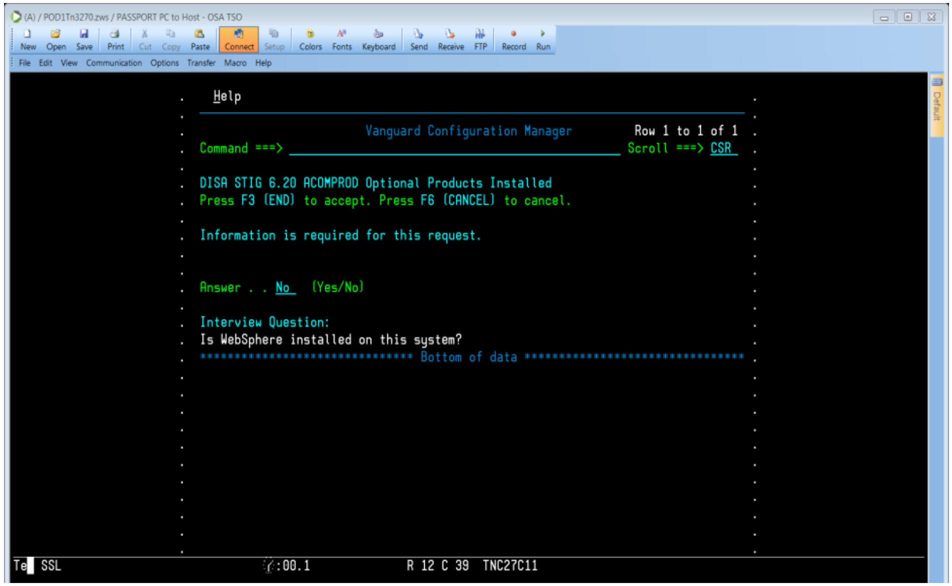
```
  Display  Help
 
                    Vanguard Configuration Manager        Row 1 to 17 of 66
 Command ===> ________________________________________________ Scroll ===> CSR
 
 DISA STIG 6.20 ACOM Common Configuration
 
 Line commands:  C - Collect/Review
                                                     - Collected/Reviewed --
 Cmd Id        Description                           Stat By       Date
 ___ ACOMPROD Optional Products Installed                 SYS28    2014/11/14
 ___ ACOM0001 IDMS CV Names
 ___ ACOM0004 Classified Systems                          WTBOURG  2015/01/12
 ___ ACOM0005 Telnet Configuration Files                  WTBOURG  2015/01/12
 ___ ACOM0006 ICSF Started Task Names                     WTBOURG  2015/01/12
 ___ ACOM0007 WebSphere MQSeries SSIDs                    WTBOURG  2015/01/12
 ___ ACOM0008 All Started Tasks                           WTBOURG  2015/01/12
 ___ ACOM0009 TADZ Started Task Names
 ___ ACOM0010 WebSphere Started Task Userids
 ___ ACOM0011 Emergency Userids                           WTBOURG  2015/01/12
 ___ ACOM0012 SDSF Application Development Users          WTBOURG  2015/01/12
 ___ ACOM0013 Operations Personnel Userids                WTBOURG  2015/01/12
 ___ ACOM0014 List of Systems Programmers                 WTBOURG  2015/01/12
 ___ ACOM0015 Storage Management Userids                  WTBOURG  2015/01/12
 ___ ACOM0016 PROFILE.TCPIP Datasets                      WTBOURG  2015/01/12
 ___ ACOM0017 Trusted Started Tasks                       WTBOURG  2015/01/12
 ___ ACOM0018 System Special Userids                      WTBOURG  2015/01/12
Te  SSL                  :01.2            R 11 C 28  TNC27C11
```

Common Config expedites the interview process by providing a central data repository from which the checks can share information.

Common Configuration


(A) / POD1Tn3270.zws / PASSPORT PC to Host - OSA TSO
New Open Save Print Cut Copy Paste Connect Setup Colors Fonts Keyboard Send Receive FTP Record Run
File Edit View Communication Options Transfer Macro Help

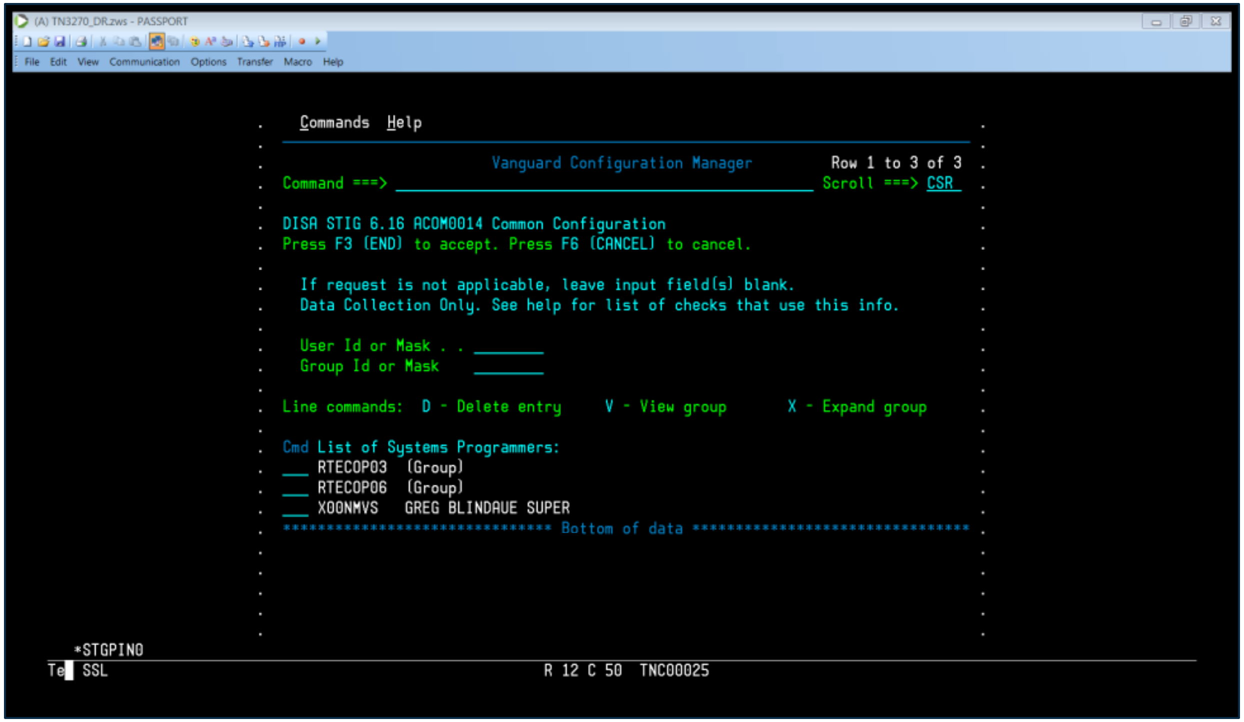
```
Help
                 Vanguard Configuration Manager          Row 1 to 1 of 1
Command ===> ________________________________________________ Scroll ===> CSR

DISA STIG 6.20 ACOMPROD Optional Products Installed
Press F3 (END) to accept. Press F6 (CANCEL) to cancel.

Information is required for this request.


Answer . . Yes  (Yes/No)

Interview Question:
Is JES2 installed on this system?
******************************* Bottom of data ********************************

Te SSL                          :00.1          R 12 C 39  TNC27C11
```


(A) / POD1Tn3270.zws / PASSPORT PC to Host - OSA TSO
New Open Save Print Cut Copy Paste Connect Setup Colors Fonts Keyboard Send Receive FTP Record Run
File Edit View Communication Options Transfer Macro Help

```
Help
                 Vanguard Configuration Manager          Row 1 to 1 of 1
Command ===> ________________________________________________ Scroll ===> CSR

DISA STIG 6.20 ACOMPROD Optional Products Installed
Press F3 (END) to accept. Press F6 (CANCEL) to cancel.

Information is required for this request.


Answer . . No   (Yes/No)

Interview Question:
Is WebSphere installed on this system?
******************************* Bottom of data ********************************

Te SSL                          :00.1          R 12 C 39  TNC27C11
```

ACOMPROD Interview questions

Common Configuration



(A) TN3270_DR.zws - PASSPORT
File Edit View Communication Options Transfer Macro Help

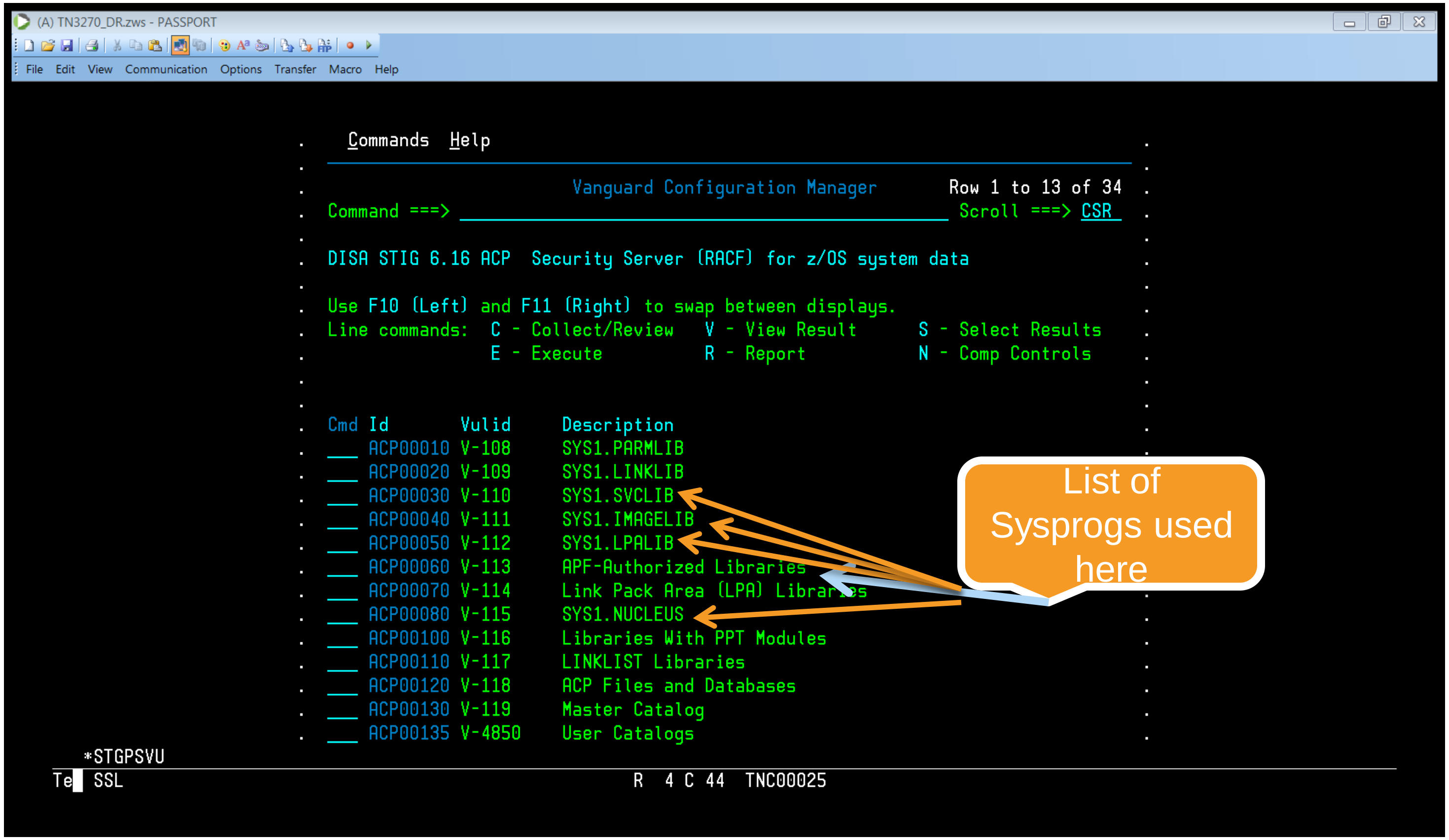
```
  Commands  Help
------------------------------------------------------------------------------
                         Vanguard Configuration Manager         Row 1 to 3 of 3
Command ===> ________________________________________________ Scroll ===> CSR

DISA STIG 6.16 ACOM0014 Common Configuration
Press F3 (END) to accept. Press F6 (CANCEL) to cancel.

  If request is not applicable, leave input field(s) blank.
  Data Collection Only. See help for list of checks that use this info.

  User Id or Mask . .  ________
  Group Id or Mask     ________

Line commands:  D - Delete entry     V - View group      X - Expand group

Cmd List of Systems Programmers:
___ RTECOP03  (Group)
___ RTECOP06  (Group)
___ X00NMVS   GREG BLINDAUE SUPER
******************************* Bottom of data ********************************

   *STGPINO
Te  SSL                                             R 12 C 50  TNC00025
```

ACOM0014 List of System Programmers

List of Systems Programmer userids Used in: over 100 checks throughout Configuration Manager

The list of sysprogs can by modified for each check that references ACOM0014

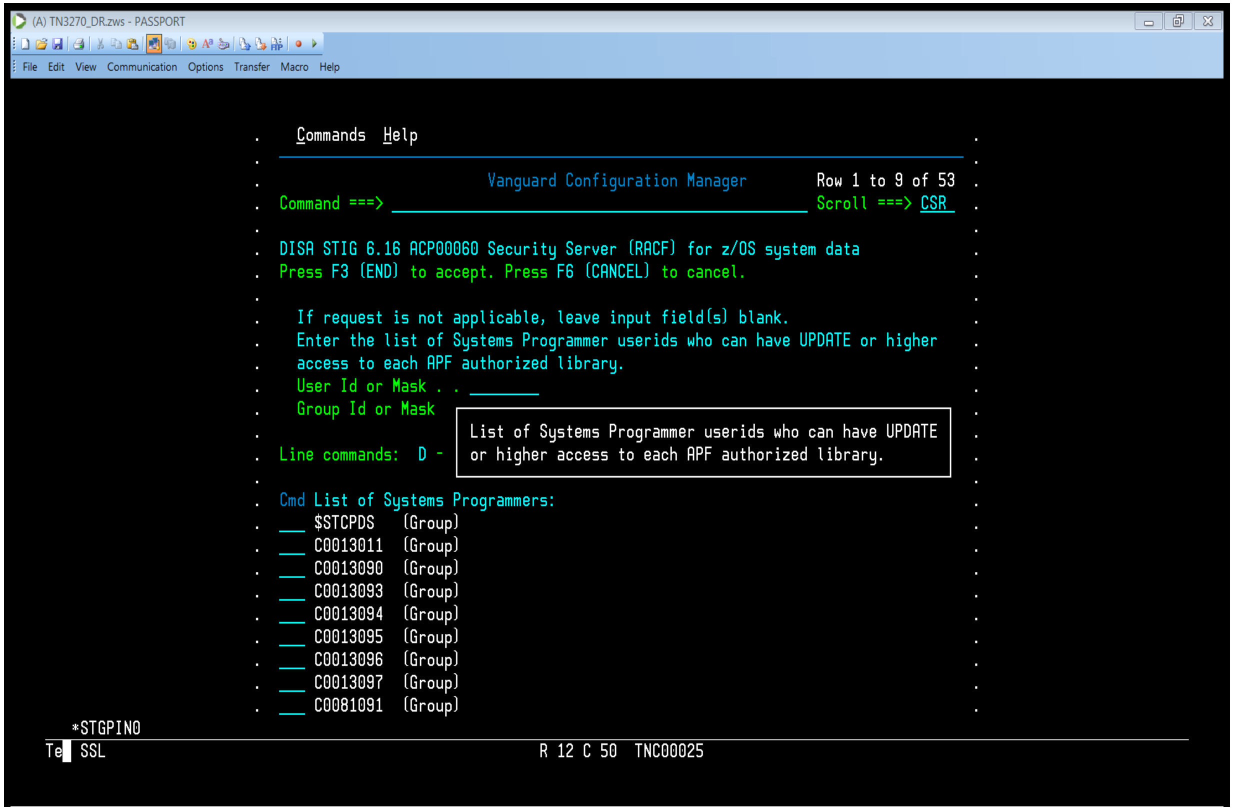
DISA STIG 6.16 ACP Security Server (RACF) for z/OS System Data


(A) TN3270_DR.zws - PASSPORT
File Edit View Communication Options Transfer Macro Help

```
 .   Commands  Help                                                       .
 .  ------------------------------------------------------------------    .
 .                    Vanguard Configuration Manager       Row 1 to 13 of 34 .
 .  Command ===> ________________________________________________ Scroll ===> CSR  .
 .                                                                        .
 .  DISA STIG 6.16 ACP  Security Server (RACF) for z/OS system data       .
 .                                                                        .
 .  Use F10 (Left) and F11 (Right) to swap between displays.              .
 .  Line commands:  C - Collect/Review    V - View Result     S - Select Results .
 .                  E - Execute           R - Report          N - Comp Controls  .
 .                                                                        .
 .                                                                        .
 .  Cmd Id        Vulid     Description                                   .
 .  ___ ACP00010 V-108     SYS1.PARMLIB                                   .
 .  ___ ACP00020 V-109     SYS1.LINKLIB                                   .
 .  ___ ACP00030 V-110     SYS1.SVCLIB                                    .
 .  ___ ACP00040 V-111     SYS1.IMAGELIB                                  .
 .  ___ ACP00050 V-112     SYS1.LPALIB                                    .
 .  ___ ACP00060 V-113     APF-Authorized Libraries                       .
 .  ___ ACP00070 V-114     Link Pack Area (LPA) Libraries                 .
 .  ___ ACP00080 V-115     SYS1.NUCLEUS                                   .
 .  ___ ACP00100 V-116     Libraries With PPT Modules                     .
 .  ___ ACP00110 V-117     LINKLIST Libraries                             .
 .  ___ ACP00120 V-118     ACP Files and Databases                        .
 .  ___ ACP00130 V-119     Master Catalog                                 .
 .  ___ ACP00135 V-4850    User Catalogs                                  .
     *STGPSVU
 Te  SSL                                       R  4 C 44   TNC00025
```

List of Sysprogs used here

ACP00060 V-113 APF-Authorized Libraries

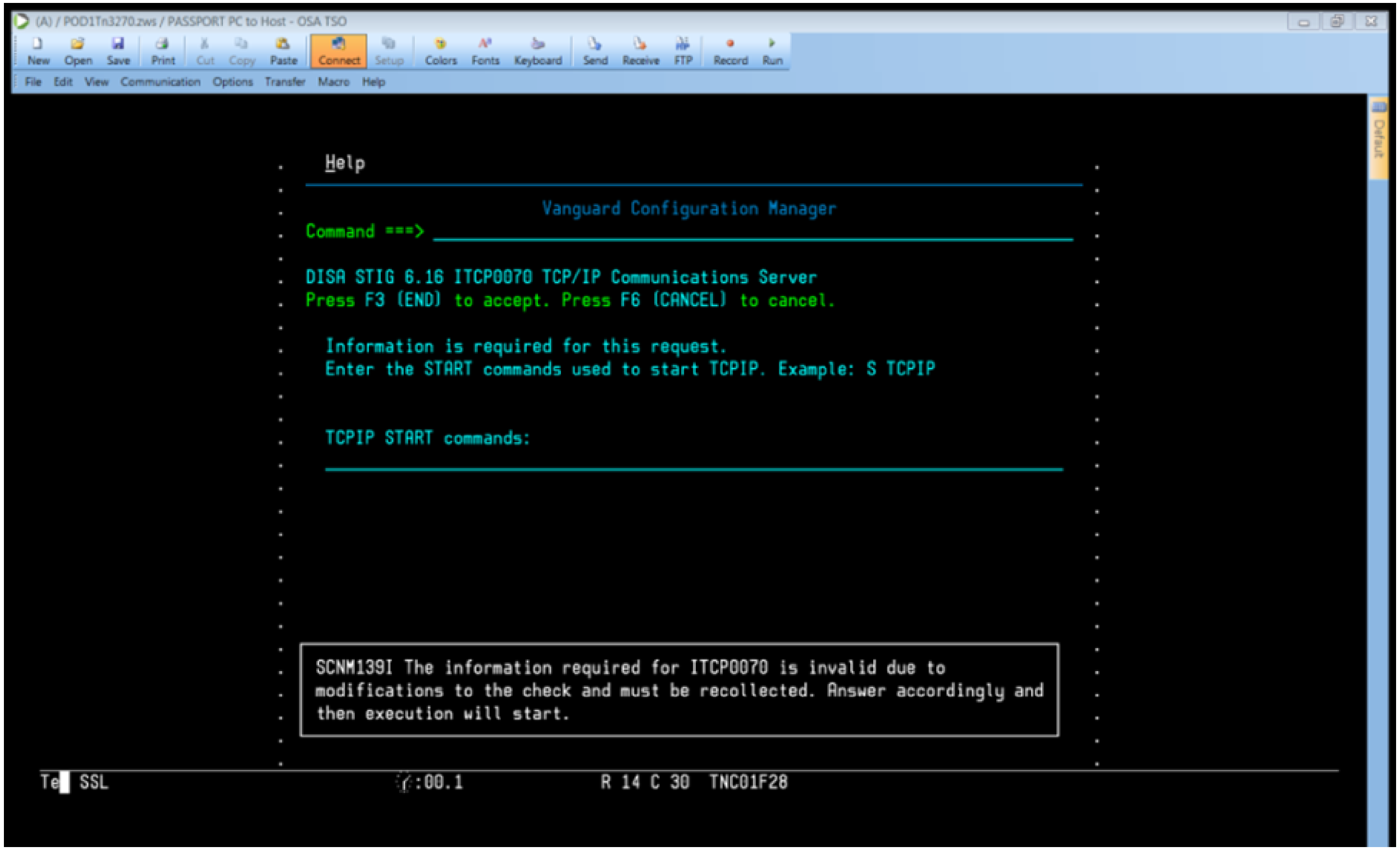


```
  Commands  Help
 ------------------------------------------------------------------------------
                        Vanguard Configuration Manager        Row 1 to 9 of 53
 Command ===> ________________________________________________ Scroll ===> CSR

 DISA STIG 6.16 ACP00060 Security Server (RACF) for z/OS system data
 Press F3 (END) to accept. Press F6 (CANCEL) to cancel.

   If request is not applicable, leave input field(s) blank.
   Enter the list of Systems Programmer userids who can have UPDATE or higher
   access to each APF authorized library.
   User Id or Mask . . ________
   Group Id or Mask   +---------------------------------------------------------+
                      | List of Systems Programmer userids who can have UPDATE  |
 Line commands:  D -  | or higher access to each APF authorized library.        |
                      +---------------------------------------------------------+
 Cmd List of Systems Programmers:
 ___ $STCPDS   (Group)
 ___ C0013011  (Group)
 ___ C0013090  (Group)
 ___ C0013093  (Group)
 ___ C0013094  (Group)
 ___ C0013095  (Group)
 ___ C0013096  (Group)
 ___ C0013097  (Group)
 ___ C0081091  (Group)
   *STGPINO
Te  SSL                                           R 12 C 50   TNC00025
```

Not all APF LIBs are administered by the original list of sysprogs as defined in ACOM0014, for specific checks you may need to add to the sysprog List

Collection - Recollect

VCM will let you know if data for a specific check needs to be recollected.

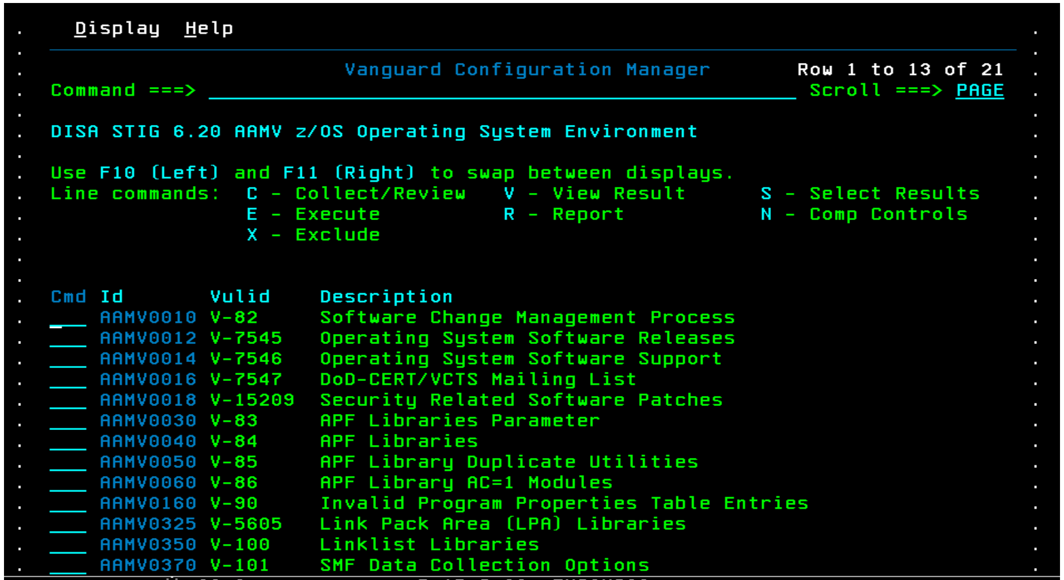


```
 Help
 ----------------------------------------------------------------------------
                        Vanguard Configuration Manager
Command ===> _______________________________________________________________

DISA STIG 6.16 ITCP0070 TCP/IP Communications Server
Press F3 (END) to accept. Press F6 (CANCEL) to cancel.

  Information is required for this request.
  Enter the START commands used to start TCPIP. Example: S TCPIP


  TCPIP START commands:

  ________________________________________________________________________








 SCNM139I The information required for ITCP0070 is invalid due to
 modifications to the check and must be recollected. Answer accordingly and
 then execution will start.

Te  SSL                          :00.1              R 14 C 30   TNC01F28
```

Collection Hints

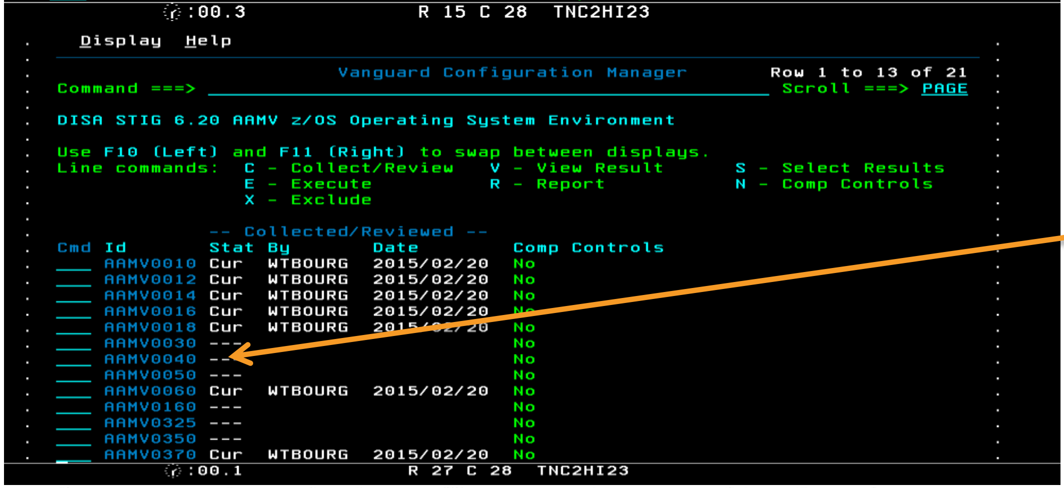
- Must have management support
- Collection questions can be printed via batch report
- You can set when data must be recollected
- DAYS_VALID specifies the number of days the collected data is valid before requiring a review. The range is 0 - 365, inclusive
- A value of 0 specifies that the collected data never expires, the default value is 30

Auto Data Collection



```
   Display  Help
 ------------------------------------------------------------------------------
                     Vanguard Configuration Manager         Row 1 to 13 of 21
 Command ===> ________________________________________________ Scroll ===> PAGE

 DISA STIG 6.20 AAMV z/OS Operating System Environment

 Use F10 (Left) and F11 (Right) to swap between displays.
 Line commands:   C - Collect/Review    V - View Result      S - Select Results
                  E - Execute           R - Report           N - Comp Controls
                  X - Exclude


 Cmd Id         Vulid     Description
 ___ AAMV0010 V-82      Software Change Management Process
 ___ AAMV0012 V-7545    Operating System Software Releases
 ___ AAMV0014 V-7546    Operating System Software Support
 ___ AAMV0016 V-7547    DoD-CERT/VCTS Mailing List
 ___ AAMV0018 V-15209   Security Related Software Patches
 ___ AAMV0030 V-83      APF Libraries Parameter
 ___ AAMV0040 V-84      APF Libraries
 ___ AAMV0050 V-85      APF Library Duplicate Utilities
 ___ AAMV0060 V-86      APF Library AC=1 Modules
 ___ AAMV0160 V-90      Invalid Program Properties Table Entries
 ___ AAMV0325 V-5605    Link Pack Area (LPA) Libraries
 ___ AAMV0350 V-100     Linklist Libraries
 ___ AAMV0370 V-101     SMF Data Collection Options
           :00.3                R 15 C 28   TNC2HI23
```

Not all checks require data collection, VCM will automatically gather the required data when the check is executed.

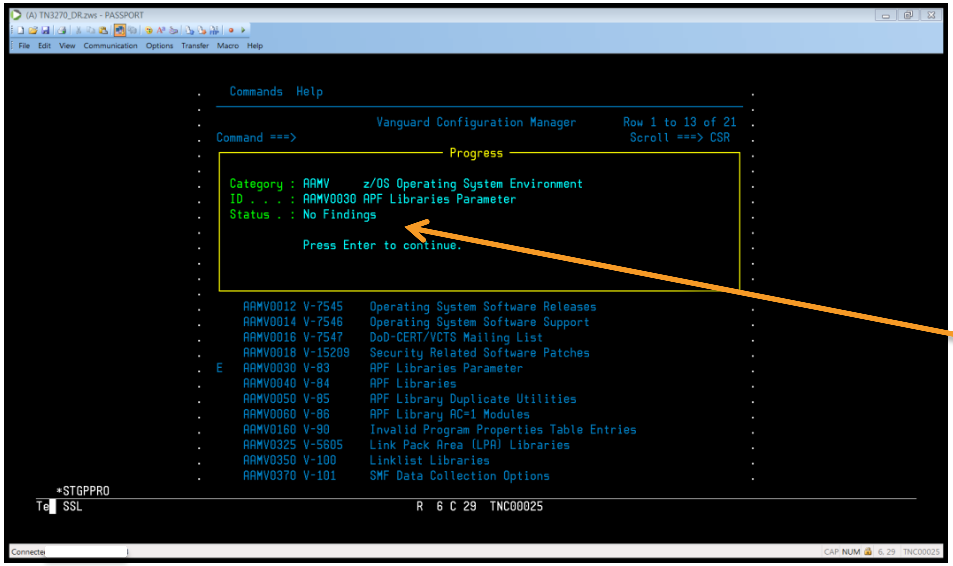


```
   Display  Help
 ------------------------------------------------------------------------------
                     Vanguard Configuration Manager         Row 1 to 13 of 21
 Command ===> ________________________________________________ Scroll ===> PAGE

 DISA STIG 6.20 AAMV z/OS Operating System Environment

 Use F10 (Left) and F11 (Right) to swap between displays.
 Line commands:   C - Collect/Review    V - View Result      S - Select Results
                  E - Execute           R - Report           N - Comp Controls
                  X - Exclude

                 -- Collected/Reviewed --
 Cmd Id          Stat By        Date        Comp Controls
 ___ AAMV0010 Cur  WTBOURG   2015/02/20  No
 ___ AAMV0012 Cur  WTBOURG   2015/02/20  No
 ___ AAMV0014 Cur  WTBOURG   2015/02/20  No
 ___ AAMV0016 Cur  WTBOURG   2015/02/20  No
 ___ AAMV0018 Cur  WTBOURG   2015/02/20  No
 ___ AAMV0030 ---                        No
 ___ AAMV0040 ---                        No
 ___ AAMV0050 ---                        No
 ___ AAMV0060 Cur  WTBOURG   2015/02/20  No
 ___ AAMV0160 ---                        No
 ___ AAMV0325 ---                        No
 ___ AAMV0350 ---                        No
 ___ AAMV0370 Cur  WTBOURG   2015/02/20  No
           :00.1                R 27 C 28   TNC2HI23
```

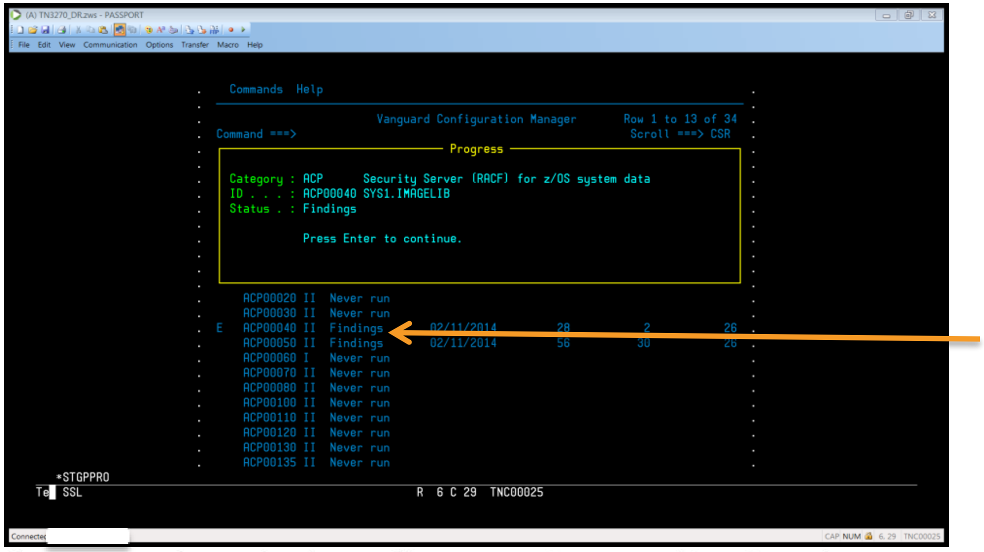
Collection in not required for checks that have --- in the Stat column.

PF11 takes you to the second screen.

Interactive Check Execution


(A) TN3270_DR.zws - PASSPORT
File Edit View Communication Options Transfer Macro Help
Connecte
CAP NUM 6, 29 TNC00025

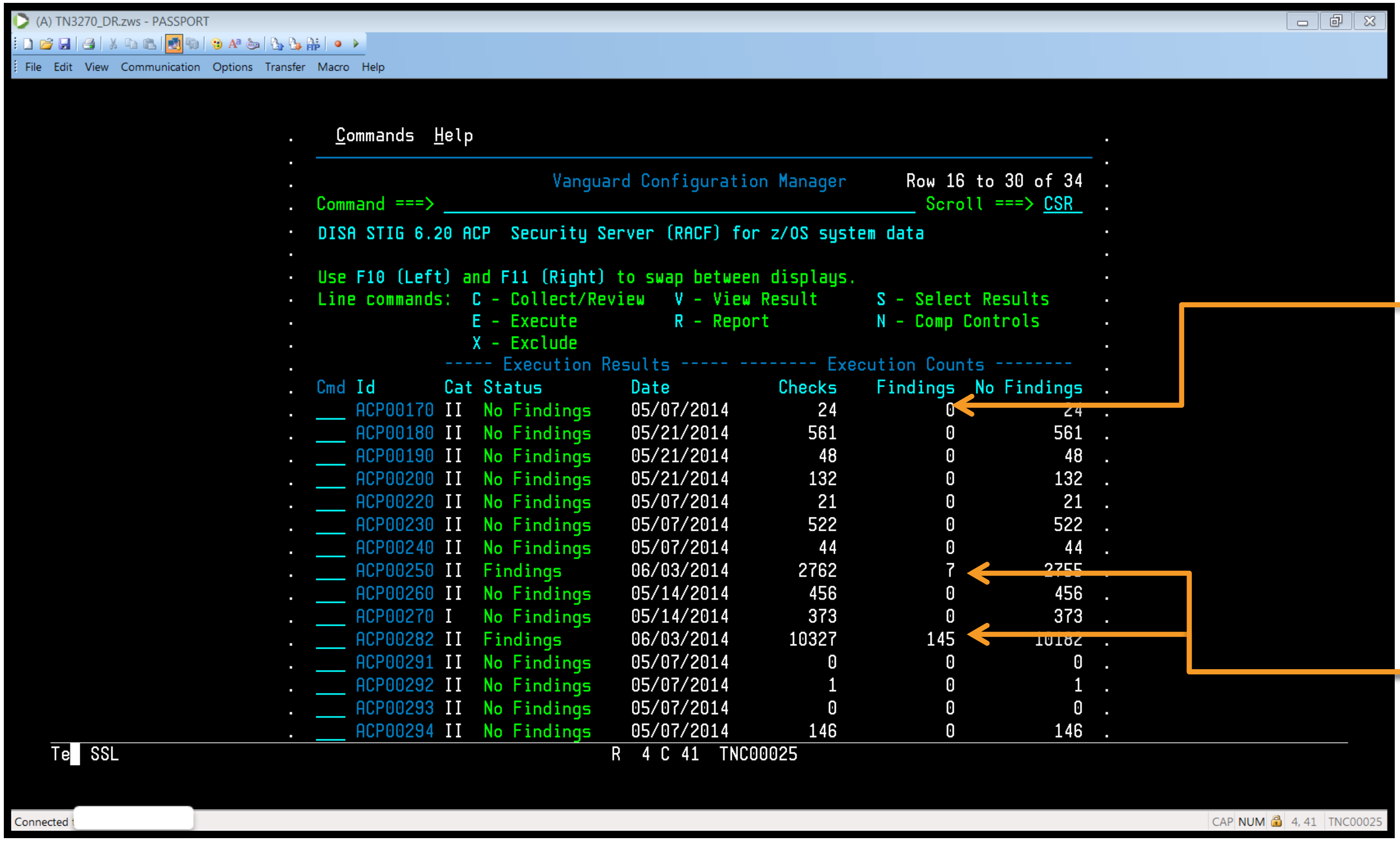
```
 Commands  Help
 
                      Vanguard Configuration Manager      Row 1 to 13 of 21
Command ===>                                                 Scroll ===> CSR
                                     Progress
 Category : AAMV     z/OS Operating System Environment
 ID . . . : AAMV0030 APF Libraries Parameter
 Status . : No Findings

            Press Enter to continue.

     AAMV0012 V-7545    Operating System Software Releases
     AAMV0014 V-7546    Operating System Software Support
     AAMV0016 V-7547    DoD-CERT/VCTS Mailing List
     AAMV0018 V-15209   Security Related Software Patches
 E   AAMV0030 V-83      APF Libraries Parameter
     AAMV0040 V-84      APF Libraries
     AAMV0050 V-85      APF Library Duplicate Utilities
     AAMV0060 V-86      APF Library AC=1 Modules
     AAMV0160 V-90      Invalid Program Properties Table Entries
     AAMV0325 V-5605    Link Pack Area (LPA) Libraries
     AAMV0350 V-100     Linklist Libraries
     AAMV0370 V-101     SMF Data Collection Options
 *STGPPRO
Te  SSL                                  R  6 C 29  TNC00025
```


(A) TN3270_DR.zws - PASSPORT
File Edit View Communication Options Transfer Macro Help
Connected
CAP NUM 6, 29 TNC00025

```
 Commands  Help
 
                      Vanguard Configuration Manager      Row 1 to 13 of 34
Command ===>                                                 Scroll ===> CSR
                                     Progress
 Category : ACP      Security Server (RACF) for z/OS system data
 ID . . . : ACP00040 SYS1.IMAGELIB
 Status . : Findings

            Press Enter to continue.

     ACP00020 II  Never run
     ACP00030 II  Never run
 E   ACP00040 II  Findings     02/11/2014      28         2         26
     ACP00050 II  Findings     02/11/2014      56        30         26
     ACP00060 I   Never run
     ACP00070 II  Never run
     ACP00080 II  Never run
     ACP00100 II  Never run
     ACP00110 II  Never run
     ACP00120 II  Never run
     ACP00130 II  Never run
     ACP00135 II  Never run
 *STGPPRO
Te  SSL                                  R  6 C 29  TNC00025
```

E to execute check

Execution Counts

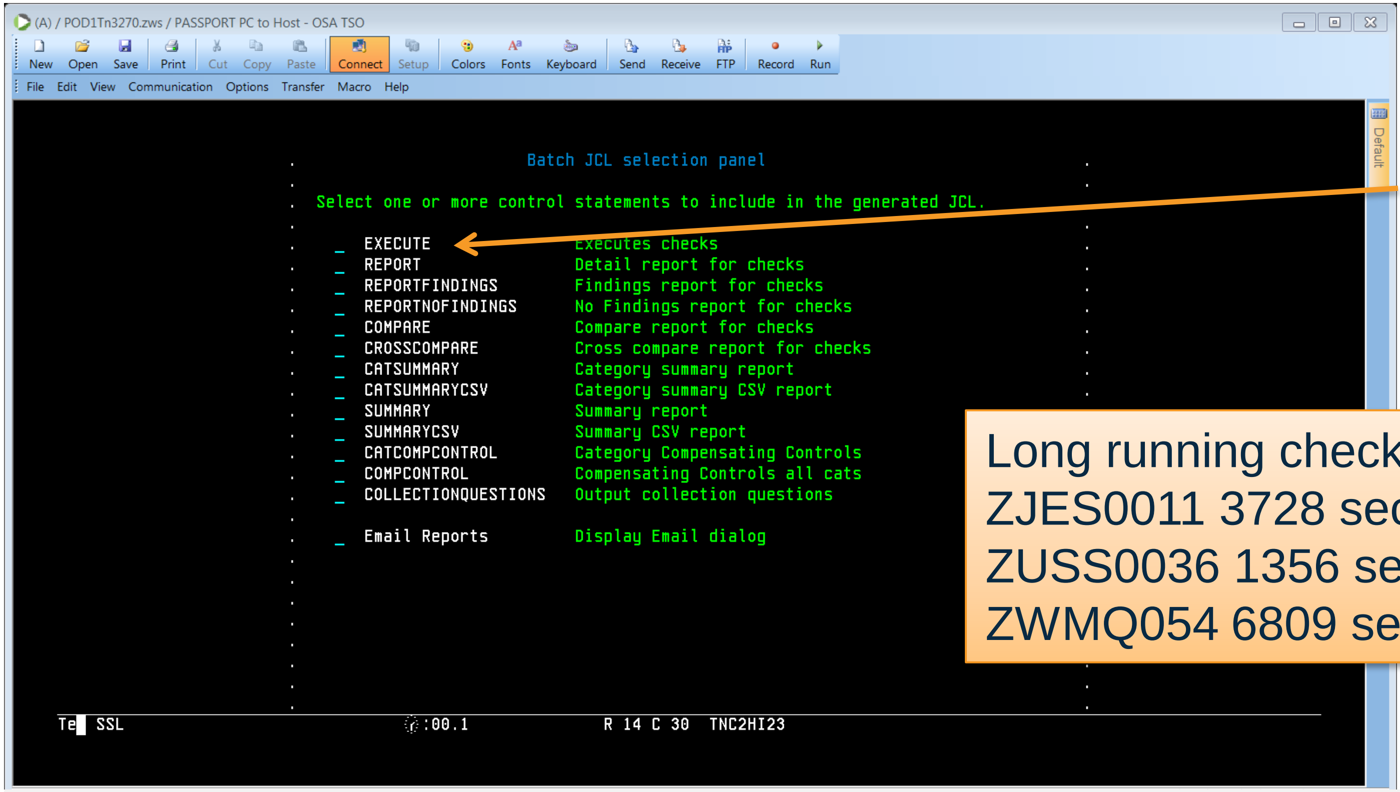

(A) TN3270_DR.zws - PASSPORT
File Edit View Communication Options Transfer Macro Help
Connected
CAP NUM 4, 41 TNC00025

```
   Commands  Help
 ------------------------------------------------------------------------------
                     Vanguard Configuration Manager       Row 16 to 30 of 34
 Command ===> ___________________________________________  Scroll ===> CSR
 DISA STIG 6.20 ACP  Security Server (RACF) for z/OS system data

 Use F10 (Left) and F11 (Right) to swap between displays.
 Line commands:  C - Collect/Review    V - View Result      S - Select Results
                 E - Execute           R - Report           N - Comp Controls
                 X - Exclude
              ----- Execution Results -----  -------- Execution Counts --------
 Cmd Id         Cat Status           Date             Checks   Findings No Findings
 ___ ACP00170  II  No Findings      05/07/2014           24          0          24
 ___ ACP00180  II  No Findings      05/21/2014          561          0         561
 ___ ACP00190  II  No Findings      05/21/2014           48          0          48
 ___ ACP00200  II  No Findings      05/21/2014          132          0         132
 ___ ACP00220  II  No Findings      05/07/2014           21          0          21
 ___ ACP00230  II  No Findings      05/07/2014          522          0         522
 ___ ACP00240  II  No Findings      05/07/2014           44          0          44
 ___ ACP00250  II  Findings         06/03/2014         2762          7        2755
 ___ ACP00260  II  No Findings      05/14/2014          456          0         456
 ___ ACP00270  I   No Findings      05/14/2014          373          0         373
 ___ ACP00282  II  Findings         06/03/2014        10327        145       10182
 ___ ACP00291  II  No Findings      05/07/2014            0          0           0
 ___ ACP00292  II  No Findings      05/07/2014            1          0           1
 ___ ACP00293  II  No Findings      05/07/2014            0          0           0
 ___ ACP00294  II  No Findings      05/07/2014          146          0         146
Te  SSL                                  R  4 C 41  TNC00025
```

We like zero's

Non-zero's
more
Work to do

Batch Execution



```
                         Batch JCL selection panel

      Select one or more control statements to include in the generated JCL.

        _  EXECUTE               Executes checks
        _  REPORT                Detail report for checks
        _  REPORTFINDINGS        Findings report for checks
        _  REPORTNOFINDINGS      No Findings report for checks
        _  COMPARE               Compare report for checks
        _  CROSSCOMPARE          Cross compare report for checks
        _  CATSUMMARY            Category summary report
        _  CATSUMMARYCSV         Category summary CSV report
        _  SUMMARY               Summary report
        _  SUMMARYCSV            Summary CSV report
        _  CATCOMPCONTROL        Category Compensating Controls
        _  COMPCONTROL           Compensating Controls all cats
        _  COLLECTIONQUESTIONS   Output collection questions

        _  Email Reports         Display Email dialog

Te  SSL              :00.1          R 14 C 30  TNC2HI23
```

Generates JCL

Long running checks at US Bank:
ZJES0011 3728 seconds
ZUSS0036 1356 seconds
ZWMQ054 6809 seconds

VCM generates the JCL for executing all of the checks. Edit as required.

HINT:
//SYSTSIN DD *
PROFILE VARSTORAGE(HIGH)   <<< Help prevent some 878 abends
ISPSTART CMD(%VCMBATCH) NEWAPPL(VCM)

Vanguard Options

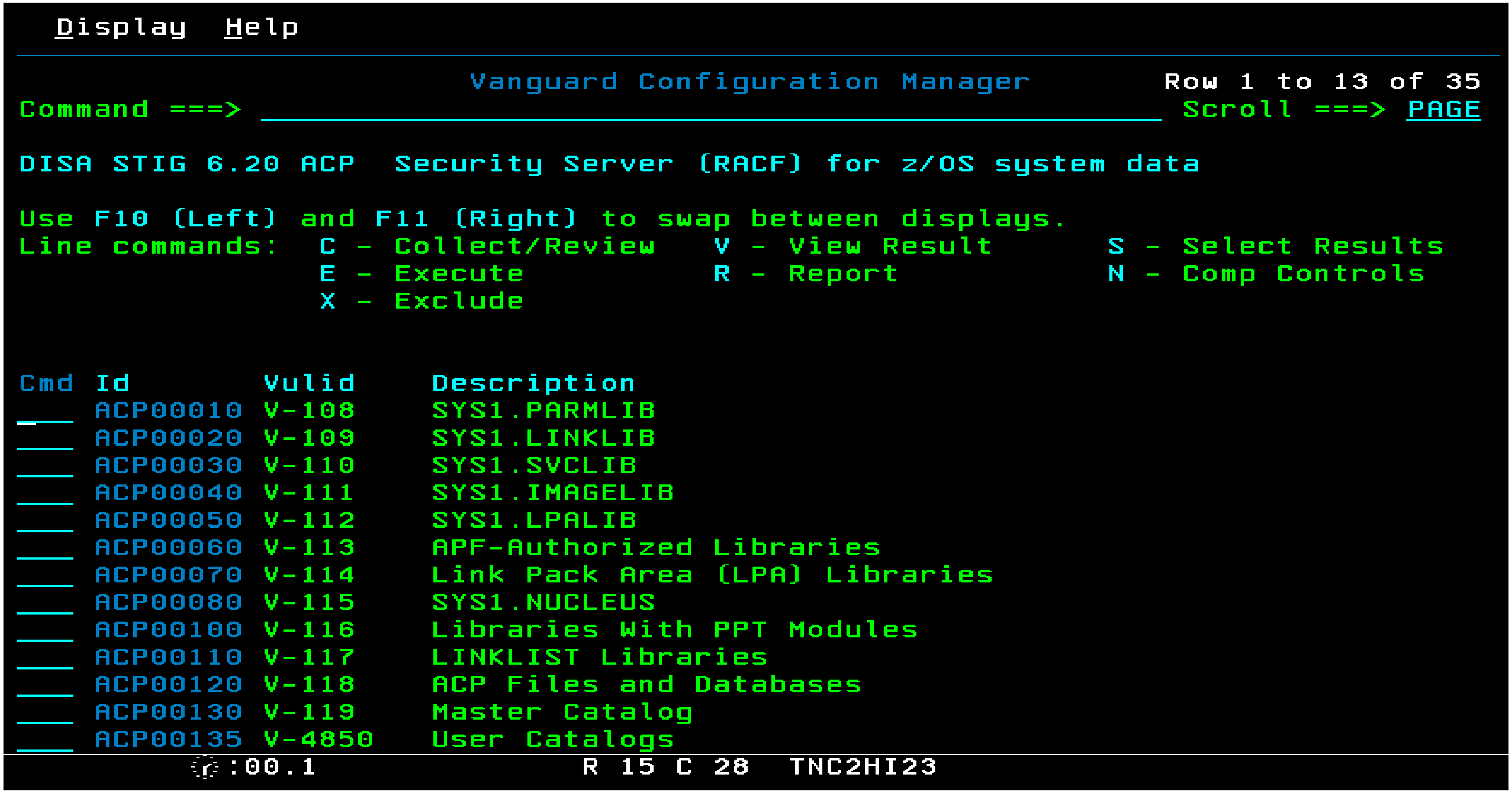
- Product settings VANOPTS(VCMOPT00)
- MAX_GENERATIONS(3)
  - Can be 1 to 20
- DETAIL_REPORT(SYS2.VCM.REPORTS.STIG616)

MAX_GENERATIONS specifies the maximum number of result generations to be saved for a check.

Value can be from 1 to 20

Will impact size of the results file

Reporting, Interactive

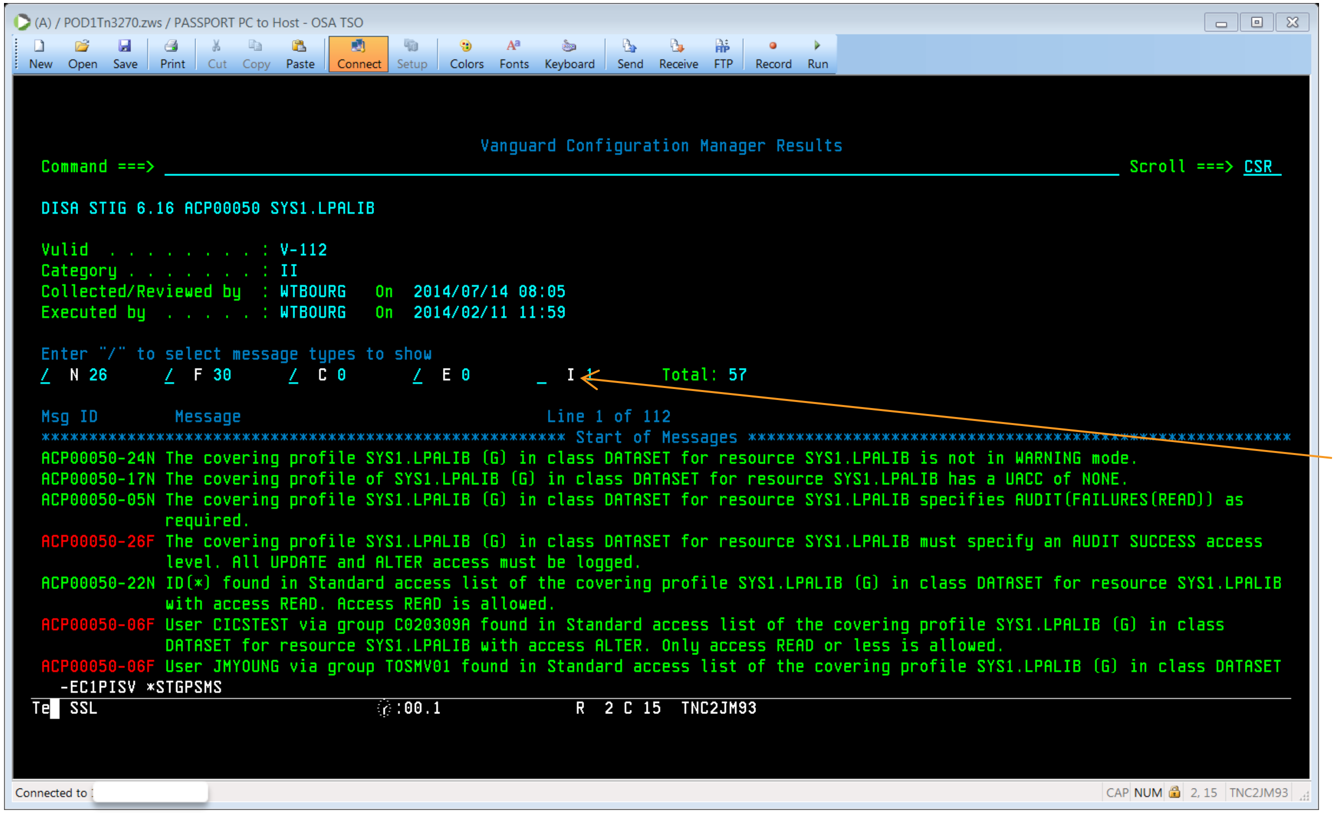


```
  Display  Help
------------------------------------------------------------------------------
                        Vanguard Configuration Manager       Row 1 to 13 of 35
Command ===> ________________________________________________ Scroll ===> PAGE

DISA STIG 6.20 ACP  Security Server (RACF) for z/OS system data

Use F10 (Left) and F11 (Right) to swap between displays.
Line commands:  C - Collect/Review    V - View Result       S - Select Results
                E - Execute           R - Report            N - Comp Controls
                X - Exclude


Cmd Id        Vulid     Description
___ ACP00010 V-108     SYS1.PARMLIB
___ ACP00020 V-109     SYS1.LINKLIB
___ ACP00030 V-110     SYS1.SVCLIB
___ ACP00040 V-111     SYS1.IMAGELIB
___ ACP00050 V-112     SYS1.LPALIB
___ ACP00060 V-113     APF-Authorized Libraries
___ ACP00070 V-114     Link Pack Area (LPA) Libraries
___ ACP00080 V-115     SYS1.NUCLEUS
___ ACP00100 V-116     Libraries With PPT Modules
___ ACP00110 V-117     LINKLIST Libraries
___ ACP00120 V-118     ACP Files and Databases
___ ACP00130 V-119     Master Catalog
___ ACP00135 V-4850    User Catalogs
          :00.1                R 15 C 28   TNC2HI23
```

V to View a report with filtering switches

R to generate a report that can be searched & emailed

View the Report



```
                                 Vanguard Configuration Manager Results
Command ===> ____________________________________________________________________________________________ Scroll ===> CSR

DISA STIG 6.16 ACP00050 SYS1.LPALIB

Vulid  . . . . . . . . . : V-112
Category . . . . . . . . : II
Collected/Reviewed by    : WTBOURG   On  2014/07/14 08:05
Executed by  . . . . . . : WTBOURG   On  2014/02/11 11:59

Enter "/" to select message types to show
/  N 26      /  F 30      /  C 0       /  E 0       _  I 1        Total: 57

Msg ID        Message                                  Line 1 of 112
******************************************************* Start of Messages *************************************************************
ACP00050-24N The covering profile SYS1.LPALIB (G) in class DATASET for resource SYS1.LPALIB is not in WARNING mode.
ACP00050-17N The covering profile of SYS1.LPALIB (G) in class DATASET for resource SYS1.LPALIB has a UACC of NONE.
ACP00050-05N The covering profile SYS1.LPALIB (G) in class DATASET for resource SYS1.LPALIB specifies AUDIT(FAILURES(READ)) as
             required.
ACP00050-26F The covering profile SYS1.LPALIB (G) in class DATASET for resource SYS1.LPALIB must specify an AUDIT SUCCESS access
             level. All UPDATE and ALTER access must be logged.
ACP00050-22N ID(*) found in Standard access list of the covering profile SYS1.LPALIB (G) in class DATASET for resource SYS1.LPALIB
             with access READ. Access READ is allowed.
ACP00050-06F User CICSTEST via group C020309A found in Standard access list of the covering profile SYS1.LPALIB (G) in class
             DATASET for resource SYS1.LPALIB with access ALTER. Only access READ or less is allowed.
ACP00050-06F User JMYOUNG via group TOSMV01 found in Standard access list of the covering profile SYS1.LPALIB (G) in class DATASET
  -EC1PISV *STGPSMS
Te  SSL                                 :00.1             R  2 C 15  TNC2JM93
```

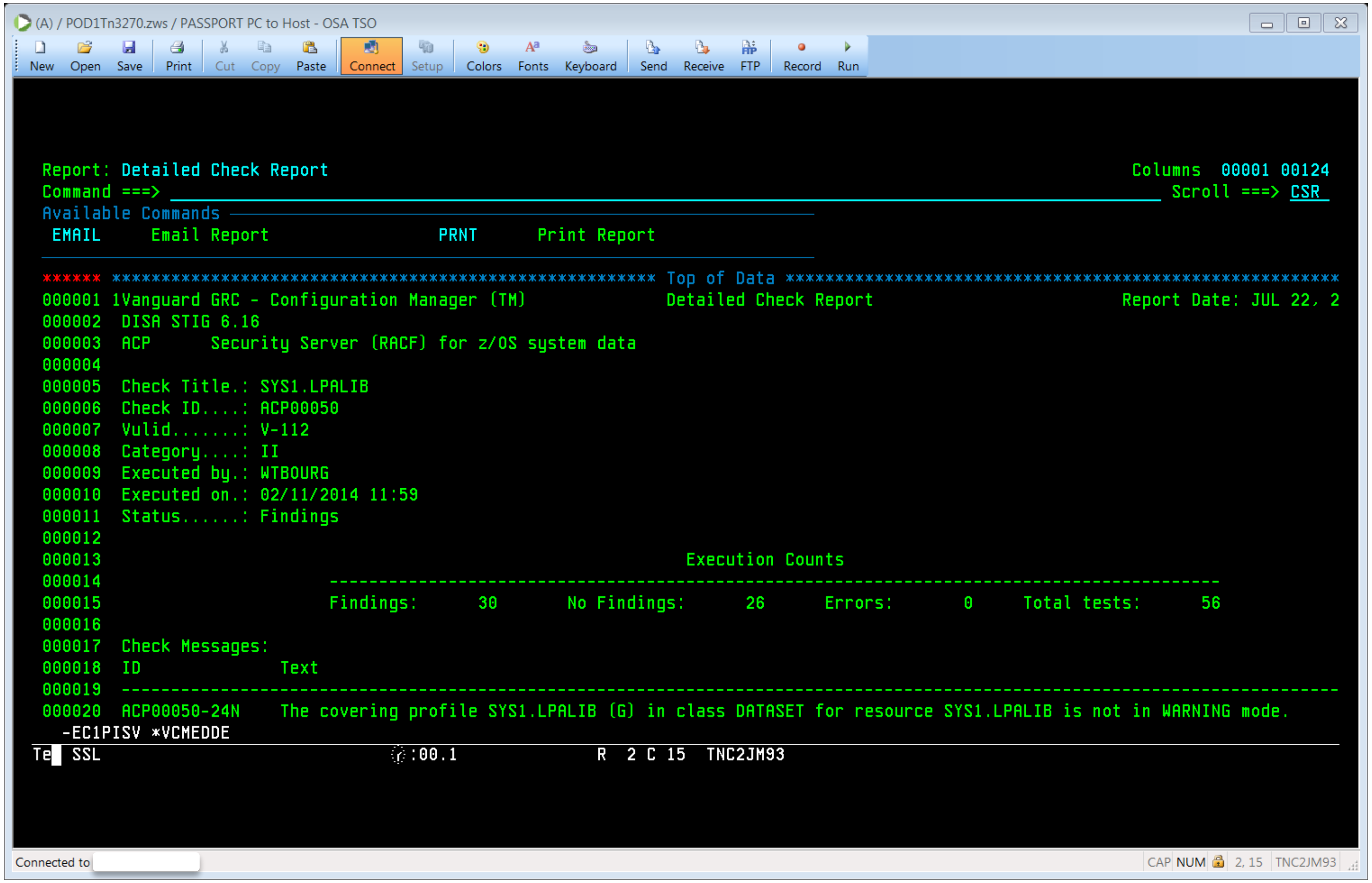
Set switch to show msgs

No Info msgs will be displayed

N = Normal
F = Findings
C = Compensating Control

E = Errors
I = Informational

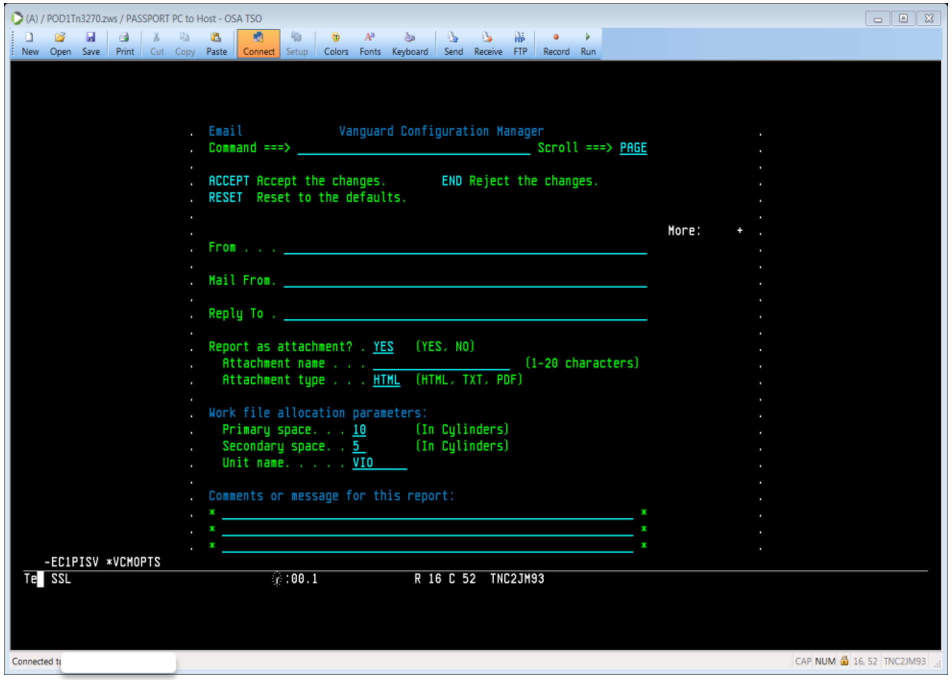
Generate a Report



```
Report: Detailed Check Report                                                                                 Columns  00001 00124
Command ===> ____________________________________________________________________________________________________ Scroll ===> CSR
Available Commands ---------------------------------------------------------
 EMAIL     Email Report                 PRNT      Print Report
------------------------------------------------------------------------------
****** ***************************************************** Top of Data *****************************************************
000001 1Vanguard GRC - Configuration Manager (TM)               Detailed Check Report                         Report Date: JUL 22, 2
000002  DISA STIG 6.16
000003  ACP      Security Server (RACF) for z/OS system data
000004
000005  Check Title.: SYS1.LPALIB
000006  Check ID....: ACP00050
000007  Vulid.......: V-112
000008  Category....: II
000009  Executed by.: WTBOURG
000010  Executed on.: 02/11/2014 11:59
000011  Status......: Findings
000012
000013                                                            Execution Counts
000014                       ------------------------------------------------------------------------------------------
000015                       Findings:      30        No Findings:      26       Errors:       0     Total tests:      56
000016
000017  Check Messages:
000018  ID              Text
000019  -----------------------------------------------------------------------------------------------------------------------------
000020  ACP00050-24N    The covering profile SYS1.LPALIB (G) in class DATASET for resource SYS1.LPALIB is not in WARNING mode.
  -EC1PISV *VCMEDDE
Te█ SSL                               :00.1              R   2 C 15   TNC2JM93
```

VCM can also generate the JCL to create a report in batch.

Convert Report to PDF



```
 .  Email                Vanguard Configuration Manager                   .
 .  Command ===> ________________________________ Scroll ===> PAGE        .
 .                                                                        .
 .  ACCEPT Accept the changes.       END Reject the changes.              .
 .  RESET  Reset to the defaults.                                         .
 .                                                                        .
 .                                                          More:     +  .
 .  From . . . _____________________________________________________       .
 .                                                                        .
 .  Mail From. _____________________________________________________       .
 .                                                                        .
 .  Reply To . _____________________________________________________       .
 .                                                                        .
 .  Report as attachment? . YES   (YES, NO)                               .
 .    Attachment name . . . ____________________  (1-20 characters)       .
 .    Attachment type . . . HTML  (HTML, TXT, PDF)                        .
 .                                                                        .
 .  Work file allocation parameters:                                      .
 .    Primary space. . . 10       (In Cylinders)                          .
 .    Secondary space. . 5        (In Cylinders)                          .
 .    Unit name. . . . . VIO                                              .
 .                                                                        .
 .  Comments or message for this report:                                  .
 .  * ____________________________________________________________ *      .
 .  * ____________________________________________________________ *      .
 .  * ____________________________________________________________ *      .
  -EC1PISV *VCMOPTS
 Te  SSL                     :00.1            R 16 C 52   TNC2JM93
```

VANOPTS(EMAILOPT)

*   The following parameters are for PDF support

*   The TXT2PDF utility must be installed to use this feature.

*

* EMAILPDFLOAD(TXT2PDF load library)

* EMAILPDFEXEC(TXT2PDF exec library)

EMAILPDFLOAD(SYS7.XMITIP.LOAD)

EMAILPDFEXEC(SYS7.XMITIP.EXEC)

*

* EMAILPDFCONFIG(<HLQ>.VANSAMP)   Sequential or PDS dataset.

* EMAILPDFCONFIGM(PDFCONFG)   EMAILPDFCONFIG is a PDS,

EMAILPDFCONFIG(SYS1.VANGUARD.VANOPTS)

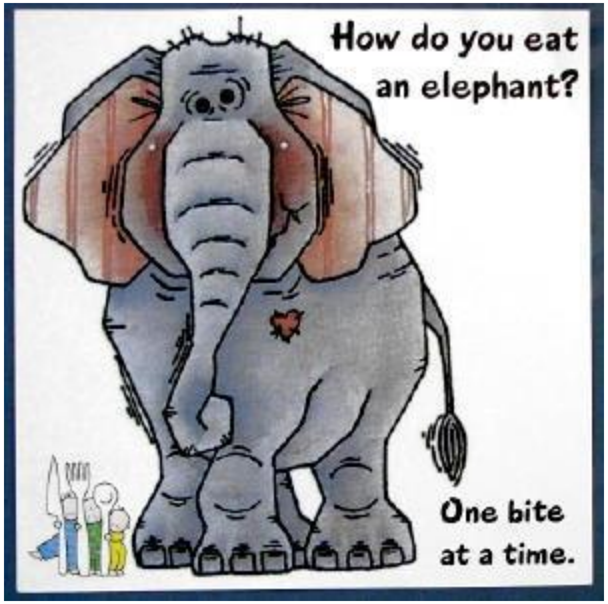
EMAILPDFCONFIGM(PDFCONFG)

TXT2PDF and XMITIP can be found at Lionel B Dyck’s site: http://www.lbdsoftware.com/

Three Choices

- Correct the reported finding
- Modify the collection data (if possible)
- Create a Compensating Control and/or a policy statement

Remediate



Some reports can be vary large
ACP Security Server (RACF) for z/OS
system data
Check Title.: APF-Authorized Libraries
Check ID....: ACP00060

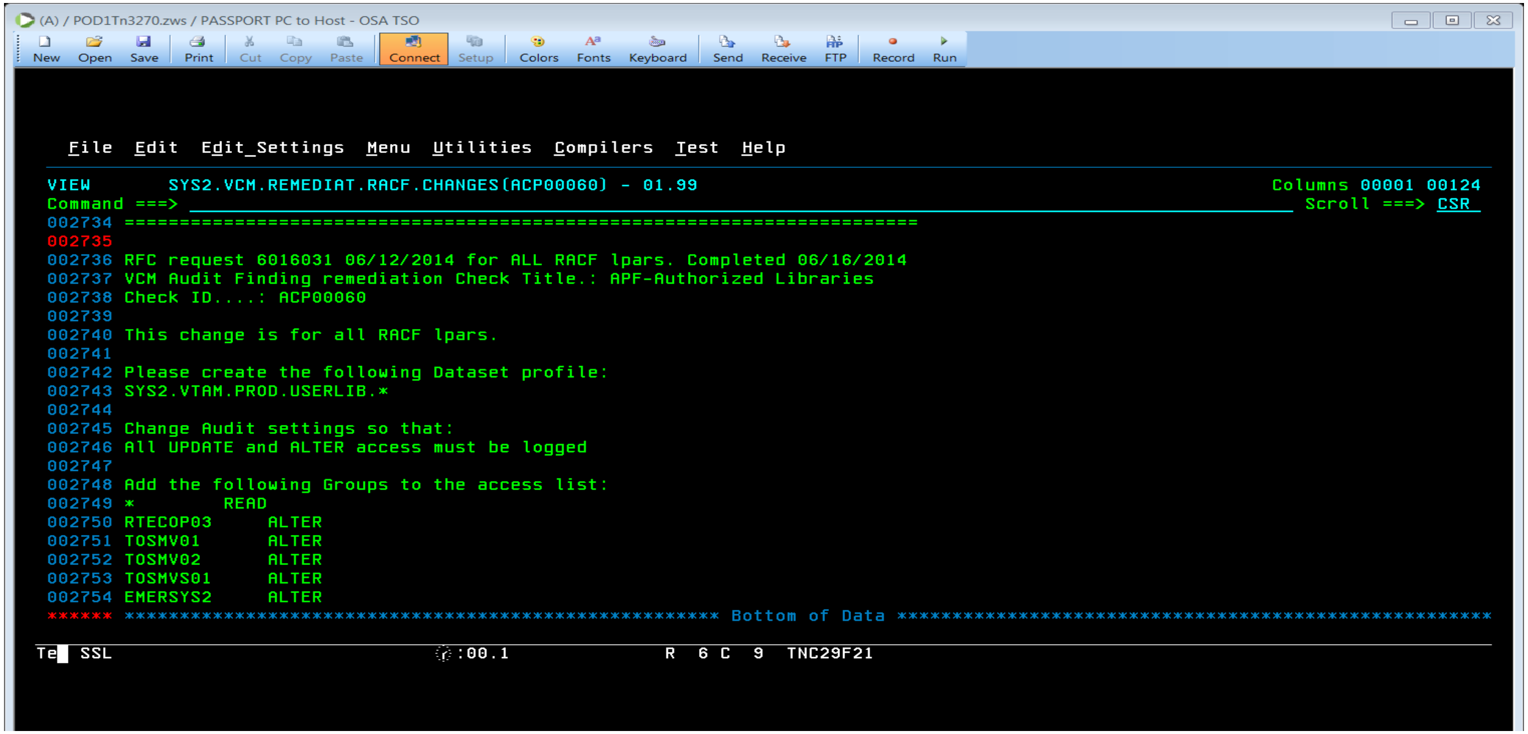
ACP0060 is about 300,000 lines.
Originally it had close to 100,000 findings.

View Report with only ‘I’ filter selected.
This will give a list of RACF profiles. Work
one profile at a time.

Use DISA STIG Addendum as guidance.

Tools to Help
VRA – UserID in access list Report
SMF data
RACF Authority ****

Track your RFCs!

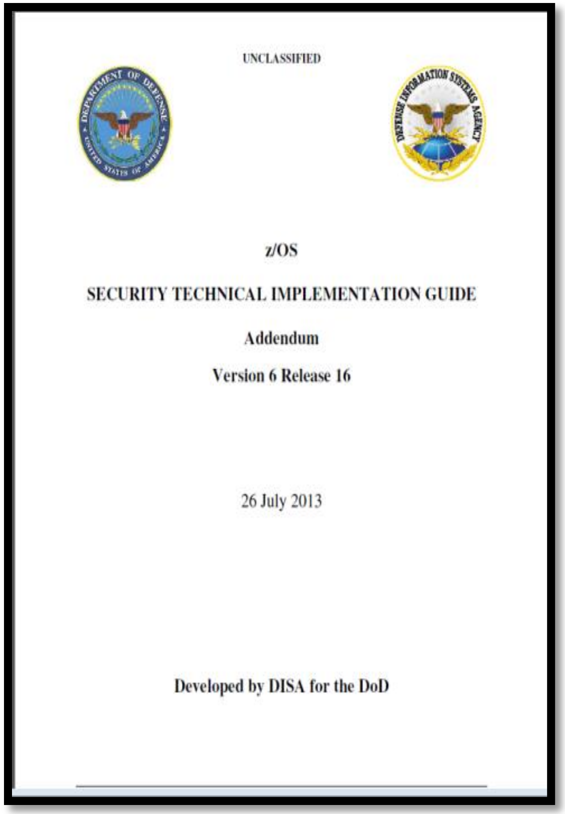


```
  File  Edit  Edit_Settings  Menu  Utilities  Compilers  Test  Help
VIEW       SYS2.VCM.REMEDIAT.RACF.CHANGES(ACP00060) - 01.99           Columns 00001 00124
Command ===>                                                             Scroll ===> CSR
002734 ========================================================================
002735
002736 RFC request 6016031 06/12/2014 for ALL RACF lpars. Completed 06/16/2014
002737 VCM Audit Finding remediation Check Title.: APF-Authorized Libraries
002738 Check ID....: ACP00060
002739
002740 This change is for all RACF lpars.
002741
002742 Please create the following Dataset profile:
002743 SYS2.VTAM.PROD.USERLIB.*
002744
002745 Change Audit settings so that:
002746 All UPDATE and ALTER access must be logged
002747
002748 Add the following Groups to the access list:
002749 *        READ
002750 RTECOP03     ALTER
002751 TOSMV01      ALTER
002752 TOSMV02      ALTER
002753 TOSMVS01     ALTER
002754 EMERSYS2     ALTER
****** ****************************************************** Bottom of Data ******************************************************

Te  SSL                          :00.1             R  6 C  9  TNC29F21
```

What did you do when?

“What happened to my access?!?!”

DISA STIG ADDENDUM



UNCLASSIFIED

z/OS

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Addendum

Version 6 Release 16

26 July 2013

Developed by DISA for the DoD

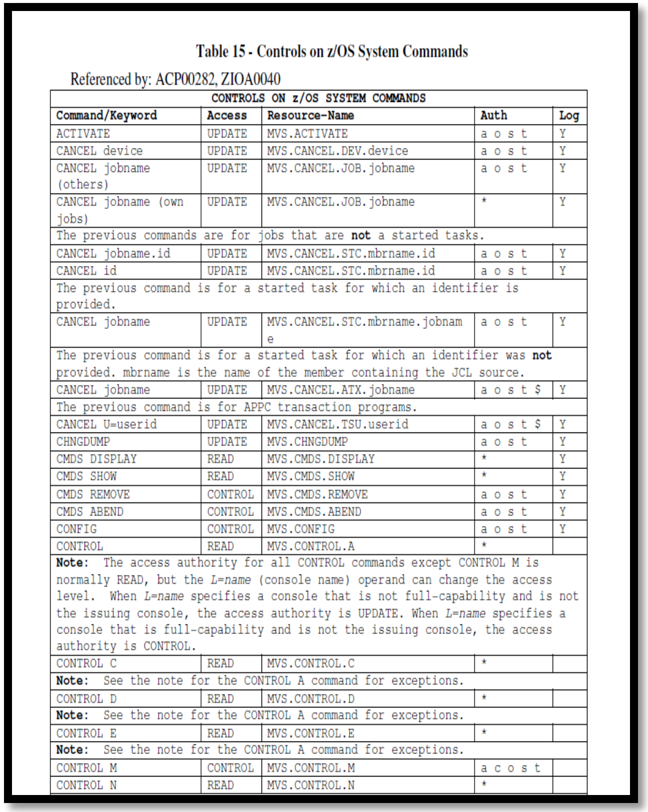


Table 15 - Controls on z/OS System Commands

Referenced by: ACP00282, ZIOA0040

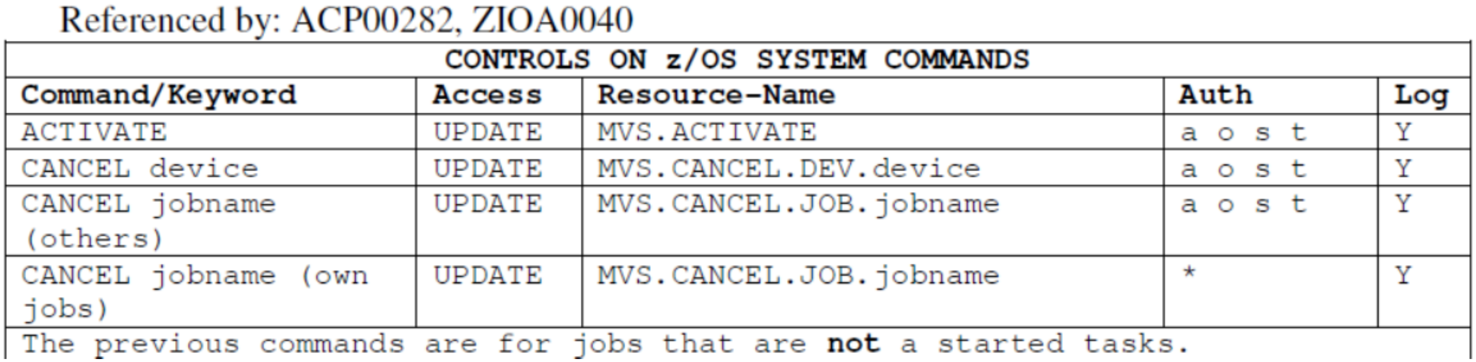
CONTROLS ON z/OS SYSTEM COMMANDS

Command/Keyword	**Access**	**Resource-Name**	**Auth**	**Log**
ACTIVATE	UPDATE	MVS.ACTIVATE	a o s t	Y
CANCEL device	UPDATE	MVS.CANCEL.DEV.device	a o s t	Y
CANCEL jobname (others)	UPDATE	MVS.CANCEL.JOB.jobname	a o s t	Y
CANCEL jobname (own jobs)	UPDATE	MVS.CANCEL.JOB.jobname	*	Y
The previous commands are for jobs that are **not** a started tasks.				
CANCEL jobname.id	UPDATE	MVS.CANCEL.STC.mbrname.id	a o s t	Y
CANCEL id	UPDATE	MVS.CANCEL.STC.mbrname.id	a o s t	Y
The previous command is for a started task for which an identifier is provided.				
CANCEL jobname	UPDATE	MVS.CANCEL.STC.mbrname.jobname	a o s t	Y
The previous command is for a started task for which an identifier was **not** provided. mbrname is the name of the member containing the JCL source.				
CANCEL jobname	UPDATE	MVS.CANCEL.ATX.jobname	a o s t $	Y
The previous command is for APPC transaction programs.				
CANCEL U=userid	UPDATE	MVS.CANCEL.TSU.userid	a o s t $	Y
CHNGDUMP	UPDATE	MVS.CHNGDUMP	a o s t	Y
CMDS DISPLAY	READ	MVS.CMDS.DISPLAY	*	Y
CMDS SHOW	READ	MVS.CMDS.SHOW	*	Y
CMDS REMOVE	CONTROL	MVS.CMDS.REMOVE	a o s t	Y
CMDS ABEND	CONTROL	MVS.CMDS.ABEND	a o s t	Y
CONFIG	CONTROL	MVS.CONFIG	a o s t	Y
CONTROL	READ	MVS.CONTROL.A	*	
Note: The access authority for all CONTROL commands except CONTROL M is normally READ, but the *L=name* (console name) operand can change the access level. When *L=name* specifies a console that is not full-capability and is not the issuing console, the access authority is UPDATE. When *L=name* specifies a console that is full-capability and is not the issuing console, the access authority is CONTROL.				
CONTROL C	READ	MVS.CONTROL.C	*	
Note: See the note for the CONTROL A command for exceptions.				
CONTROL D	READ	MVS.CONTROL.D	*	
Note: See the note for the CONTROL A command for exceptions.				
CONTROL E	READ	MVS.CONTROL.E	*	
Note: See the note for the CONTROL A command for exceptions.				
CONTROL M	CONTROL	MVS.CONTROL.M	a c o s t	
CONTROL N	READ	MVS.CONTROL.N	*	

Contains background, guidance, definitions, and so on…

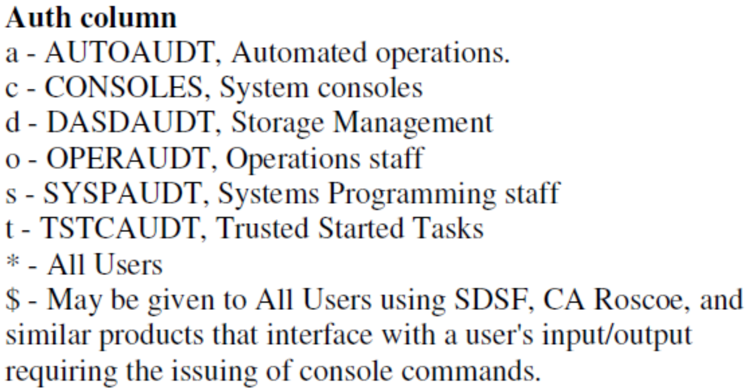
Download from Vanguard
https://www.go2vanguard.com/download_checklist1.php
Download from DISA Website
http://iase.disa.mil/stigs/os/mainframe/z_os.html

DISA STIG ADDENDUM



Referenced by: ACP00282, ZIOA0040

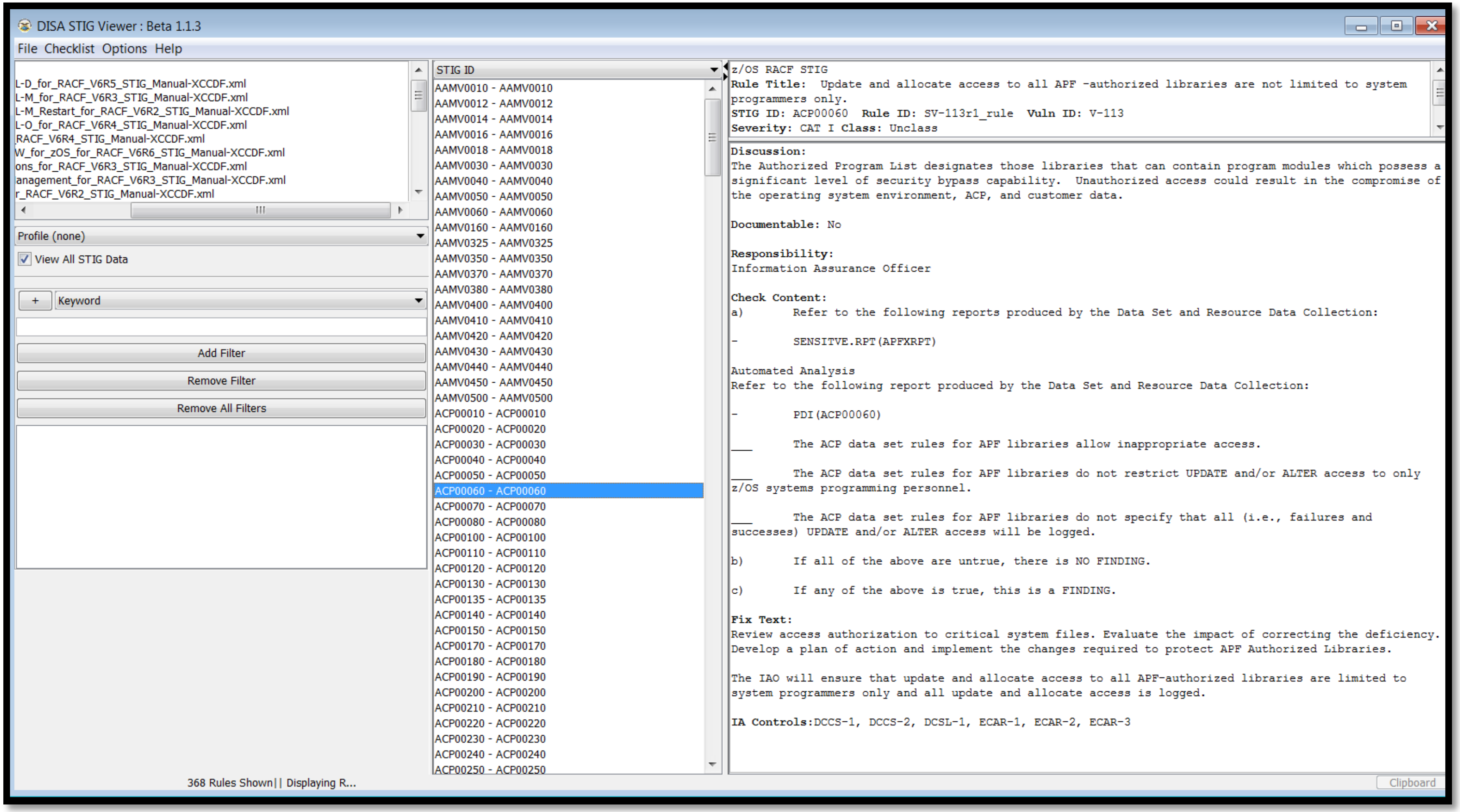
CONTROLS ON z/OS SYSTEM COMMANDS				
Command/Keyword	**Access**	**Resource-Name**	**Auth**	**Log**
ACTIVATE	UPDATE	MVS.ACTIVATE	a o s t	Y
CANCEL device	UPDATE	MVS.CANCEL.DEV.device	a o s t	Y
CANCEL jobname (others)	UPDATE	MVS.CANCEL.JOB.jobname	a o s t	Y
CANCEL jobname (own jobs)	UPDATE	MVS.CANCEL.JOB.jobname	*	Y
The previous commands are for jobs that are **not** a started tasks.				



Auth column

a - AUTOAUDT, Automated operations.
c - CONSOLES, System consoles
d - DASDAUDT, Storage Management
o - OPERAUDT, Operations staff
s - SYSPAUDT, Systems Programming staff
t - TSTCAUDT, Trusted Started Tasks
* - All Users
$ - May be given to All Users using SDSF, CA Roscoe, and similar products that interface with a user's input/output requiring the issuing of console commands.

Java Viewer



L-D_for_RACF_V6R5_STIG_Manual-XCCDF.xml
L-M_for_RACF_V6R3_STIG_Manual-XCCDF.xml
L-M_Restart_for_RACF_V6R2_STIG_Manual-XCCDF.xml
L-O_for_RACF_V6R4_STIG_Manual-XCCDF.xml
RACF_V6R4_STIG_Manual-XCCDF.xml
W_for_zOS_for_RACF_V6R6_STIG_Manual-XCCDF.xml
ons_for_RACF_V6R3_STIG_Manual-XCCDF.xml
anagement_for_RACF_V6R3_STIG_Manual-XCCDF.xml
r_RACF_V6R2_STIG_Manual-XCCDF.xml

Profile (none)

☑ View All STIG Data

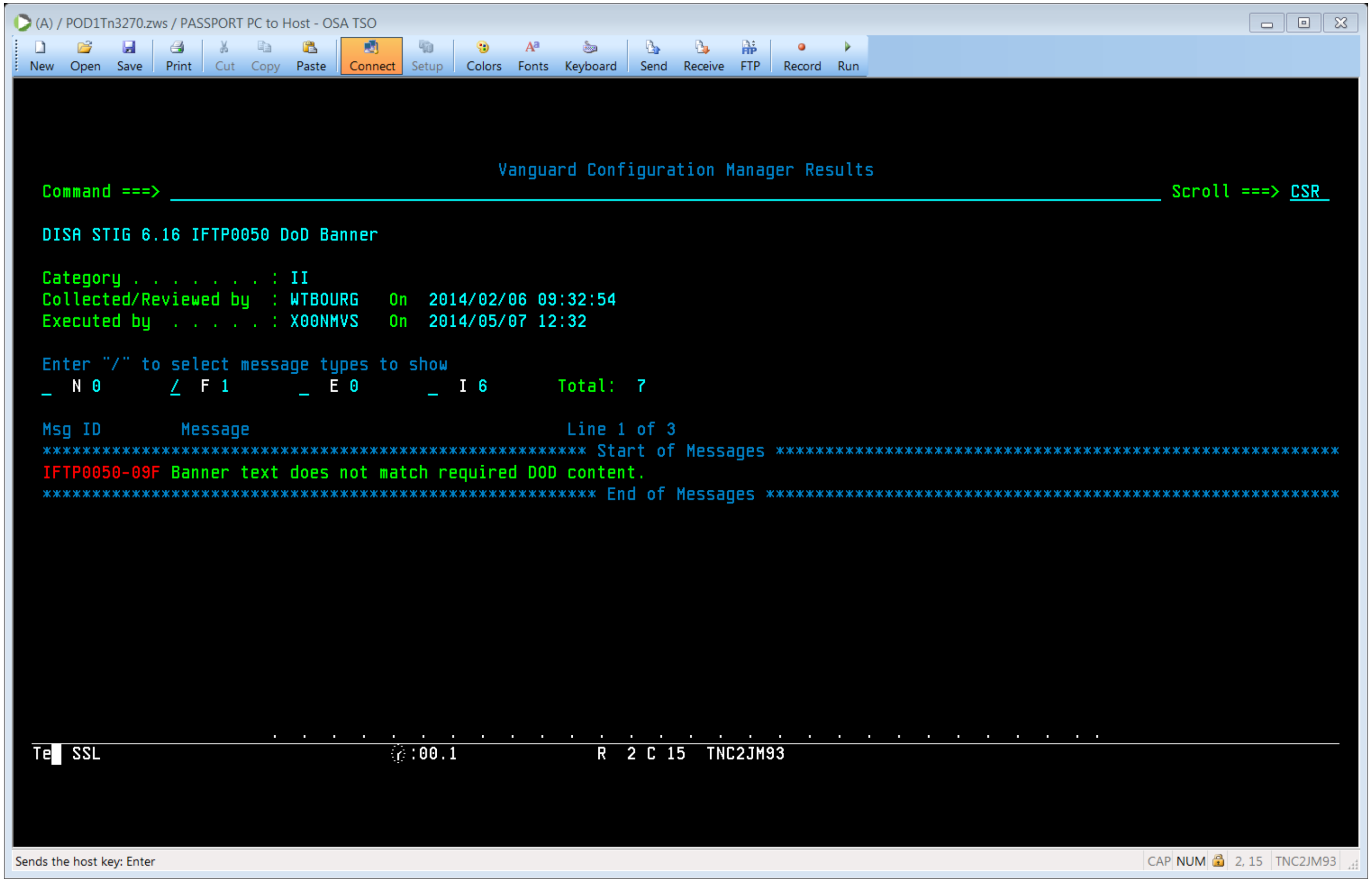
AAMV0010 - AAMV0010
AAMV0012 - AAMV0012
AAMV0014 - AAMV0014
AAMV0016 - AAMV0016
AAMV0018 - AAMV0018
AAMV0030 - AAMV0030
AAMV0040 - AAMV0040
AAMV0050 - AAMV0050
AAMV0060 - AAMV0060
AAMV0160 - AAMV0160
AAMV0325 - AAMV0325
AAMV0350 - AAMV0350
AAMV0370 - AAMV0370
AAMV0380 - AAMV0380
AAMV0400 - AAMV0400
AAMV0410 - AAMV0410
AAMV0420 - AAMV0420
AAMV0430 - AAMV0430
AAMV0440 - AAMV0440
AAMV0450 - AAMV0450
AAMV0500 - AAMV0500
ACP00010 - ACP00010
ACP00020 - ACP00020
ACP00030 - ACP00030
ACP00040 - ACP00040
ACP00050 - ACP00050
ACP00060 - ACP00060
ACP00070 - ACP00070
ACP00080 - ACP00080
ACP00100 - ACP00100
ACP00110 - ACP00110
ACP00120 - ACP00120
ACP00130 - ACP00130
ACP00135 - ACP00135
ACP00140 - ACP00140
ACP00150 - ACP00150
ACP00170 - ACP00170
ACP00180 - ACP00180
ACP00190 - ACP00190
ACP00200 - ACP00200
ACP00210 - ACP00210
ACP00220 - ACP00220
ACP00230 - ACP00230
ACP00240 - ACP00240
ACP00250 - ACP00250

```
z/OS RACF STIG
Rule Title:  Update and allocate access to all APF -authorized libraries are not limited to system
programmers only.
STIG ID: ACP00060  Rule ID: SV-113r1_rule  Vuln ID: V-113
Severity: CAT I Class: Unclass

Discussion:
The Authorized Program List designates those libraries that can contain program modules which possess a
significant level of security bypass capability.  Unauthorized access could result in the compromise of
the operating system environment, ACP, and customer data.

Documentable: No

Responsibility:
Information Assurance Officer

Check Content:
a)        Refer to the following reports produced by the Data Set and Resource Data Collection:

-         SENSITVE.RPT(APFXRPT)

Automated Analysis
Refer to the following report produced by the Data Set and Resource Data Collection:

-         PDI(ACP00060)

___       The ACP data set rules for APF libraries allow inappropriate access.

___       The ACP data set rules for APF libraries do not restrict UPDATE and/or ALTER access to only
z/OS systems programming personnel.

___       The ACP data set rules for APF libraries do not specify that all (i.e., failures and
successes) UPDATE and/or ALTER access will be logged.

b)        If all of the above are untrue, there is NO FINDING.

c)        If any of the above is true, this is a FINDING.

Fix Text:
Review access authorization to critical system files. Evaluate the impact of correcting the deficiency.
Develop a plan of action and implement the changes required to protect APF Authorized Libraries.

The IAO will ensure that update and allocate access to all APF-authorized libraries are limited to
system programmers only and all update and allocate access is logged.

IA Controls:DCCS-1, DCCS-2, DCSL-1, ECAR-1, ECAR-2, ECAR-3
```

368 Rules Shown|| Displaying R...

Download from http://iase.disa.mil/stigs/stig_viewing_guidance.html

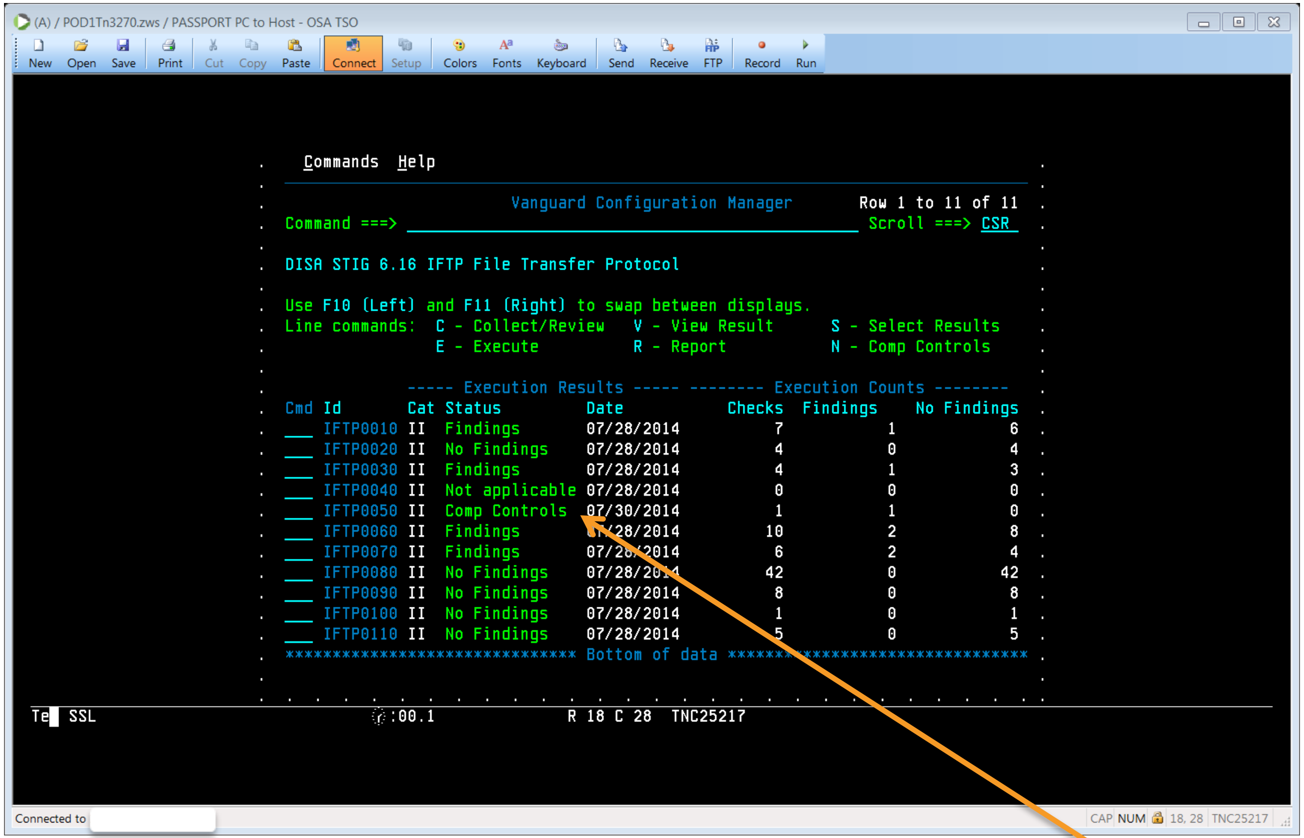
Compensating Controls



```
                                         Vanguard Configuration Manager Results
  Command ===> ____________________________________________________________________________________ Scroll ===> CSR

  DISA STIG 6.16 IFTP0050 DoD Banner

  Category . . . . . . . : II
  Collected/Reviewed by  : WTBOURG   On  2014/02/06 09:32:54
  Executed by  . . . . . : X00NMVS   On  2014/05/07 12:32

  Enter "/" to select message types to show
  _  N 0        /  F 1        _  E 0        _  I 6       Total:  7

  Msg ID         Message                                     Line 1 of 3
  ******************************************************** Start of Messages *********************************************************
  IFTP0050-09F Banner text does not match required DOD content.
  ********************************************************* End of Messages **********************************************************



 Te  SSL                              :00.1              R  2 C 15  TNC2JM93
```

But we are a Bank not the DOD!

Compensating Controls

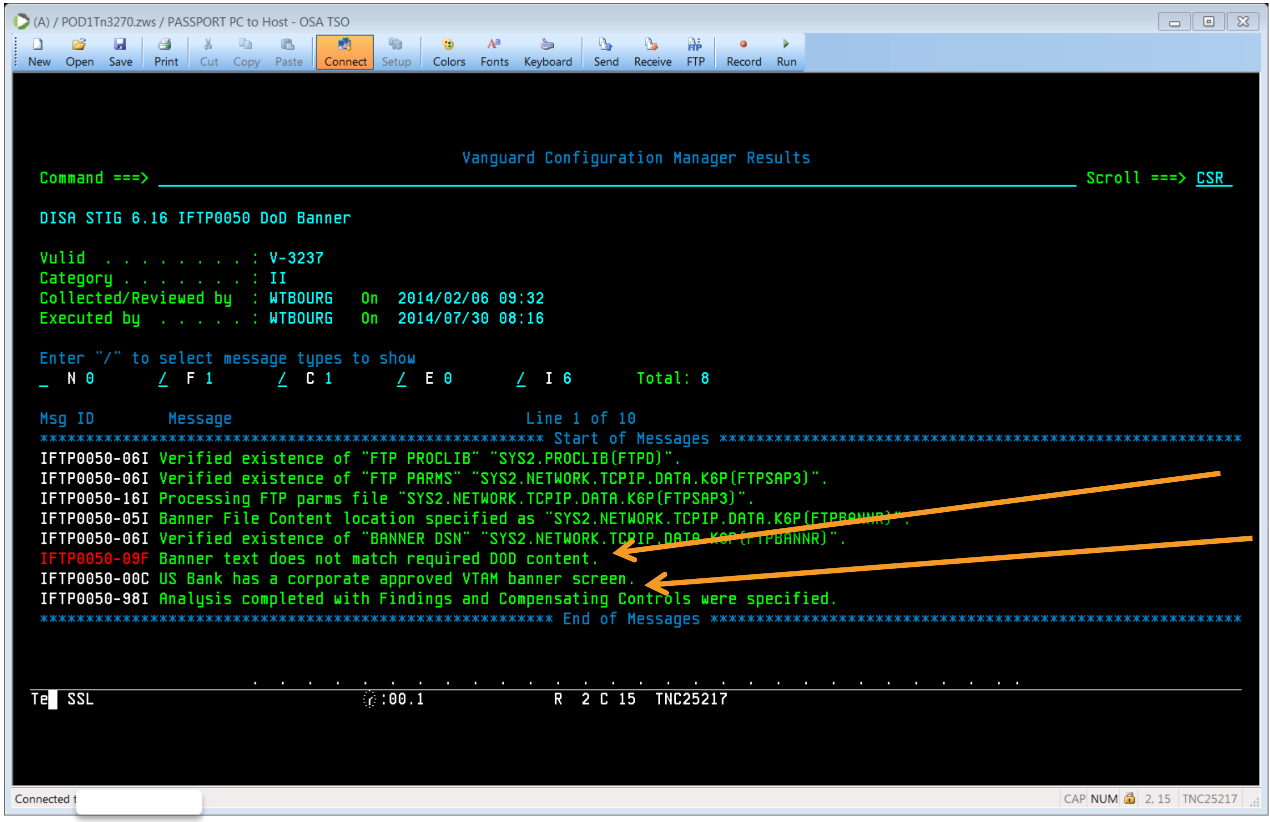


```
  Commands  Help
                        Vanguard Configuration Manager       Row 1 to 11 of 11
Command ===> ________________________________________________ Scroll ===> CSR

DISA STIG 6.16 IFTP File Transfer Protocol

Use F10 (Left) and F11 (Right) to swap between displays.
Line commands:  C - Collect/Review    V - View Result      S - Select Results
                E - Execute           R - Report           N - Comp Controls

             ----- Execution Results ----- -------- Execution Counts --------
Cmd Id       Cat Status          Date           Checks  Findings    No Findings
___ IFTP0010 II  Findings        07/28/2014          7         1              6
___ IFTP0020 II  No Findings     07/28/2014          4         0              4
___ IFTP0030 II  Findings        07/28/2014          4         1              3
___ IFTP0040 II  Not applicable  07/28/2014          0         0              0
___ IFTP0050 II  Comp Controls   07/30/2014          1         1              0
___ IFTP0060 II  Findings        07/28/2014         10         2              8
___ IFTP0070 II  Findings        07/28/2014          6         2              4
___ IFTP0080 II  No Findings     07/28/2014         42         0             42
___ IFTP0090 II  No Findings     07/28/2014          8         0              8
___ IFTP0100 II  No Findings     07/28/2014          1         0              1
___ IFTP0110 II  No Findings     07/28/2014          5         0              5
******************************* Bottom of data ********************************

Te  SSL                              :00.1            R 18 C 28   TNC25217
```

N to open text box to enter Compensating Control

Re-execute the check, status changes to Comp Controls

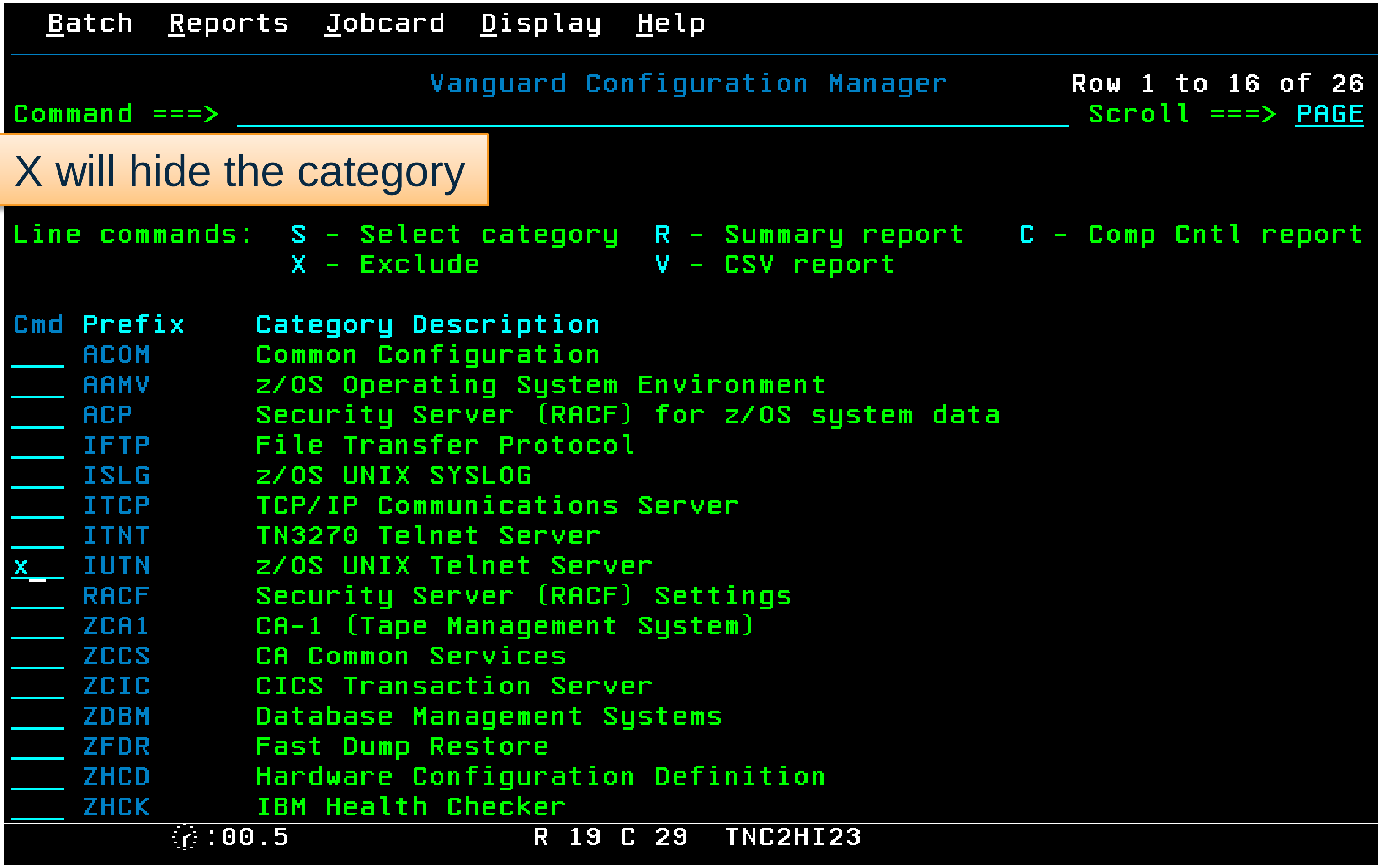
Compensating Controls



```
                              Vanguard Configuration Manager Results
Command ===> ____________________________________________________________________ Scroll ===> CSR_

DISA STIG 6.16 IFTP0050 DoD Banner

Vulid  . . . . . . . . . : V-3237
Category . . . . . . . . : II
Collected/Reviewed by    : WTBOURG   On  2014/02/06 09:32
Executed by  . . . . . . : WTBOURG   On  2014/07/30 08:16

Enter "/" to select message types to show
_  N 0      /  F 1      /  C 1      /  E 0      /  I 6      Total: 8

Msg ID        Message                              Line 1 of 10
******************************************************* Start of Messages *********************************************************
IFTP0050-06I Verified existence of "FTP PROCLIB" "SYS2.PROCLIB(FTPD)".
IFTP0050-06I Verified existence of "FTP PARMS" "SYS2.NETWORK.TCPIP.DATA.K6P(FTPSAP3)".
IFTP0050-16I Processing FTP parms file "SYS2.NETWORK.TCPIP.DATA.K6P(FTPSAP3)".
IFTP0050-05I Banner File Content location specified as "SYS2.NETWORK.TCPIP.DATA.K6P(FTPBANNR)".
IFTP0050-06I Verified existence of "BANNER DSN" "SYS2.NETWORK.TCPIP.DATA.K6P(FTPBANNR)".
IFTP0050-09F Banner text does not match required DOD content.
IFTP0050-00C US Bank has a corporate approved VTAM banner screen.
IFTP0050-98I Analysis completed with Findings and Compensating Controls were specified.
******************************************************** End of Messages *********************************************************

                                        . . . . . . . . . . . . . . . . . . . . . . . . . . . .
Te  SSL                          :00.1              R  2 C 15   TNC25217
```

The finding is still there; Why the number will never be zero Msg IFTP0050-00C

VCM Filters

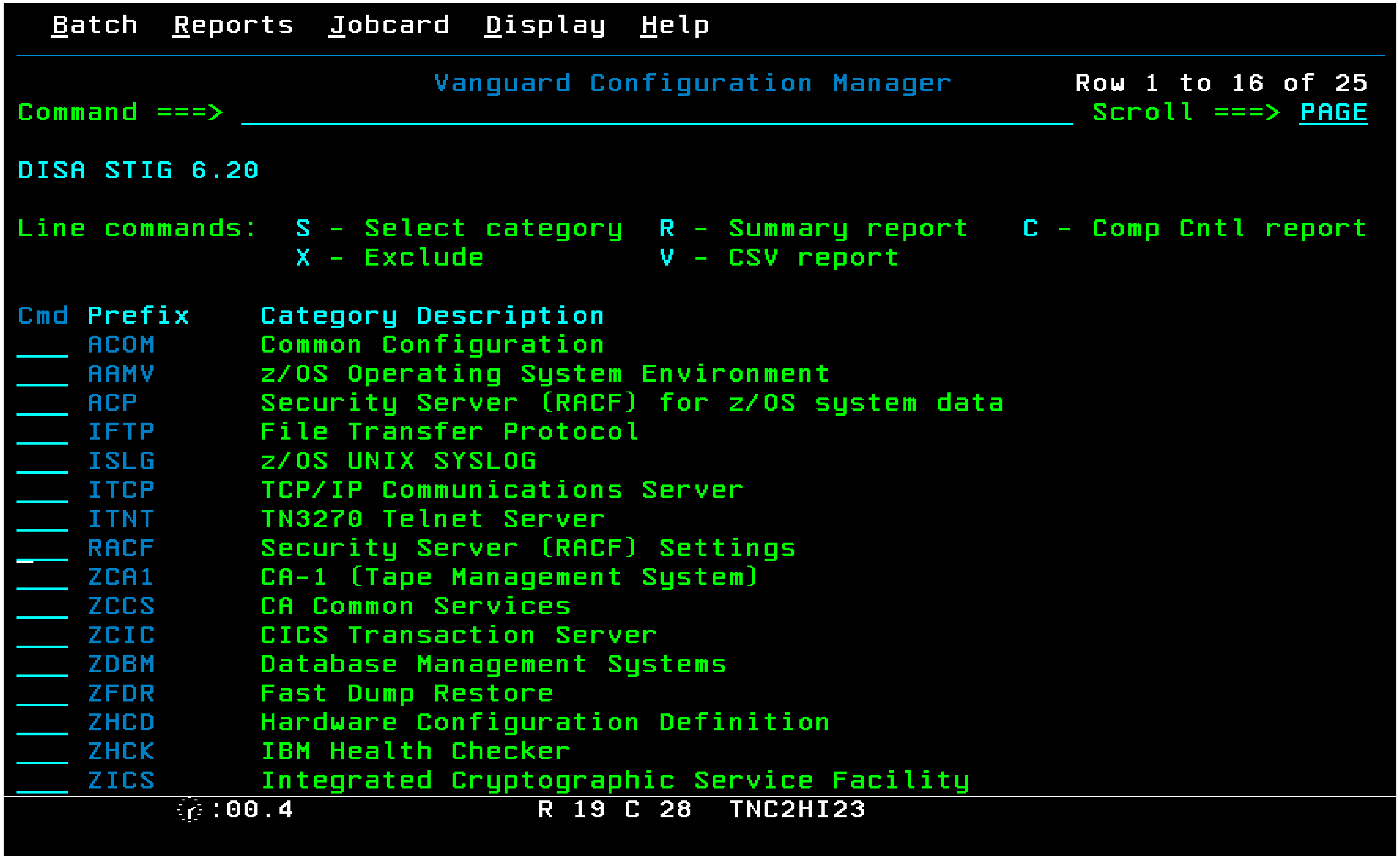


```
  Batch  Reports  Jobcard  Display  Help
-------------------------------------------------------------------------------
                        Vanguard Configuration Manager          Row 1 to 16 of 26
Command ===> ________________________________________________ Scroll ===> PAGE


Line commands:  S - Select category  R - Summary report   C - Comp Cntl report
                X - Exclude          V - CSV report

Cmd Prefix     Category Description
___ ACOM       Common Configuration
___ AAMV       z/OS Operating System Environment
___ ACP        Security Server (RACF) for z/OS system data
___ IFTP       File Transfer Protocol
___ ISLG       z/OS UNIX SYSLOG
___ ITCP       TCP/IP Communications Server
___ ITNT       TN3270 Telnet Server
x__ IUTN       z/OS UNIX Telnet Server
___ RACF       Security Server (RACF) Settings
___ ZCA1       CA-1 (Tape Management System)
___ ZCCS       CA Common Services
___ ZCIC       CICS Transaction Server
___ ZDBM       Database Management Systems
___ ZFDR       Fast Dump Restore
___ ZHCD       Hardware Configuration Definition
___ ZHCK       IBM Health Checker
          :00.5              R 19 C 29   TNC2HI23
```

An X will hide the category

Remove unwanted categories and individual checks from your display

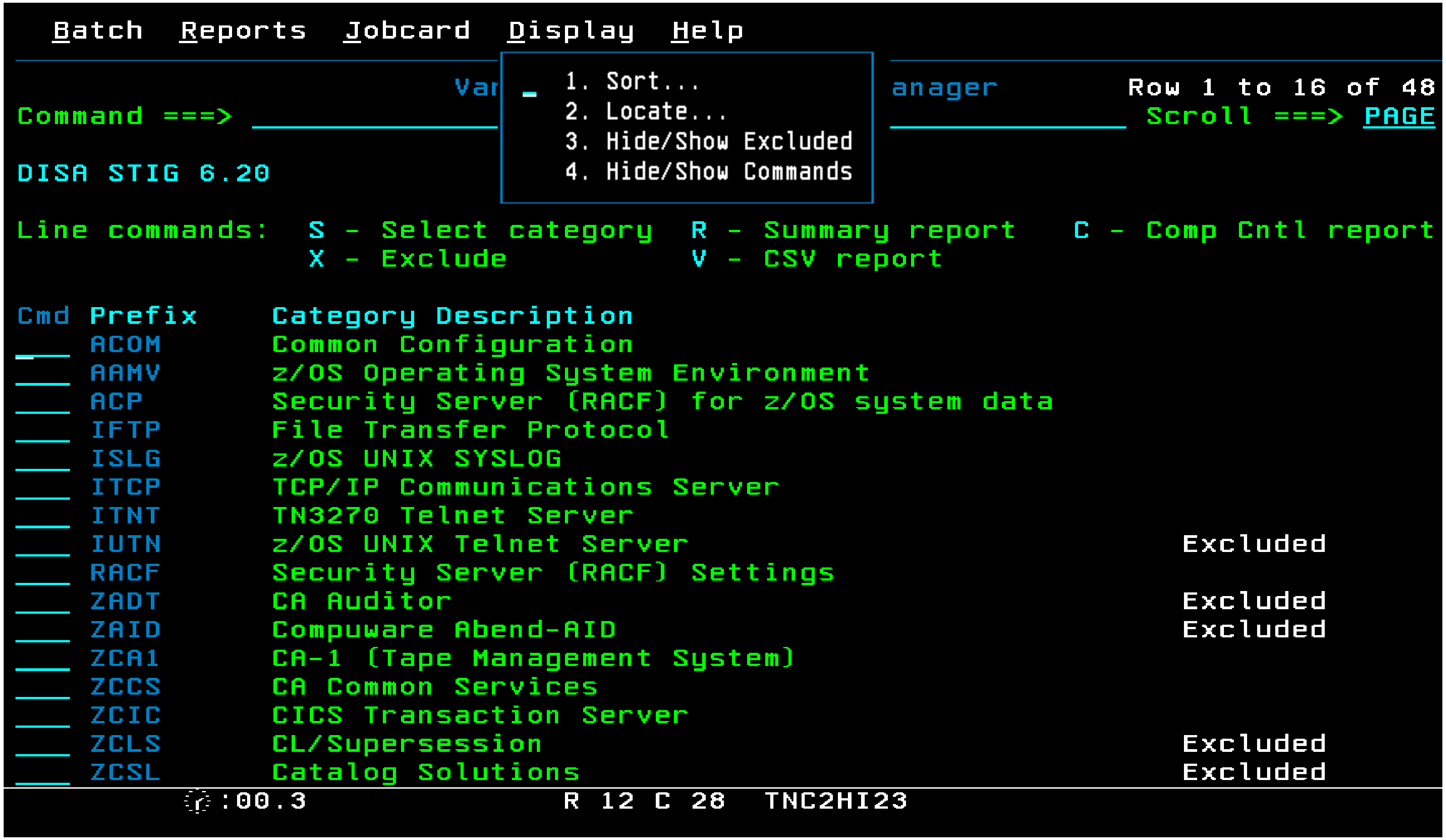
VCM Filters



```
  Batch  Reports  Jobcard  Display  Help

                        Vanguard Configuration Manager       Row 1 to 16 of 25
Command ===> ________________________________________________ Scroll ===> PAGE

DISA STIG 6.20

Line commands:  S - Select category  R - Summary report   C - Comp Cntl report
                X - Exclude          V - CSV report

Cmd Prefix    Category Description
___ ACOM      Common Configuration
___ AAMV      z/OS Operating System Environment
___ ACP       Security Server (RACF) for z/OS system data
___ IFTP      File Transfer Protocol
___ ISLG      z/OS UNIX SYSLOG
___ ITCP      TCP/IP Communications Server
___ ITNT      TN3270 Telnet Server
___ RACF      Security Server (RACF) Settings
___ ZCA1      CA-1 (Tape Management System)
___ ZCCS      CA Common Services
___ ZCIC      CICS Transaction Server
___ ZDBM      Database Management Systems
___ ZFDR      Fast Dump Restore
___ ZHCD      Hardware Configuration Definition
___ ZHCK      IBM Health Checker
___ ZICS      Integrated Cryptographic Service Facility
          :00.4              R 19 C 28   TNC2HI23
```

The IUNT z/OS UNIX Telnet Server category is now filtered from the display.

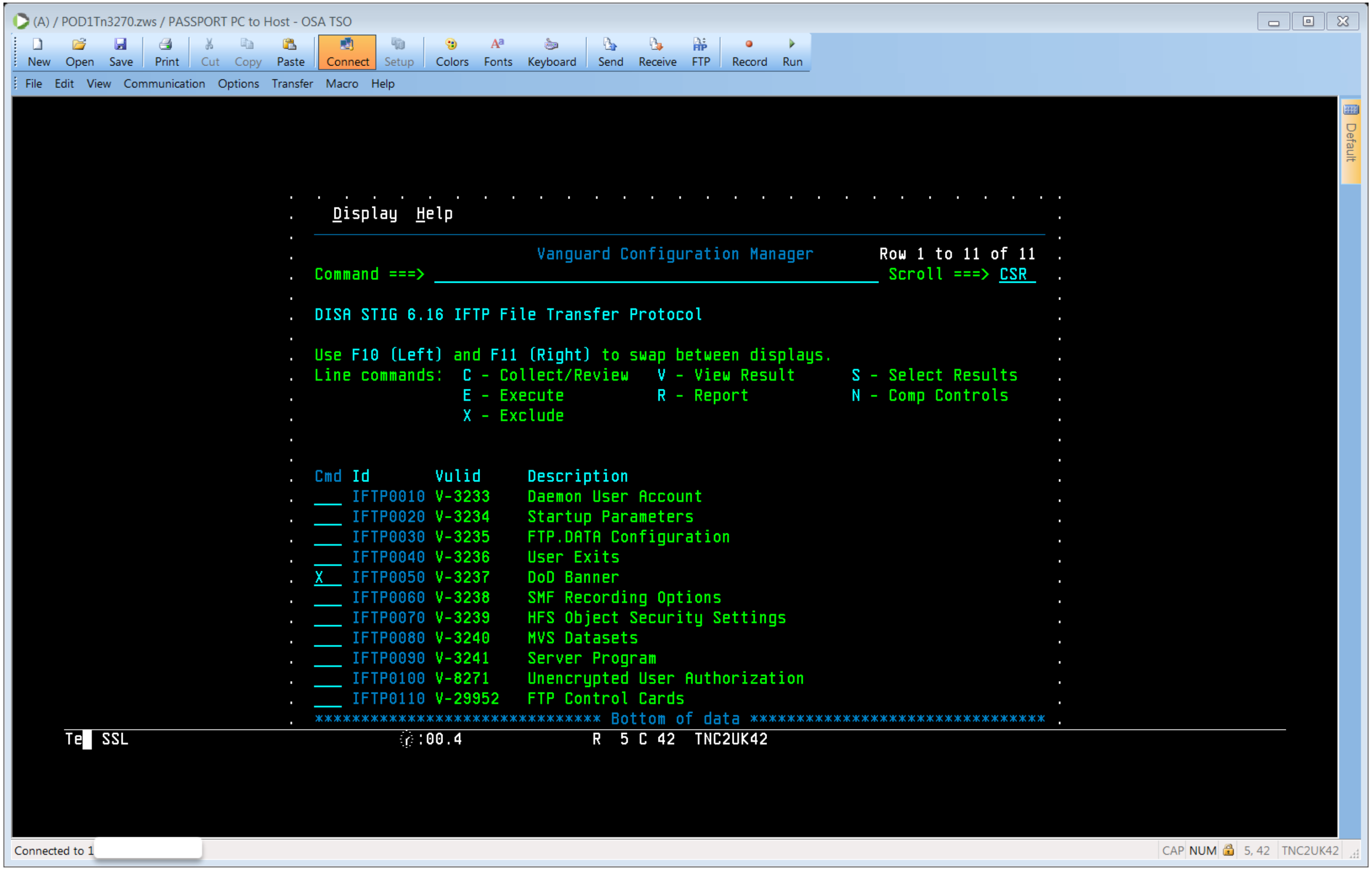
VCM Filters



```
  Batch  Reports  Jobcard  Display  Help
                             ┌─────────────────────┐
                         Var │ _  1. Sort...       │anager       Row 1 to 16 of 48
Command ===> _____________   │    2. Locate...     │_____________  Scroll ===> PAGE
                             │    3. Hide/Show Excluded │
DISA STIG 6.20               │    4. Hide/Show Commands │
                             └─────────────────────┘
Line commands:  S - Select category   R - Summary report   C - Comp Cntl report
                X - Exclude           V - CSV report

Cmd Prefix    Category Description
___ ACOM      Common Configuration
___ AAMV      z/OS Operating System Environment
___ ACP       Security Server (RACF) for z/OS system data
___ IFTP      File Transfer Protocol
___ ISLG      z/OS UNIX SYSLOG
___ ITCP      TCP/IP Communications Server
___ ITNT      TN3270 Telnet Server
___ IUTN      z/OS UNIX Telnet Server                              Excluded
___ RACF      Security Server (RACF) Settings
___ ZADT      CA Auditor                                           Excluded
___ ZAID      Compuware Abend-AID                                  Excluded
___ ZCA1      CA-1 (Tape Management System)
___ ZCCS      CA Common Services
___ ZCIC      CICS Transaction Server
___ ZCLS      CL/Supersession                                      Excluded
___ ZCSL      Catalog Solutions                                    Excluded
          :00.3                  R 12 C 28   TNC2HI23
```

Use the Display drop down menu to see what is currently removed from the category list.

VCM Filters

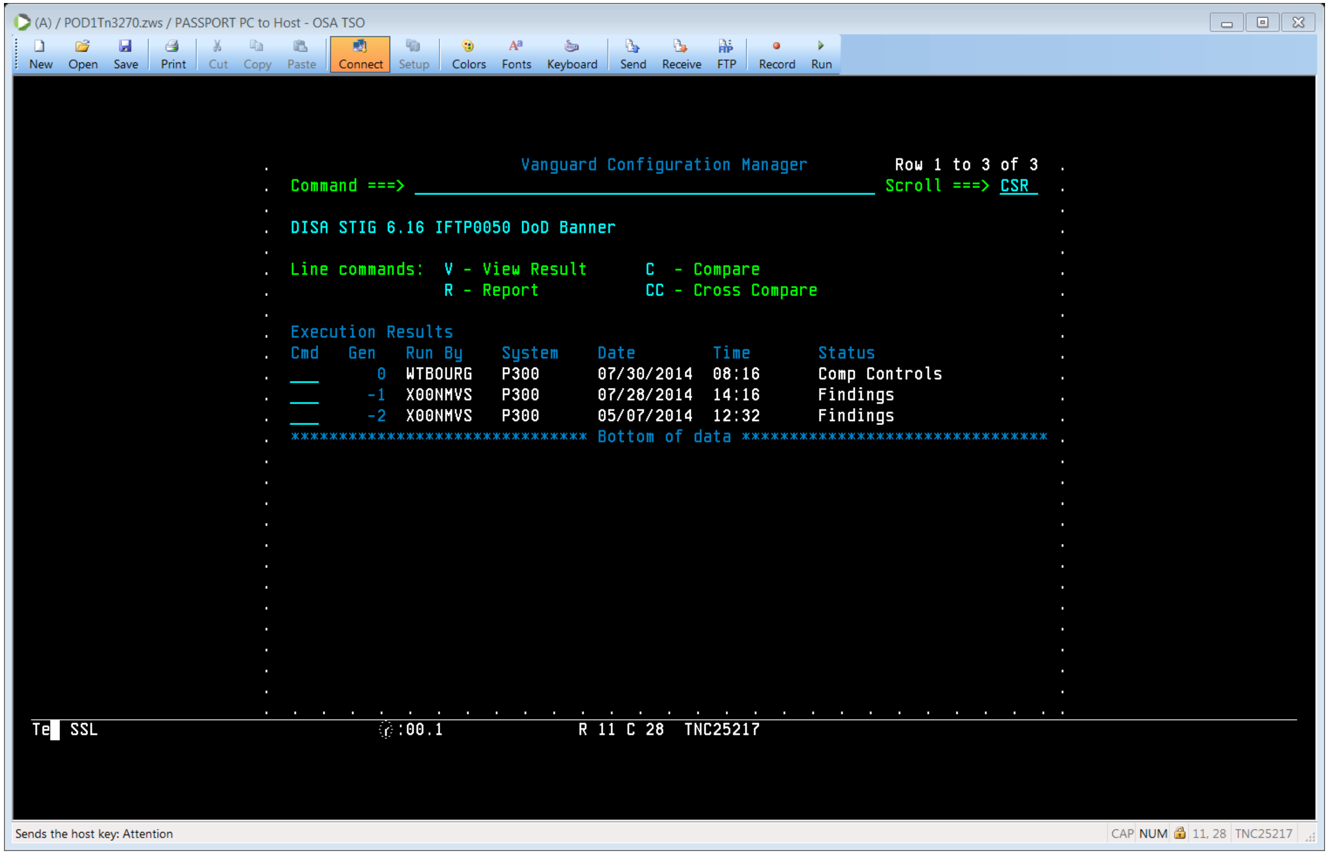


(A) / POD1Tn3270.zws / PASSPORT PC to Host - OSA TSO
New Open Save Print Cut Copy Paste Connect Setup Colors Fonts Keyboard Send Receive FTP Record Run
File Edit View Communication Options Transfer Macro Help
Default
Connected to 1
CAP NUM 5, 42 TNC2UK42

```
 Display  Help
 
                        Vanguard Configuration Manager        Row 1 to 11 of 11
 Command ===> ________________________________________________ Scroll ===> CSR_
 
 DISA STIG 6.16 IFTP File Transfer Protocol
 
 Use F10 (Left) and F11 (Right) to swap between displays.
 Line commands:  C - Collect/Review     V - View Result      S - Select Results
                 E - Execute            R - Report           N - Comp Controls
                 X - Exclude
 
 
 Cmd Id        Vulid     Description
 ___ IFTP0010 V-3233    Daemon User Account
 ___ IFTP0020 V-3234    Startup Parameters
 ___ IFTP0030 V-3235    FTP.DATA Configuration
 ___ IFTP0040 V-3236    User Exits
 X__ IFTP0050 V-3237    DoD Banner
 ___ IFTP0060 V-3238    SMF Recording Options
 ___ IFTP0070 V-3239    HFS Object Security Settings
 ___ IFTP0080 V-3240    MVS Datasets
 ___ IFTP0090 V-3241    Server Program
 ___ IFTP0100 V-8271    Unencrypted User Authorization
 ___ IFTP0110 V-29952   FTP Control Cards
 ****************************** Bottom of data ******************************
Te  SSL                 :00.4              R  5 C 42   TNC2UK42
```

X to exclude an individual check

VCM Compare



```
                        Vanguard Configuration Manager         Row 1 to 3 of 3
Command ===> ________________________________________________ Scroll ===> CSR

DISA STIG 6.16 IFTP0050 DoD Banner

Line commands:  V - View Result      C  - Compare
                R - Report           CC - Cross Compare

Execution Results
Cmd    Gen    Run By     System     Date          Time        Status
___      0    WTBOURG    P300       07/30/2014    08:16       Comp Controls
___     -1    X00NMVS    P300       07/28/2014    14:16       Findings
___     -2    X00NMVS    P300       05/07/2014    12:32       Findings
******************************* Bottom of data ********************************

Te  SSL                        :00.1                R 11 C 28   TNC25217
```

Sends the host key: Attention

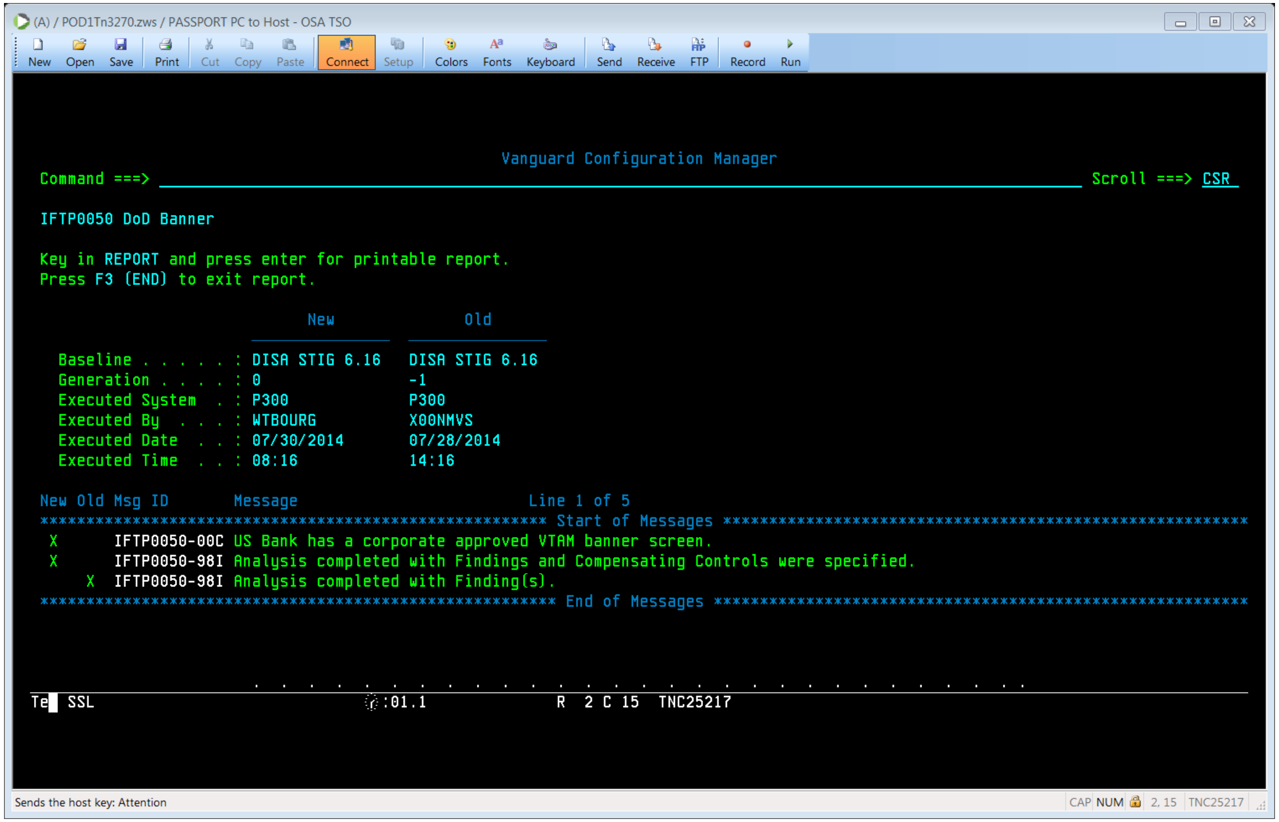
CAP NUM 11, 28 TNC25217

From main category list select using an S to get this panel

C is used to pick the new and old Gen to compare

CC is used for a cross stig level compare

Compare Results

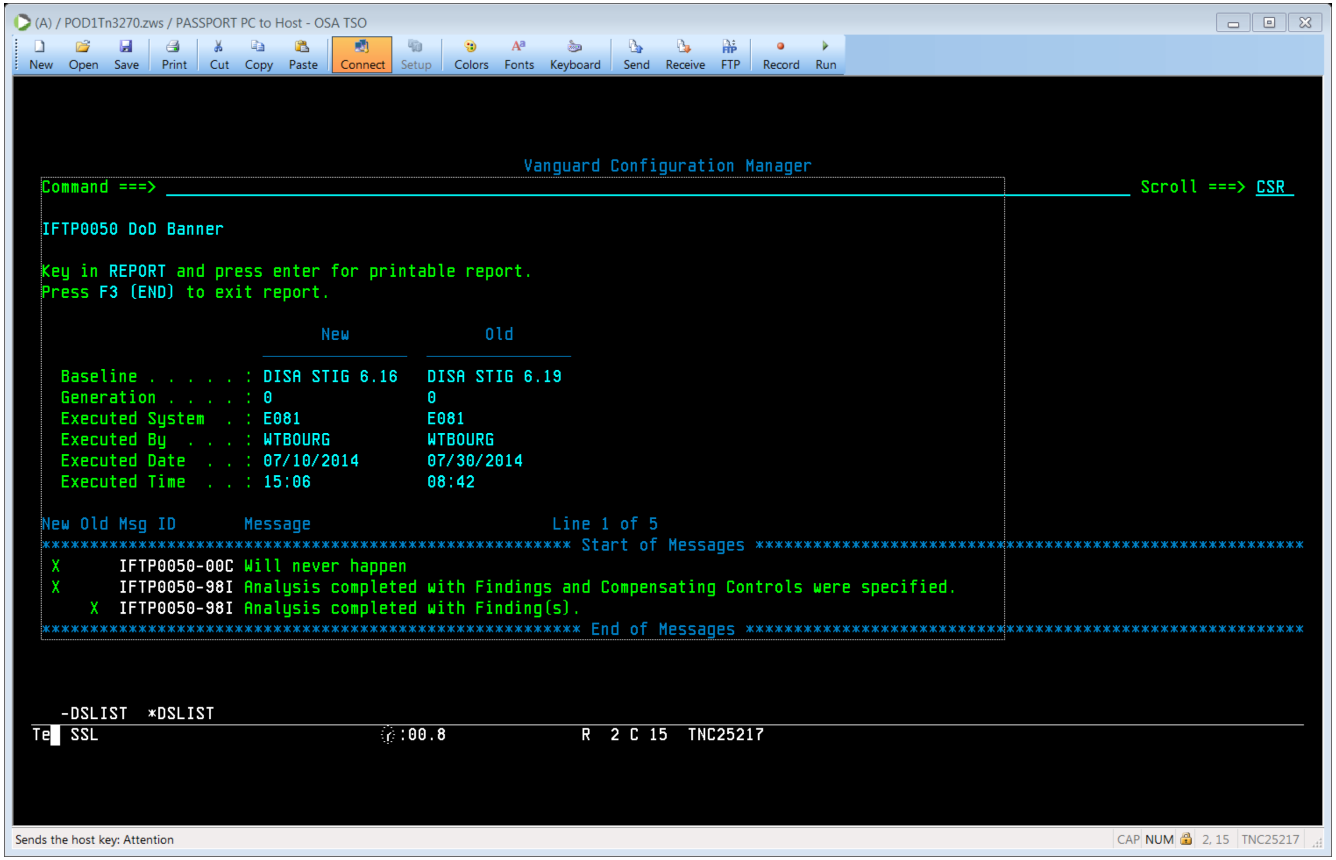


```
                                                  Vanguard Configuration Manager
Command ===> ____________________________________________________________________________________________________ Scroll ===> CSR

IFTP0050 DoD Banner

Key in REPORT and press enter for printable report.
Press F3 (END) to exit report.

                             New              Old
                       _______________  _______________
  Baseline . . . . . . : DISA STIG 6.16   DISA STIG 6.16
  Generation . . . . . : 0                -1
  Executed System  . . : P300             P300
  Executed By  . . . . : WTBOURG          X00NMVS
  Executed Date  . . . : 07/30/2014       07/28/2014
  Executed Time  . . . : 08:16            14:16

New Old Msg ID       Message                          Line 1 of 5
******************************************************* Start of Messages *********************************************************
 X      IFTP0050-00C US Bank has a corporate approved VTAM banner screen.
 X      IFTP0050-98I Analysis completed with Findings and Compensating Controls were specified.
     X  IFTP0050-98I Analysis completed with Finding(s).
******************************************************** End of Messages **********************************************************

Te█ SSL                              :01.1             R  2 C 15  TNC25217
```

Sends the host key: Attention

CAP NUM 2, 15 TNC25217

Cross STIG Level Compare



```
                                                  Vanguard Configuration Manager
Command ===> ________________________________________________________________________________________________ Scroll ===> CSR_

IFTP0050 DoD Banner

Key in REPORT and press enter for printable report.
Press F3 (END) to exit report.

                             New              Old
                       _______________  _______________
  Baseline . . . . . . : DISA STIG 6.16   DISA STIG 6.19
  Generation . . . . . : 0                0
  Executed System  . . : E081             E081
  Executed By  . . . . : WTBOURG          WTBOURG
  Executed Date  . . . : 07/10/2014       07/30/2014
  Executed Time  . . . : 15:06            08:42

New Old Msg ID        Message                         Line 1 of 5
******************************************************* Start of Messages *********************************************************
 X      IFTP0050-00C Will never happen
 X      IFTP0050-98I Analysis completed with Findings and Compensating Controls were specified.
     X  IFTP0050-98I Analysis completed with Finding(s).
******************************************************** End of Messages **********************************************************


  -DSLIST  *DSLIST
Te▌ SSL                                  :00.8            R  2 C 15  TNC25217
```

Sends the host key: Attention

CAP NUM 2, 15 TNC25217

More Information

- www.go2vanguard.com
- iase.disa.mil/stigs/

Stop by and visit us at Booth 607!