

UNCLASSIFIED



# **z/OS STIG INSTRUCTION**

Version 6 Release 22

20 January 2015

**Developed by DISA for the DoD**

---

UNCLASSIFIED

## TABLE OF CONTENTS

	Page
Data Collection .....	4
z/OS Data Collection Setup .....	4
z/OS Data Collection .....	25
ACF2 Data Collection .....	33
RACF Data Collection .....	37
TSS Data Collection .....	41
CA 1 Data Collection .....	49
CICS Data Collection .....	52
IBM Communications Server Data Collection .....	54
IDMS Data Collection .....	55
Integrated Operation Architecture (IOA) Data Collection .....	57
WebSphere MQ Data Collection .....	58
UNIX System Services Data Collection .....	59
Data Set and Resource Data Collection .....	62
ACF2 Data Set and Resource Data Collection .....	64
RACF Data Set and Resource Data Collection .....	66
TSS Data Set and Resource Data Collection .....	68
SRRDB Data Collection .....	69

## Summary of Changes

Changes for this release (Version 6, Release 22) since the previous version/release (Version 6, Release 21, dated 24 October 2014) are listed below.

### GENERAL:

- No changes.

## Data Collection z/OS Data Collection Setup

The following instructions will be used to collect information and data that will be used in the collection process in conducting the Security Readiness Review (SRR).

**NOTE:** *This document contains several references to the character strings 'xxxx' and 'mmmyyyy'. Throughout this document, replace all occurrences of:*

- 1) **xxxx** with the SYSNAME specified in the IEASYSxx member in the logical parmlib concatenation.
- 2) **mmmyyyy** with the month and year of the review, e.g., MAR1997.

**NOTE:** *This document contains several references to the character strings 'VxRxx' and 'Vvrr':*

**VxRxx** refers to Version and Release of the z/OS STIG Instruction. (e.g. V5R12)  
**Vvrr** refers to Version and Release of the z/OS STIG Instruction. (e.g. V512)

The data gathered will be saved in the following partitioned data sets:

- 1) **SYS3.FSO.xxxx.mmmyyyy.CNTL** - Script, JCL, and Tables
- 2) The data set that contains the information collected in the z/OS SRRAUDIT Dialog Management Procedures.

These permanent data sets must be located on a domain accessible to the reviewing personnel and will be required for follow-up SRR data analysis. The data sets should be backed up and retained by the site for future reference.

A copy of the z/OS STIG Instruction should be provided to the site prior to the start of the SRR process.

---

\_\_\_ **1. Process to be run for Sites running SRRAUDIT**

\*\*\*\*\* **If not running SRRAUDIT skip this step and go on to Step 2** \*\*\*\*\*

- \_\_\_ a) Edit **SYS2.SRRAUDIT.CNTL(CACJAUFU)**.

Replace the JOB card with a valid JOB card.

Change *xxxx* and *mmmyyyy* in the SRRHLQ variable as follows

- 1) *xxxx* with the *SYSNAME* specified in the *IEASYSxx* member in the logical *parmlib* concatenation.
- 2) *mmmyyyy* with the month and year of the review, e.g., *MAR1997*.

- \_\_\_ b) Submit **CACJAUFU** for execution. CACJAUFU job Creates and copies members from the SRRAUDIT libraries to SYS3.FSO libraries. This job prepares the information for a full review to be performed after completing the SRRAUDIT Process.
- \_\_\_ c) Skip to Step 5

\_\_\_ 2. Upload the files located in FOUO\_zOS\_VxRxx\_yyyymmdd.zip to the host.

- \_\_\_ a) Allocate two (2) partitioned data sets on the host.

Using ISPF/PDF data set utilities or an equivalent program, allocate the following data sets with the indicated characteristics:

**SYS3.FSO.Vvrr.JCL** - Batch restore JCL data set.

Organization:**PO**  
Record format:**FB**  
Record length:**80**  
Block size:**6160** (suggested)  
Primary tracks:**1**  
Secondary tracks:**1**  
Directory blocks:**1**

**SYS3.FSO.xxxx.mmmyyyy.PARMLIB** - Copies of system parmlib members

Organization:**PO**  
Record format:**FB**  
Record length:**80**  
Block size:**6160** (suggested)  
Primary tracks:**2**  
Secondary tracks:**1**  
Directory blocks:**5**

- \_\_\_ b) Using any 3270 Terminal Host Emulation or File Transfer Protocol software, establish a host connection:

- \_\_\_ 1) Perform a **Text** transfer of **RESTJCL.txt** to **SYS3.FSO.Vvrr.JCL(RESTJCL)**. Ensure that Transfer Options are set to **ASCII CRLF**.
- \_\_\_ 2) Perform a **Binary** transfer of **VxRxx.DUMP.xmi** to create **SYS3.FSO.Vvrr.DUMP.XML**. Ensure that Transfer Options are set to the following:

**RECFM(F) BLKSIZE(6160) LRECL(80) SPACE(75 15) TRACKS**

---

\_\_\_ **3. Submit RESTJCL to receive and restore data sets**

- \_\_\_ a) Edit **SYS3.FSO.Vvrr.JCL(RESTJCL)** and perform the following:
- 1) Replace the JOB card with a valid JOB card.
  - 2) Make changes specified in the JCL comments.
  - 3) Make changes to the UNIT and VOLUME entries for the RECEIVE in STEP1.
- \_\_\_ b) Submit **RESTJCL** for execution. This JOB will receive and restore data sets used in the Data Collection Process. Review the job for error messages to ensure successful execution, particularly the following:
- \_\_\_ 1) The ISPLOG and SYSTSPRT files of each report step.
- \_\_\_ 2) The JOBLOG or JESLOG files.

The **RESTJCL** job will create the following data sets:

**SYS3.FSO.Vvrr.DUMP**  
**SYS3.FSO.xxxx.mmmyyyy.CNTL**  
**SYS3.FSO.xxxx.mmmyyyy.EXAM.SCRIPT**  
**SYS3.FSO.xxxx.mmmyyyy.LOADLIB**

- \_\_\_ c) Upon successful completion and creation of the above data sets, the following data set may be deleted:

**SYS3.FSO.Vvrr.DUMP**  
**SYS3.FSO.Vvrr.DUMP.XMI**  
**SYS3.FSO.Vvrr.JCL**

#### \_\_\_ 4. Customize CA Auditor report options.

Invoke the CA Auditor (formally known as CA Examine) application from within ISPF/PDF. This is typically done by executing **%EXAMINE** from ISPF/PDF option 6.

From the CA Auditor primary menu, enter **0.3** from the command line to display the **SELECT REPORT OPTIONS** menu. Enter the following values:

Page header:	<b>SRR - site name - xxxx</b>
Maximum lines per page:	<b>55</b> (suggested)
Report destination:	<b>LOCAL</b>
Sysout class:	<b>X</b> (must be a JES held output class)
Upper case:	<b>YES</b> (suggested)
Allocated hold:	<b>YES</b>

After all the information is entered, press the **ENTER** key to save the values and return to the CA Auditor primary menu.

**NOTE:** *If the **PF3** key or the **END** command is issued, the report option values will not be saved.*



---

**5. Verify that Dialog Dataset is populated.**

**NOTE:** Review the instructions in the z/OS SRRAUDIT Dialog Management Procedures.

- \_\_\_ a) Verify the Authorized User Groups are complete.

**NOTE:** For sites to determine if the SRRAUDIT process is installed, review data sets that have the high level qualifiers of SYS2.SRRAUDIT and SYS3.SRRAUDIT. The symbolic SRRAUL will be data set SYS3.SRRAUDIT.DATA. *The members in this data set should be evaluated to verify that the contents are correct.* This data set should contain the following members:

APPDAUDT	APPSAUDT	AUDTAUDT	AUTOAUDT
BMCADMIN	BMCUSER	CHGOWNER	CICBAUDT
CICDAUDT	CICSAUDT	CICSDEF	CICUAUDT
CONSOLES	DABAAUDT	DAEMAUDT	DASBAUDT
DASDAUDT	DPCSAUDT	DUMPAUDT	EMERAUDT
FTPUSERS	MICSADM	MICSUSER	MQSAAUDT
MQSDAUDT	MVREAD	MVUPDT	OMVSAUDT
OPERAUDT	PARMSTC	PCSPAUDT	PRODAUDT
SECAAUDT	SECBAUDT	SECDAUDT	SERVAUDT
SMFBAUDT	STCGAUDT	SUPRAUDT	SYSCAUDT
SYSPAUDT	TAPEAUDT	TSTCAUDT	WEBAAUDT

- \_\_\_ b) Ensure that all Products are identified.
- \_\_\_ c) Ensure that all IAVMs are applicable to the system.
- \_\_\_ d) Ensure that all Vulnerability Questions are answered.
- \_\_\_ e) Ensure that the VMS Asset Creation Process is completed to provide the scripts with the Classification of the system being reviewed.

\_\_\_ 6. Resources that may be required for Auditor.

- \_\_\_ a) Review the following table for possible resource that the Auditor may require. This table includes resources for specific products.

Product	Resource Class	Resource	Access	Logging
General	DATASET	System level data sets	READ	As Required
General	DATASET	Data sets created by the jobs in this document	ALTER	No
General	TSOAUTH	CONSOLE	READ	No
General	TSOAUTH	PARMLIB	READ	No
General	OPERCMDS	MVS.DISPLAY	READ	No
General	OPERCMDS	MVS.MCSOPER.*	READ	No
General	OPERCMDS	JES2.DISPLAY	READ	No
General	SERVAUTH	EZB.STACKACCESS		
SDSF	OPERCMDS	MVS.MODIFY.STC.SDSF	UPDATE	Yes
SDSF	OPERCMDS	SDSF.MODIFY.DISPLAY	READ	No
SDSF	SDSF	ISFOPER.SYSTEM	READ	No
SDSF	SDSF	ISFCMD.ODSP.ULOG	READ	No
WebSphere MQ	PROGRAM	CSQUTIL	EXECUTE	No
WebSphere MQ	MQCONN	ssid.BATCH	READ	No
WebSphere MQ	MQCMD	ssid.DISPLAY.	READ	No
WebSphere MQ	MQQUEUE	ssid.SYSTEM.COMMAND.INPUT	UPDATE	No
WebSphere MQ	MQQUEUE	ssid.SYSTEM.COMMAND.REPLY	UPDATE	No
WebSphere MQ	MQQUEUE	ssid.SYSTEM.CSQUTIL.-	UPDATE	No
Unix System Services	UNIXPRIV	SUPERUSER.FILESYS	READ	No
Unix System Services	FACILITY	BPX.SUPERUSER	READ	No
CA Auditor	FACILITY	CSVDPYNEX.LIST	READ	No
CA Auditor	PROGRAM	LTDMMMAIN	EXECUTE	No

---

**7. Modify members in SYS3.FSO.xxxx.mmmmyyy.CNTL.****a) Customize JCL member JOBCARD.**

- 1) Change JOB card statement to reflect a valid JOB card for the site.
- 2) Change **XXXX** to reflect the current SYSNAME specified in the IEASYSxx member.
- 3) Change **MMMYYYY** to reflect the current month and year.
- 4) Optional approach, change **XXXX.MMMYYYY** to any identifiable qualifiers for the data sets created in this process.

**b) Review the JCL, edit, and make changes where necessary to the member EXAMRPTS. Change the variables to reflect the current SYS3.FSO.xxxx.mmmmyyy.CNTL and the data set used to run CA-Examine. The following are the current defaults:**

```

CNTL=SYS2.SRRAUDIT.CNTL
CAILIB=SYS2A.EXAMINE.CAILIB
CAICLIB=SYS2.EXAMINE.CAICLIB
CAIISPP=SYS2.EXAMINE.CAIISPP
CAIISPM=SYS2.EXAMINE.CAIISPM
CAIISPT=SYS2.EXAMINE.CAIISPT
CAIDBS1=SYS3.EXAMINE.CAIDBS1
CAIDBS2=SYS2.EXAMINE.CAIDBS2

```

Change any of the above entries to reflect the correct data sets.

**c) Customize member STCILIST. The member contains the identifier and the STC/Job name list. Review all STCs and Jobs that are currently running on the system to determine if the STCs or Jobs can be used to collect data sets that queued to the STC/Job. The identifier can be repeated for each STC/Job that falls into the identifier type process. The following example is for four (4) CICS regions:**

CA CICSJ1	CICS	ZCICR010	ZCICT010	ZCICA010
CA DFHSTART	CICS	ZCICR010	ZCICT010	ZCICA010
CA CICST1	CICS	ZCICR010	ZCICT010	ZCICA010
CA CICSPI	CICS	ZCICR010	ZCICT010	ZCICA010

\_\_\_ 8. Modify the list of data set entries for the DSNLIST member.

- \_\_\_ a) The **DSNLIST** member is used as input into the Sensitive Reporting Subsystem. Before the Sensitive Reports are produced, duplicate elimination is performed to ensure that data sets are only referred once within the **SENSITIVE.RPT** PDS report members. The duplicate elimination process occurs after **all** input is processed, which includes this **DSNLIST** member and automatic extracts from numerous CA Auditor (formally known as CA Examine) and ACP reports.

Edit **SYS3.FSO.xxxx.mmmmyyyy.CNTL(DSNLIST)** to create a list of system and product data set entries using the following guidelines and table. The suggestions following the table will help determine the proper data set names to use.

- 1) Use a two-character identifier to indicate the type of data set entry.
- 2) The same identifier can be repeated as often as necessary.
- 3) Data set entries must be a fully qualified data set name.
- 4) All identifiers must begin in Column 1.
- 5) All data set entries must begin in Column 4.
- 6) Do not use quotes with the data set entry.

This table includes a list of valid data set identifiers, the type of data set entry associated with each identifier, and the member name of the report saved in the **SENSITIVE.RPT** PDS.

**NOTE:** *The identifier codes followed by a footnote are **optional** input into the **DSNLIST**. The Sensitive Reporting process generates these entry types automatically. Unless you have a special circumstance, you do not need to code these entries in the **DSNLIST**.*

## UNCLASSIFIED

z/OS STIG Instruction, V6R22  
20 January 2015

DISA Field Security Operations  
Developed by DISA for the DoD

<b>Identifier Code</b>	<b>Dataset Group</b>	<b>Report Name</b>	<b>Note</b>
AA	SYS1.PARMLIB (Logical Parmlib data sets)	PARMRPT	<sup>1</sup>
AB	SYS1.LINKLIB	LINKRPT	<sup>2</sup>
AC	SYS1.SVCLIB	SVCRPT	<sup>2</sup>
AD	SYS1.IMAGELIB	IMAGERPT	<sup>2</sup>
AE	SYS1.LPALIB	LPARPT	<sup>2</sup>
AF	SYS1.NUCLEUS	NUCLRPT	<sup>2</sup>
AG	SYS1.UADS	UADSRPT	<sup>3</sup>
AH	SYS1.DUMP	DUMPRPT	<sup>3 4</sup>
AI	SYS1.TRACE	TRACERPT	<sup>2 4</sup>
BA	APF-authorized	APFXRPT	<sup>5</sup>
BB	LINKLIST	LNKXRPT	<sup>5</sup>
BC	LPA	LPAXRPT	<sup>5</sup>
BD	Libraries containing PPT modules	PPTXRPT	<sup>5</sup>
BE	Libraries containing system exits	MVSXRPT	<sup>5</sup>
BF	TSO APF-authorized	APFTRPT	<sup>5</sup>
BG	SMF collection (i.e., SYS1.MAN)	SMFXRPT	<sup>3 5</sup>
BH	JES2 procedures	PROCRPT	<sup>3 6</sup>
BI	Master System catalog	CATMRPT	<sup>3</sup>
BJ	System User catalogs	CATURPT	<sup>3 5</sup>
BK	SMP/E installation (i.e., CSIs)	SMPERPT	<sup>5</sup>
BL	System PAGE	PGXXRPT	<sup>3</sup>
BM	JES2 System data sets	JES2RPT	<sup>5</sup>
BN	SMF dump/backup	SMFBKRPT	<sup>4 7</sup>
BO	System DASD backup	BKUPRPT	<sup>4 7</sup>
BP	ACP and security-related	ACPRPT	<sup>3 8</sup>
BQ	System-level product installation	PRODRPT	
BR	FDR Installation Datasets	FDRRPT	<sup>7</sup>
BS	IBM Health Checker STC Datasets	HCKSTC	<sup>7</sup>
C1	CA VTape Installation Datasets	VTAPERPT	<sup>7</sup>
C2	BMC MAINVIEW for z/OS STC Datasets	MVZSTC	<sup>7</sup>
C3	BMC MAINVIEW for z/OS Installation Datasets	MVZRPT	<sup>7</sup>
C4	Compuware Abend-Aid STC Datasets	AIDSTC	<sup>7</sup>
C5	Compuware Abend-Aid Installation Datasets	AIDRPT	<sup>7</sup>
C6	CA MIM STC Datasets	MIMSTC	<sup>7</sup>

<sup>1</sup> SYS1.PARMLIB and/or Logical Parmlib obtained from System Control Blocks that are set during an IPL.

<sup>2</sup> Datasets are hard coded within the script.

<sup>3</sup> Datasets obtained from commands and/or System Control Blocks available to the system.

<sup>4</sup> Additional datasets can be obtained from detailed instructions.

<sup>5</sup> The datasets for this group are obtained from SYS3.FSO.xxxx.mmmmyyy.EXAM.RPT data set.

<sup>6</sup> The datasets for this group are obtained from the STC's JCL.

<sup>7</sup> Datasets obtained from information requested in the Dialog Process.

<sup>8</sup> Datasets obtained from Product reports.

<b>Identifier Code</b>	<b>Dataset Group</b>	<b>Report Name</b>	<b>Note</b>
C7	CA MIM Installation Datasets	MIMRPT	7
C8	CA MICS User Datasets	MICSUSER	7
C9	CA MICS Installation Datasets	MICSRPT	7
CA	CICS STC Datasets	CICSSTC	47
CB	FEP/NCP	NCPRPT	47
CC	VTAM	VTAMRPT	47
CD	NC-PASS STC Datasets	NCPASSTC	47
CE	UNIX HFS Files	HFSRPT	3
CF	UNIX System Services	USSRPT	
CG	UNIX STEPLIBLIST	STLLRPT	3
CH	CL/SuperSession STC datasets	KLSSTC	7
CI	DFSMS	SMSRPT	
CJ	CA 1 (TMC, AUDIT, and optional RDS and VPD datasets)	CA1RPT	478
CK	IDMS	IDMSRPT	
CL	WebSphere MQ	MQSRPT	
CM	TCPIP	TCPRPT	
CN	CA Auditor (CA Examine) User Datasets	ADTUSER	7
CO	CA Auditor (CA Examine) Installation Datasets	ADTRPT	7
CP	HTTP	HTTPRPT	
CQ	CICS Installation Datasets	CICSRPT	47
CR	FTP	FTPRPT	
CS	WebSphere Application Service	WASRPT	
CT	SDSF	ISFRPT	
CU	HASPINDEX	SDSFRPT	
CV	NETVIEW STC Datasets	NETVSTC	7
CW	NETVIEW Installation Datasets	NETVRPT	7
CX	TADz STC Datasets	TADZSTC	7
CY	TADz Installation Datasets	TADZRPT	7
CZ	CA VTape STC Datasets	VTAPESTC	7
D0	CONTROL-M/Restart Installation/Operations Datasets	CTRRPT	7
D1	CONTROL-O User Datasets	CTOSTC	7
D2	CONTROL-O Install/Operations Datasets	CTORPT	7
DA	CA-1 Installation Datasets	CA1PROD	47
DB	Catalog Solution Installation Datasets	CSLPROD	47
DC	CL/SuperSession Installation Datasets	KLSRPT	47
DD	NC-PASS Installation Datasets	NCPASRPT	7
DE	SRRAUDIT User Datasets	SRRUSER	7
DF	SRRAUDIT Installation Datasets	SRRPROD	7
DG	ROSCOE STC Datasets	ROSCSTC	7
DH	ROSCOE Installation Datasets	ROSCRPT	7
DI	TDMF Installation Datasets	TDMFRPT	7
DJ	VSS User Datasets	VSSUSER	7
DK	VSS Installation Datasets	VSSRPT	7
DL	HCD User Datasets	HCDUSER	7
DM	HCD Installation Datasets	HCDRPT	7
DN	ICSF STC Datasets	ICSFSTC	7

<i>Identifier Code</i>	<i>Dataset Group</i>	<i>Report Name</i>	<i>Note</i>
DO	ICSF Installation Datasets	ICSFRPT	7
DP	INCONTROL (IOA) User Datasets	IOAUSER	7
DQ	INCONTROL (IOA) STC Datasets	IOASTC	7
DR	INCONTROL (IOA) Installation Datasets	IOARPT	7
DS	CONTROL-D User Datasets	CTDUSER	7
DT	CONTROL-D STC Datasets	CTDSTC	7
DU	CONTROL-D Installation Datasets	CTDRPT	7
DV	CONTROL-M User/Application JCL Datasets	CTMJCL	7
DW	CONTROL-M User Datasets	CTMUSER	7
DX	CONTROL-M STC Datasets	CTMSTC	7
DY	CONTROL-M Installation Datasets	CTMRPT	7
DZ	CONTROL-M/Restart User Datasets	CTRUSER	7
EA	CA Common Services Installation Datasets	CCSRPT	7

**NOTE:** All references for dataset masks are used to collect dataset that may be associated with the Dataset Group. The list of datasets should be reviewed to ensure that the datasets collected are associated to the Dataset Group.

**Example:** The dataset mask of **\*\*.\*SMF\*** will collect all datasets that have a second, third, fourth, etc qualifier that contains SMF. Ensure that all datasets collected are associated to the SMF dump/backup data set type.

**Example:** Additional data set masks (such as **\*\*.\*BPX\***, **\*\*BPA\***, **\*\*CMX\***, **\*\*OMVS\***, **\*\*.\*FOM\***, **\*\*CTM\***, **\*\*CTO\***, **\*\*CTR\***, **\*\*.\*ECS\***, **\*\*.\*IOA\***.) are used to collect datasets associated with the Dataset Group. The list of datasets should be reviewed to ensure that the datasets collected are associated to the Executive software being reviewed and not datasets associated with a respective application.

➔ **SYS1.DUMP** - The **SYS1.DUMPxx** data set are automatically collected. Addition Dump data sets can be identified by reviewing the logical parmlib concatenation data sets for the current **COMMNDxx** member. Find the **COM=** which specifies the **DUMPDS NAME (DD NAME=name-pattern)** entry, the name-pattern is used to identify additional Dump data sets. Another option to obtain the name-pattern is to issue the **D D,ST MVS** command under SDSF.

➔ **SYS1.TRACE** - The **SYS1.TRACE** data set is collected in this process. Addition Trace data set can be obtained by a search of the JES2 proclibs for the member that executes program **AHLGTF**, **HHLGTF**, and **IHLGTF**. Obtain the data set specified in the **IEFRDER DD** statement.

➔ **SMF dump/backup** - Determine the names of the automated procedures used to dump the SMF data sets by reviewing **SYSLOG** messages. Review

these procedures in the JES2 proclibs for the data sets created. Use ISPF/PDF option 3.4 data set name list to enter **\*\*.\*SMF\***, or replace **SMF** with the *actual domain SMF ID (DAILY, WEEKLY, etc.)*.

➔ System DASD backup - If DFHSM is used, review the **DFHSM** procedure and note the **CMD=xx** parameter on the EXEC statement. Browse the **ARCCMDxx** member of the data set allocated by the **HSM Parm DD** statement for the entries **BACKUPPREFIX(prefix)** and **MIGRATEPREFIX(prefix1)**. The system backup data set names will be **prefix.BACKTAPE.DATASET** and **prefix1.HMIGTAPE.DATASET**.

If FDR is used, use **FDRABR.** for the data set prefix.

➔ System-level product installation - SMP/E target and distribution data sets, and non-SMP/E installation data sets.

***NOTE:** SMP/E CSI data sets are automatically included in the **SMPERPT** report.*

➔ CICS STC Datasets - Review **EXAM.RPT(CICS PROC)**. CICS system data set names are identified by DD names beginning with **DFH**. These data sets are data sets that are maintained by the CICS STC and/or batch job and the system programming personnel. Use ISPF/PDF option 3.4 data set name list (e.g., **\*\*.\*CICS\***) to obtain a comprehensive list of CICS STC data sets, these data sets are referenced in proclib members or the CICS batch JCL.

➔ FEP/NCP - Search the JES2 proclibs for the member that executes program **ISTINM01**. These data sets are used for the FEP at the site, if the domain does not have a FEP the collection of these data sets can be bypassed. Review the VTAM procedure for load and dump data sets for the FEP. Use ISPF/PDF option 3.4 data set name list to enter **\*\*.\*NCP\***, this can be used to obtain the **NCP** system, **NCP** source definition, **NCP** load modules, **NCP** host dump, and **NCP** utility programs data sets.

➔ VTAM – Review the **VTAM** procedures, and search the JES2 proclibs for the member that executes program **ISTINM01**. Obtain data set names containing all VTAM start options, configuration lists, network resource definitions, commands, procedures, exit routines, all SMP/E TLIBs, and all SMP/E DLIBs used for installation and in development/production VTAM environments. Use ISPF/PDF option 3.4 data set name list to enter **\*\*.\*VTAM\***.

➔ NC-PASS STC Datasets – Search the JES2 proclibs for the member that executes program **NCI**. Use ISPF/PDF option 3.4 data set name list to enter **\*\*.\*NCPASS\***. These data sets are updated and maintained by the NC-PASS STC.

➔ UNIX HFS Files – Review the **BPXPRMxx** members in PARMLIB for the **ROOT** and **MOUNT** statements. Include the data set specified in the



FILESYSTEM parameter. Current information can be obtained from the *df* Unix command.

➔ UNIX System Services Product Data Sets – Use ISPF/PDF option 3.4 data set name list to enter **\*\*.\*BPX\***, **\*\*.\*BPA\***, **\*\*.\*CMX\***, **\*\*.\*OMVS\***, and **\*\*.\*FOM\***.

➔ UNIX STEPLIBLIST – Review the **BPXPRMxx** members in PARMLIB for the **STEPLIBLIST** statement. This statement specifies the name of the HFS file (usually /etc/steplib) that contains the list of data sets to be used as step libraries authorized for set-user-ID and set-group-ID programs. Review the USSCMDS.RPT(ESTEPLL) report or the TSO command “**oshell cat /etc/steplib**” to get the list of data sets to include. If the STEPLIBLIST statement is commented out, there are no data sets to include.

➔ CL/SuperSession STC Datasets – Review the CL/SuperSession **KLS** procedure, and search the JES2 proclibs for members that execute programs with prefixes of **MVP** and **EZA**. Use ISPF/PDF option 3.4 data set name list to enter **\*\*.\*OMEG\***. These data sets are updated and maintained by the CL/SuperSession STC.

➔ DFSMS – Review **IGDSMSxx** members in **SYS1.PARMLIB** to obtain the ACDS and COMMDS data set names. Use the prefixes of these data sets to obtain the SCDS, ACS routine, and any backup data set names. Use ISPF/PDF option 3.4 data set name list to enter **\*\*.\*DFSMS\***.

➔ CA 1 (TMC, AUDIT, and optional RDS and VPD datasets) – The TMC and Audit data sets can be obtained from **CA1.RPT(TMSSTATS)**. Please note that this report has not been generated at this time.

➔ IDMS – Search the JES2 proclibs for members that execute program **IDMSDC**.

➔ WebSphere MQ – Search the JES2 proclibs for members that execute programs with the prefix of **CSQ**. Review proclib members for *ssidMSTR* and *ssidCHIN*. Additional data sets can be found by reviewing the *ssidMSTR* JESMSG LG. Find **CSQJ001I** messages to obtain the LOGCOPY data sets. Find the **CSQY122I** message to obtain the **ARCPRFX1** and **ARCPRFX2** data set high-level qualifiers. Use ISPF/PDF option 3.4 data set name list to enter **\*\*.\*MQ\***.

➔ TCP/IP - Review the **TCPIP** procedures, and search the JES2 proclibs for members that execute programs with prefixes of **MVP** and **EZA**. Use ISPF/PDF option 3.4 data set name list to enter **\*\*.\*TCP\*** and **SYS1.TCPIP.SEZ\***. The prefixes of the product data sets begin with **SYS1.TCPIP.AEZA**, and **SYS1.TCPIP.SEZA**.

- ➔ **INCONTROL (IOA) Installation Datasets** – Obtain the BASEPREF, ILPREFA, SPAPREF, SPCPREF, SPCPREFD, SPCPREFT, and SPDPREF variables, these variables contain the dataset prefixes for these data sets. These variables can be found within the INCONTROL Installation and Customization Engine (ICE) process.
- ➔ **INCONTROL (IOA) STC Datasets** – Obtain the OLPREFA variable, this variable contain the dataset prefix for these data sets. This variable can be found within the INCONTROL Installation and Customization Engine (ICE) process.
- ➔ **INCONTROL (IOA) User Datasets** – Obtain the DBPREFA variable, this variable contain the dataset prefix for these data sets. This variable can be found within the INCONTROL Installation and Customization Engine (ICE) process.
- ➔ **CONTROL-D Installation Datasets** – Obtain the ILPREFD variable, this variable contain the dataset prefix for these data sets. This variable can be found within the INCONTROL Installation and Customization Engine (ICE) process.
- ➔ **CONTROL-D STC Datasets** – Obtain the OLPREFD variable, this variable contain the dataset prefix for these data sets. This variable can be found within the INCONTROL Installation and Customization Engine (ICE) process.
- ➔ **CONTROL-D User Datasets** – Obtain the DBPREFD, AMPREF, AMPREFD, and JB1PREF variables, these variables contain the dataset prefixes for these data sets. These variables can be found within the INCONTROL Installation and Customization Engine (ICE) process.
- ➔ **CONTROL-M Installation Datasets** – Obtain the ILPREFM variable, this variable contain the dataset prefix for these data sets. This variable can be found within the INCONTROL Installation and Customization Engine (ICE) process.
- ➔ **CONTROL-M STC Datasets** – Obtain the OLPREFM variable, this variable contain the dataset prefix for these data sets. This variable can be found within the INCONTROL Installation and Customization Engine (ICE) process.
- ➔ **CONTROL-M User Datasets** – Obtain the DBPREFM variable, this variable contain the dataset prefix for these data sets. This variable can be found within the INCONTROL Installation and Customization Engine (ICE) process.
- ➔ **CONTROL-M User/Application JCL Datasets** – Obtain a list of User/Application JCL datasets by reviewing Job the DBPREFD, AMPREF, AMPREFD, and JB1PREF variables, these variables contain the dataset

prefixes for these data sets. These variables can be found within the INCONTROL Installation and Customization Engine (ICE) process.

➔ HTTP – Review the **HTTP** procedures, and search the JES2 proclibs for members that execute program **IMWHTTPD**. Use ISPF/PDF option 3.4 data set name list to enter **SYS1.IMW**.

➔ CICS Installation Datasets - Review **EXAM.RPT(CICSPROC)**. CICS system data sets that are maintained by the system programming personnel. These datasets include the CICS SIT allocated by the **SYSIN** DD statement. Use ISPF/PDF option 3.4 data set name list (e.g., **\*\*.\*CICS\***) to obtain a comprehensive list of CICS Installation data sets, including installation data sets not referenced in proclib members.

***NOTE:** The libraries allocated by the **STEPLIB** DD statement are APF-authorized and are automatically included in the **APFXRPT** report.*

➔ FTP – Review the **FTPD** procedure, and search the JES2 proclibs for members that execute programs with prefix of **FTP**. Review the data set allocated to the **SYSFTPD** DD statement in the **FTPD** procedure for the **BANNER** entry that is identified to a data set.

➔ WebSphere Application Service – Use ISPF/PDF option 3.4 data set name list to enter **SYS2.WAS\***, **SYS2.OE**, **SYS2.EJS**, **SYS1.JAVA**, **SYS1.DB2**, and **SYS1.GLD**. And data sets **SYS1.CSSLIB**, **SYS1.LE.SCEELKED**, **SYS1.LE.SCEELKEX**, and **SYS1.LE.SCEE OBJ**.

➔ SDSF – Use ISPF/PDF option 3.4 data set name list to enter **SYS1.ISF\***. Review the **SDSF** procedure, and search the JES2 proclibs for members that execute program **ISFHCTL**. Review the data set allocated to the **SDSFARM** DD statement.

➔ HASPINDEX –Review the **SDSF** procedure, and search the JES2 proclibs for members that execute program **ISFHCTL**. Review the data set allocated to the **SDSFARM** DD statement, member **ISFPRMxx**. The data set is identified in the **INDEX** control statement.

➔ CA 1 Installation datasets – Search the JES2 proclibs for the member that executes program **TMSINIT**. Use ISPF/PDF option 3.4 data set name list to enter **\*\*.\*CA1\*** and **\*\*.\*TMS\***.

➔ Catalog Solution Installation datasets – Use ISPF/PDF option 3.4 data set name list to enter **SYS2.CSL**.

➔ CL/SuperSession Installation Datasets – Review the CL/SuperSession **KLS** procedure, and search the JES2 proclibs for members that execute

programs with prefixes of **MVP** and **EZA**. Use ISPF/PDF option 3.4 data set name list to enter **\*\*OMEG\***. These data sets are installation data sets and data sets that are maintained by the system programming personnel.

➔ **NC-PASS Installation Datasets** – Search the JES2 proclibs for the member that executes program **NCI**. Use ISPF/PDF option 3.4 data set name list to enter **\*\*NCPASS\***. These data sets are installation data sets and data sets that are maintained by the system programming personnel.

➔ **NETVIEW STC Datasets** – Search the JES2 proclibs for the NETVIEW started task members. The data sets in this group are the data sets that are updated and/or allocated by the started tasks.

➔ **NETVIEW Installation Datasets** – Search the JES2 proclibs for the NETVIEW started task members. Use ISPF/PDF option 3.4 data set name list to enter **\*\*NETVIEW\***. These data sets are installation data sets and data sets that are maintained by the system programming personnel.

➔ **SRRAUDIT User Datasets** – Data sets created by the SRRAUDIT Process, **SYS3.SRRAUDIT**. Included in this list are also data sets with **SYS3.FSO**. Use ISPF/PDF option 3.4 to obtain these data set names.

➔ **SRRAUDIT Installation Datasets** – Data sets are the data sets installed for the SRRAUDIT Process, **SYS2.SRRAUDIT**. Use ISPF/PDF option 3.4 to obtain these data set names.

➔ **ROSCOE STC Datasets** – Search the JES2 proclibs for the ROSCOE members or review the ROSCOE batch jobs. The data sets in this group are the data sets identified in the ROSACTxx, ROSLIBxx, and SYSAWSx DD statements. These data sets are updated and maintained by the ROSCOE STC and/or batch job.

➔ **ROSCOE Installation Datasets** – Search the JES2 proclibs for the ROSCOE members or review the ROSCOE batch jobs. Use ISPF/PDF option 3.4 data set name list to enter **\*\*ROSCOE\***. These data sets are installation data sets and data sets that are maintained by the system programming personnel.

➔ **TDMF Installation Datasets** – Use ISPF/PDF option 3.4 data set name list to enter **\*\*TDMF\***. These data sets are installation data sets and data sets that are maintained by the system programming personnel.

➔ **TADz STC Datasets** – Search the JES2 proclibs for the TADz started members and/or review the TADz batch jobs. The data sets in this group are the data sets that are updated and/or allocated by the TADz started members and/or the TADz batch jobs.

➔ **TADz Installation Datasets** – Search the JES2 proclibs for the TADz started members and/or review the TADz batch jobs. Use ISPF/PDF option

3.4 data set name list to enter **\*\*TADZ\***. These data sets are installation data sets and data sets that are maintained by the system programming personnel.

➔ VSS User Datasets – Use ISPF/PDF option 3.4 data set name list to enter **\*\*VSS\***, **\*\*VRA\***, and **\*\*VSR\***. These data sets are user modifiable data sets that are maintained by system programming personnel, security personnel, and batch users.

➔ VSS Installation Datasets – Use ISPF/PDF option 3.4 data set name list to enter **\*\*VSS\***, **\*\*VRA\***, and **\*\*VSR\***. These data sets are installation data sets and data sets that are maintained by the system programming personnel.

➔ HCD User Datasets – Use ISPF/PDF option 3.4 data set name list to enter **\*\*IODF\***. From the results of IPLINFO script, find the currently active IODF data set. These data sets are user modifiable data sets that are maintained by system programming personnel.

➔ HCD Installation Datasets – Use ISPF/PDF option 3.4 data set name list to enter **SYS1.ACBD\*** and **SYS1.SCBD\***. These data sets are installation data sets and data sets that are maintained by the system programming personnel.

➔ ICSF STC Datasets – Search the JES2 proclibs for the ICSF started members and/or review the ICSF batch jobs. Review contents of the data set identified in the **CSFPARM DD** statement, the entries for **CKDSN** and **PKDSN** specify the data sets for this group. The data sets in this group are the data sets that are updated and/or allocated by the ICSF started task members and/or the ICSF batch jobs.

➔ ICSF Installation Datasets – Search the JES2 proclibs for the TADz started members and/or review the TADz batch jobs. Use ISPF/PDF option 3.4 data set name list to enter **SYS1.CSF**. These data sets are installation data sets and data sets that are maintained by the system programming personnel.

➔ BMC MAINVIEW Installation Datasets – Use ISPF/PDF option 3.4 data set name list to enter **SYS2.BMCVIEW**. These data sets are installation data sets and data sets that are maintained by the system programming personnel.

➔ BMC MAINVIEW STC Datasets – Use ISPF/PDF option 3.4 data set name list to enter **SYS3.BMCVIEW** data sets that are updated and/or allocated by the products STCs. The data sets in this group are the data sets that are updated and/or allocated by the started task members and/or the batch jobs.

➔ CA VTape Installation Datasets – Use ISPF/PDF option 3.4 data set name list to enter **SYS2.VTAPE** and **SYS3.VTAPE** data sets that are not

update/allocated by the products STCs. These data sets are installation data sets and data sets that are maintained by the system programming personnel.

➔ CA VTape STC Datasets – Use ISPF/PDF option 3.4 data set name list to enter **SYS3.VTAPE** data sets that are update/allocated by the products STCs. The data sets in this group are the data sets that are updated and/or allocated by the started task members and/or the batch jobs.

➔ CA Common Services Installation Datasets – Use ISPF/PDF option 3.4 data set name list to enter **SYS2.CCS**, **SYS2A.CCS**, **SYS3.CCS**, and **SYS3A.CCS** data sets. These data sets are installation data sets and data sets that are maintained by the system programming personnel.

➔ IBM Health Checker STC Datasets – Review the **HZSPROC** started task member to obtain the data set specified in the **HZSDATA DD** statement.

➔ Compuware Abend-AID Installation Datasets – Use ISPF/PDF option 3.4 data set name list to enter **SYS2.ABENDAID**, **SYS2A.ABENDAID**, and **SYS3A.ABENDAID** data sets that are not update/allocated by the products STCs. These data sets are installation data sets and data sets that are maintained by the system programming personnel.

➔ Compuware Abend-AID STC Datasets – Use ISPF/PDF option 3.4 data set name list to enter **SYS3.ABENDAID** data sets that are update/allocated by the products STCs. The data sets in this group are the data sets that are updated and/or allocated by the started task members and/or the batch jobs.

➔ CA MIM Installation Datasets – Use ISPF/PDF option 3.4 data set name list to enter **SYS2.MIMGR** and **SYS3.MIMGR** data sets that are not update/allocated by the products STCs. These data sets are installation data sets and data sets that are maintained by the system programming personnel.

➔ CA MIM STC Datasets – Use ISPF/PDF option 3.4 data set name list to enter **SYS3.MIMGR** data sets that are update/allocated by the products STCs. The data sets in this group are the data sets that are updated and/or allocated by the started task members and/or the batch jobs.

---

**9. For sites that have ACF2 as the Security Product:**

- a) Review, edit, and make changes where necessary to **SYS3.FSO.xxxx.mmmmyyyy.CNTL(CAAT0001)**. It is recommended that the member CAAT0001 be reviewed and modified to ensure that all resources have been identified. The format for this member is an eight (8) character Resource Class name, **starting in column 1**, and a three (3) character Type Code, **starting in column 9**, used by ACF2.

This information is verified in this process using the internal and external CLASMAP definitions. The Resource Classes and Type Codes that are identified in CAAT0001 may or may not be defined in the CLASMAP definitions. A Resource Class can be repeated with different Type Codes within CAAT0001. An example:

C	+	1
C123456789012		
TRANS		CKC
TRANS		CKA

If a Resource Class is identified in both internal and external CLASMAP definitions, the process will use the Type Code that is in the external CLASMAP definition. If a Resource Class is not in the external CLASMAP definition, the process will use the *first* occurrence of the Resource Class in the internal CLASMAP definition.

If the Resource Class does not appear in the CLASMAP or the Type Code for the Resource Class is not appropriate enter the Resource Class and Type Code into CAAT0001 to be used by the process. An example where Resource Class PROGRAM is not defined in the external CLASMAP definition, enter the following into CAAT0001:

**PROGRAM PGM**

The process will possibly use the following:

**PROGRAM CPC**

The INFODIR entries may identify Type Codes that are not defined in the CLASMAP definition. If a Type Code can be identified to a Resource Class to be collected enter the information into **CAAT0001**.

*Note for CICS:* Review CICS STCs for ACF2PARM DD statement. Within each ACF2PARM data set find CICSKEY for RESOURCE=TRANS, enter the TYPE= entry in CAAT0001. An example follows:

**CICSKEY OPTION=VALIDATE,TYPE=KTS,RESOURCE=TRANS**

Enter the following in CAAT0001:

**TRANS    KTS**



## **z/OS Data Collection**

CA Auditor (formally known as CA Examine) will be used as the primary vehicle to collect the z/OS data necessary to conduct the Security Readiness Review (SRR). Almost all CA Auditor data collection will be accomplished in batch. However, some on-line interaction using ISPF/PDF and CA Auditor will be necessary.

The data gathered will be saved in the following partitioned data sets:

- 1) **SYS3.FSO.xxxx.mmmmyyyy.EXAM.RPT** - CA Auditor reports
- 2) **SYS3.FSO.xxxx.mmmmyyyy.PARMLIB** - Copies of various system parmlib members
- 3) **SYS3.FSO.xxxx.mmmmyyyy.PARMLIB.ACCESS** - Inaccessible data sets referred to in SYS1.PARMLIB.
- 4) **SYS3.FSO.xxxx.mmmmyyyy.PDI** – Finding Analysis Detail reports.

These permanent data sets must be located on a domain accessible to the reviewing personnel and will be required for follow-up SRR data analysis. The data sets should be backed up and retained by the site for future reference.

\_\_\_ 1. **Submit JCL to execute the batch CA Auditor job.**

- \_\_\_ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.xxxx.mmmmyyyy.CNTL(EXAMJOB)**.
- \_\_\_ b) Copy **SYS3.FSO.xxxx.mmmmyyyy.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.
- \_\_\_ c) Submit **EXAMJOB** for execution. CA Auditor (formally known as CA Examine) report steps may end with a condition code of **0** although errors occurred. Review the job for error messages to ensure successful execution, particularly the following:
  - \_\_\_ 1) The ISPLOG and SYSTSPRT files of each report step.
  - \_\_\_ 2) The JOBLOG or JESLOG files.

***NOTE:** The CA Auditor job accesses numerous system level data sets. Access authorization problems may not be obvious at first because the CA Auditor reports will still be produced. However, the information in these reports may not be complete. It is imperative that the job is thoroughly examined for error messages, especially from the ACP.*

The **EXAMJOB** job will create the PDS **SYS3.FSO.xxxx.mmmmyyyy.EXAM.RPT** and save each report in individual members. These members will be referenced in the z/OS STIG under the Vulnerability Checks for subsequent analysis.

---

\_\_\_ **2. Collect data using the on-line CA Auditor ISPF application.**

Some functions under CA Auditor (formally known as CA Examine) are not supported in batch. Therefore, certain CA Auditor reports must be executed on-line.

**NOTE:** If JES2 contains dynamic proclibs there may be a problem with CA Auditor reporting these proclib data sets. If the system proclibs, data sets containing started task and TSO procedures, are dynamically allocated to JES2, this step will have to be bypassed.

\_\_\_ a) Collect JES2 proclib member lists.

- \_\_\_ 1) From ISPF/PDF option 6, issue the following command. This will allow CA Auditor to write output to this PDS member when using the CA Auditor **REPORT** command:

**alloc f(exam\$out) da('sys3.fso.xxxx.mmmmyyyy.exam.rpt(proclibs)')**

- \_\_\_ 2) Invoke the CA Auditor application. From the CA Auditor primary menu, enter **4.2** from the command line to display the **JES2 PROCLIB DISPLAY** menu.
- \_\_\_ 3) Enter the command **REPORT ON** from the command line to activate CA Auditor continuous reporting mode.
- \_\_\_ 4) Select each proclib that contains started task procedures and TSO procedures, they are displayed at the bottom of the **JES2 PROCLIB DISPLAY** menu and press the **ENTER** key.
- \_\_\_ 5) From the **PROCLIB SEARCH DATA** menu, enter a *hyphen* (-) for a program mask and press the **ENTER** key. After the list of proclib members is displayed, press the **PF3** key twice to display the next proclib. Repeat this same program mask search for each proclib.
- \_\_\_ 6) After all proclibs are searched, enter the command **REPORT OFF** from the command line to deactivate CA Auditor continuous reporting mode and exit the CA Auditor application.
- \_\_\_ 7) Exit CA Auditor and issue the following command:

**free fi(exam\$out)**

\_\_\_ b) Collect CICS proclib member lists and JCL.

- \_\_\_ 1) From ISPF/PDF option 6, issue the following command. This will allow CA Auditor to write output to this PDS member when using the CA Auditor **REPORT** command:

**alloc f(exam\$out) da('sys3.fso.xxxx.mmmyyyyy.exam.rpt(cicsproc)')**

- \_\_\_ 2) Invoke the CA Auditor application. From the CA Auditor primary menu, enter **4.2** from the command line to display the **JES2 PROCLIB DISPLAY** menu.
- \_\_\_ 3) Select each proclib displayed at the bottom of the **JES2 PROCLIB DISPLAY** menu and press the **ENTER** key.
- \_\_\_ 4) From the **PROCLIB SEARCH DATA** menu, enter **DFHSIP** for the program name and press the **ENTER** key.
- \_\_\_ 5) After the list of CICS proclib members is displayed, enter the command **REPORT ON** from the **SELECTED PROCLIB MEMBERS** menu to activate CA Auditor continuous reporting mode.
- \_\_\_ 6) Select all CICS proclib members. When completed, enter the command **REPORT OFF** from the **SELECTED PROCLIB MEMBERS** menu to deactivate continuous reporting mode. Press the **PF3** key twice to display the next proclib. Repeat steps 4 through 6 for each proclib.
- \_\_\_ 7) After all proclibs are searched, exit CA Auditor and issue the following command:

**free fi(exam\$out)**

---

\_\_\_ **3. Other required information that is not obtained from CA Auditor.**

The means and tools used to gather the following information is discretionary, but this information must be recorded.

- \_\_\_ a) Save a copy of the JES2 initialization parameter member(s) in **SYS3.FSO.xxxx.mmmmyyy.PARMLIB** using the same JES2 member name(s). This parameter list is referenced by the **HASPPARM DD** statement in the JES2 system procedure.
- \_\_\_ b) Save a copy of each of the following Logical Parmlib data sets or **SYS1.PARMLIB** members (where **xx** is any two-character suffix) in **SYS3.FSO.xxxx.mmmmyyy.PARMLIB** using the same member name:

**IKJTSOxx**  
**IEAAPPxx**  
**BPXPRMxx**

\_\_\_ 4. Submit JCL to execute the batch **SYS1.PARMLIB** members inquiry.

- \_\_\_ a) Review the JCL, edit and make changes where necessary to **SYS3.FSO.xxxx.mmmmyyyy.CNTL(CACJ0001)**.

**NOTE:** **PARMDSN** can be added to point to the primary parmlib data set that contains the **IEASYSxx**, **IEAAPFxx**, **PROGxx**, **LPALSTxx**, **IEAFIXxx**, **IEALPApp**, and **LNKLSTxx** members. If **PARMDSN** is not specified the job will collect the logical parmlib concatenation

The following is an example:

```
ISPSTART CMD(%CACCC0003 TERMMSGSGS(ON) +  
PARMDSN(SYS2.PARMLIB))
```

Or

```
ISPSTART CMD(%CACCC0003 TERMMSGSGS(ON) +  
PARMDSN('SYS2.PARMLIB SYS1.PARMLIB'))
```

- \_\_\_ b) Copy **SYS3.FSO.xxxx.mmmmyyyy.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.
- \_\_\_ c) Submit **CACJ0001** for execution. Review the job for error messages to ensure successful execution, particularly the following:
- \_\_\_ 1) The ISPLOG and SYSTSPRT files of each report step.
- \_\_\_ 2) The JOBLLOG or JESLOG files.

The **CACJ0001** job will create the data sets **SYS3.FSO.xxxx.mmmmyyyy.PARMLIB.ACCESS** and **SYS3.FSO.xxxx.mmmmyyyy.PDI**, saving each report in individual members. These members will be referenced in the z/OS STIG under the Vulnerability Checks for subsequent analysis.

---

**5. Submit JCL to execute SRRAUDIT Product Analysis**

**NOTE:** If WebSphere MQ is identified in the Products ensure that the individual submitting the **CACJ0005** job has the following resource access authorizations (where *ssid* is the subsystem name for each WebSphere MQ):

Resource Class	Entity	Access
PROGRAM	CSQUTIL	EXECUTE
MQCONN	<i>ssid</i> .BATCH	READ
MQCMDS	<i>ssid</i> .DISPLAY.	READ
MQQUEUE	<i>ssid</i> .SYSTEM.COMMAND.INPUT	UPDATE
MQQUEUE	<i>ssid</i> .SYSTEM.COMMAND.REPLY	UPDATE
MQQUEUE	<i>ssid</i> .SYSTEM.CSQUTIL.-	UPDATE

Ensure that each WebSphere MQ STCs are active on the system before job submission.

**NOTE:** Additional access requirements may be required for the individual submitting this job dependent upon the products used on the system.

- \_\_\_ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.xxxx.mmmmyyy.CNTL(CACJ0005)**.
- \_\_\_ b) Copy **SYS3.FSO.xxxx.mmmmyyy.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.
- \_\_\_ c) If WebSphere MQ is installed on the system, ensure the data sets allocated by the **STEPLIB** DD statement in **MQS20** contain modules **CSQUTIL** and **CSQCMTXT** (**SCSQAUTH** and **SCSQANLE** data sets).
- \_\_\_ d) Submit **CACJ0005** for execution. Review the job for error messages to ensure successful execution, particularly the following:
  - \_\_\_ 1) The ISPLOG and SYSTSPRT files of each report step.
  - \_\_\_ 2) The JOBLOG or JESLOG files.

The **CACJ0005** job will modify/add members to data set **SYS3.FSO.xxxx.mmmmyyy.PDI**, saving each report in individual members. These members will be referenced in the z/OS STIG under the Vulnerability Checks for subsequent analysis.

The **CACJ0005** job will create and/or modify/add members to data sets:  
**SYS3.FSO.xxxx.mmmmyyyy.TABLE**, table information on Products. This data set will be used during subsequent data collection jobs.

The following data sets will be created depending on the Products used on the system:

**SYS3.FSO.xxxx.mmmmyyyy.CA1RPT** – CA 1 utility reports  
**SYS3.FSO.xxxx.mmmmyyyy.CONSOLE** – CA Examine Console report  
**SYS3.FSO.xxxx.mmmmyyyy.MQSRPT** – WebSphere MQ utility reports  
**SYS3.FSO.xxxx.mmmmyyyy.IOA.RPT** – IOA product configuration data.  
**SYS3.FSO.xxxx.mmmmyyyy.SMFOPTS** – CA Examine SMF Options report  
**SYS3.FSO.xxxx.mmmmyyyy.TABLE** – SRRAUDIT CNTL table entries

**NOTE:** *If STEP0020 produces a condition code of 4, Review the SYSTSPRT output and correct the Dialog data set as specified using the SRRAUDIT Dialog Management document. Other steps will run only if STEP0020 receives a return code of 0. Return codes from other steps will be checked to mark vulnerabilities from unused products as N/A and in future releases to automatically bypass collection steps and steps that will be run to validate vulnerabilities.*

**NOTE:** *For this release all Product STEPS to be bypassed based on a RC=4 will be specified with a flower box that states the following.*

```
*****
*   IF THE RETURN CODE FROM xxxxxx00 OF JOB CACJ0005   *
*           HAS A RC=4 THIS PRODUCT CAN BE SKIPPED      *
*****
```



## ACF2 Data Collection

```
*****  
* Follow the instruction in this Section only if the *  
*               System is running ACF2               *  
*****
```

These instructions will use batch processing to collect the ACF2 and z/OS data necessary to conduct the Security Readiness Review (SRR).

The data gathered will be saved in the following partitioned data sets:

- 1) **SYS3.FSO.xxxx.mmmyyyy.ACF2CMDS.RPT** - ACF2 command reports
- 2) **SYS3.FSO.xxxx.mmmyyyy.ALIAS.RPT** - Master Catalog aliases
- 3) **SYS3.FSO.xxxx.mmmyyyy.PDI** - Finding Analysis Detail reports.

These permanent data sets must be located on a domain accessible to the reviewing personnel and will be required for follow-up SRR data analysis. The data sets should be backed up and retained by the site for future reference.

\_\_\_ 1. **Produce the ACF2CMDS report.**

- \_\_\_ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.xxxx.mmmmyyyy.CNTL(ACF2CMDS)**.
- \_\_\_ b) Copy **SYS3.FSO.xxxx.mmmmyyyy.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.
- \_\_\_ c) Submit **ACF2CMDS** for execution. Review the job for error messages to ensure successful execution, particularly the following:
  - \_\_\_ 1) The SYSPRINT files of each report step.
  - \_\_\_ 2) The JOBLLOG or JESLOG files.

The **ACF2CMDS** job will create the PDS **SYS3.FSO.xxxx.mmmmyyyy.ACF2CMDS.RPT**, saving each report in individual members. These members will be referenced in the z/OS STIG under the Vulnerability Checks for subsequent analysis.

---

\_\_\_ **2. Produce the Master Catalog ALIAS report.**

- \_\_\_ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.xxxx.mmmmyyyy.CNTL(ACFLSTA)**.
- \_\_\_ b) Copy **SYS3.FSO.xxxx.mmmmyyyy.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.
- \_\_\_ c) Submit **ACFLSTA** for execution. Review the job for error messages to ensure successful execution, particularly the following:
  - \_\_\_ 1) The SYSPRINT files of each report step.
  - \_\_\_ 2) The JOBLLOG or JESLOG files.

The **ACFLSTA** job will create the data set **SYS3.FSO.xxxx.mmmmyyyy.ALIAS.RPT**, saving a list of Master Catalog aliases in it. This information will be referenced in the z/OS STIG under the Vulnerability Checks for subsequent analysis.

\_\_\_ **3. Evaluate ACF2 Configuration.**

- \_\_\_ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.xxxx.mmmyyyy.CNTL(CAAJ0003)**.
- \_\_\_ b) Copy **SYS3.FSO.xxxx.mmmyyyy.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.
- \_\_\_ c) Submit **CAAJ0003** for execution. Review the job for error messages to ensure successful execution, particularly the following:
  - \_\_\_ 1) The ISPLOG and SYSTSPRT output files of each step.
  - \_\_\_ 2) The JOBLOG or JESLOG files.

The **CAAJ0003** job will create members in the following data set:

**SYS3.FSO.xxxx.mmmyyyy.PDI** - Finding Analysis Detail reports.

## RACF Data Collection

```
*****  
* Follow the instruction in this Section only if the *  
*               System is running RACF               *  
*****
```

These instructions will use batch processing to collect the RACF and z/OS data necessary to conduct the Security Readiness Review (SRR).

The data gathered will be saved in the following partitioned data sets:

- 1) **SYS3.FSO.xxxx.mmmmyyyy.ALIAS.RPT** - Master Catalog aliases
- 2) **SYS3.FSO.xxxx.mmmmyyyy.DSMON.RPT** - RACF DSMON reports
- 3) **SYS3.FSO.xxxx.mmmmyyyy.RACFCMDS.RPT** - RACF command reports
- 4) **SYS3.FSO.xxxx.mmmmyyyy.PDI** - Finding Analysis Detail reports.

These permanent data sets must be located on a domain accessible to the reviewing personnel and will be required for follow-up SRR data analysis. The data sets should be backed up and retained by the site for future reference.

\_\_\_ 1. **Produce the RACF command reports.**

- \_\_\_ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.xxxx.mmmmyyyy.CNTL(RACFCMD1)**.
- \_\_\_ b) Copy **SYS3.FSO.xxxx.mmmmyyyy.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.
- \_\_\_ c) Submit **RACFCMD1** for execution. After the job has ended, review the following for error messages to ensure successful execution:
  - \_\_\_ 1) The **RACFCMD1** batch job.

***NOTE:** A job step condition code of **4** typically indicates that no information was available.*

- \_\_\_ 2) All PDS members in **SYS3.FSO.xxxx.mmmmyyyy.RACFCMDS.RPT**.

***NOTE:** RACF command error messages will be located in these PDS members used to hold command output.*

The **RACFCMD1** job will create the PDS **SYS3.FSO.xxxx.mmmmyyyy.RACFCMDS.RPT**, saving each report in individual members. These members will be referenced in the z/OS STIG under the Vulnerability Checks for subsequent analysis.

---

\_\_\_ **2. Produce the Master Catalog ALIAS and DSMON reports.**

- \_\_\_ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.xxxx.mmmmyyyy.CNTL(RACFCMD2)**.
- \_\_\_ b) Copy **SYS3.FSO.xxxx.mmmmyyyy.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.
- \_\_\_ c) Submit **RACFCMD2** for execution. Review the job for error messages to ensure successful execution, particularly the following:
  - \_\_\_ 1) The SYSPRINT files of each report step.
  - \_\_\_ 2) The JOBLOG or JESLOG files.

The **RACFCMD2** job will create the following data sets:

**SYS3.FSO.xxxx.mmmmyyyy.ALIAS.RPT** - A list of Master Catalog aliases

**SYS3.FSO.xxxx.mmmmyyyy.RACFCMDS.RPT(UNDALIAS)** - A list of undefined Master Catalog aliases

**SYS3.FSO.xxxx.mmmmyyyy.DSMON.RPT** - RACF-specific information such as exits, resource classes, etc.

This information will be referenced in the z/OS STIG under the Vulnerability Checks for subsequent analysis.

\_\_\_ 3. Evaluate RACF Configuration.

- \_\_\_ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.xxxx.mmmmyyyy.CNTL(CARJ0003)**.
- \_\_\_ b) Copy **SYS3.FSO.xxxx.mmmmyyyy.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.
- \_\_\_ c) Submit **CARJ0003** for execution. Review the job for error messages to ensure successful execution, particularly the following:
  - \_\_\_ 1) The ISPLOG and SYSTSPRT output files of each step.
  - \_\_\_ 2) The JOBLOG or JESLOG files.

The **CARJ0003** job will create members in the following data set:

**SYS3.FSO.xxxx.mmmmyyyy.PDI** - Finding Analysis Detail reports.



## TSS Data Collection

```
*****
* Follow the instruction in this Section only if the *
*               System is running TSS               *
*****
```

These instructions will use batch processing to collect the TOP SECRET SECURITY (TSS) and z/OS data necessary to conduct the Security Readiness Review (SRR).

The data gathered will be saved in the following partitioned data sets:

- 1) **SYS3.FSO.xxxx.mmmmyyyy.TSSCMD.S.RPT** - TSS command reports
- 2) **SYS3.FSO.xxxx.mmmmyyyy.TSSDUMP.RPT** - IDCAMS report
- 3) **SYS3.FSO.xxxx.mmmmyyyy.ALIAS.RPT** - Master Catalog aliases
- 4) **SYS3.FSO.xxxx.mmmmyyyy.TSSPRIV.RPT** - TSS privileges (short) report
- 5) **SYS3.FSO.xxxx.mmmmyyyy.TSSCHNGS.RPT** - TSS changes report
- 6) **SYS3.FSO.xxxx.mmmmyyyy.PDI** - Finding Analysis Detail reports.

These permanent data sets must be located on a domain accessible to the reviewing personnel and will be required for follow-up SRR data analysis. They should be backed up and retained by the site for future reference.

\_\_\_ 1. **Produce the TSSCMDS report.**

- \_\_\_ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.xxxx.mmmmyyyy.CNTL(TSSCMDS)**. Change **STEP23** to point to the correct data set that contains the **TSSINSTX** program.
- \_\_\_ b) Copy **SYS3.FSO.xxxx.mmmmyyyy.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.
- \_\_\_ c) Submit **TSSCMDS** for execution. After the job has ended, review the job for error messages to ensure successful execution, particularly the following:

**NOTE:** Submitting this job using the MSCA's ACID will help in identifying which ACIDs have NOPW specified as a password.

- \_\_\_ 1) The SYSPRINT files of each report step.
- \_\_\_ 2) The JOBLOG or JESLOG files.

The **TSSCMDS** job will create the PDSs **SYS3.FSO.xxxx.mmmmyyyy.TSSCMDS.RPT**, **SYS3.FSO.xxxx.mmmmyyyy.TSSDUMP.RPT**, and **SYS3.FSO.xxxx.mmmmyyyy.TSSACIDS**, saving each report in individual members.

These data sets and members will be referenced in the z/OS STIG under the Vulnerability Checks for subsequent analysis.

---

\_\_\_ **2. Produce the Master Catalog ALIAS report and the Undefined ALIAS report.**

- \_\_\_ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.xxxx.mmmmyyyy.CNTL(TSSLSTA)**.
- \_\_\_ b) Copy **SYS3.FSO.xxxx.mmmmyyyy.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.
- \_\_\_ c) Submit **TSSLSTA** for execution. After the job has ended, review the job for error messages to ensure successful execution, particularly the following:
  - \_\_\_ 1) The SYSPRINT files of each report step.
  - \_\_\_ 2) The JOBLLOG or JESLOG files.

The **TSSLSTA** job will create the following:

**SYS3.FSO.xxxx.mmmmyyyy.ALIAS.RPT**, which contains a list of Master Catalog aliases.

**SYS3.FSO.xxxx.mmmmyyyy.TSSCMDS.RPT(UNDALIAS)**, saving a list of Master Catalog aliases that are not defined to the TSS database.

This information will be referenced in the z/OS STIG under the Vulnerability Checks for subsequent analysis.

\_\_\_ 3. **Produce the TSSAUDIT reports.**

- \_\_\_ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.xxxx.mmmmyyyy.CNTL(TSSAUDIT)**.
- \_\_\_ b) Copy **SYS3.FSO.xxxx.mmmmyyyy.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.
- \_\_\_ c) Submit **TSSAUDIT** for execution. Review the job for error messages to ensure successful execution.

The **TSSAUDIT** job will create the data sets:

**SYS3.FSO.xxxx.mmmmyyyy.TSSPRIV.RPT**, saving a report on special privileges.

**SYS3.FSO.xxxx.mmmmyyyy.TSSCHNGS.RPT**, saving a report of security changes.

This information will be referenced in the z/OS STIG under the Vulnerability Checks for subsequent analysis.

---

\_\_\_ **4. Copy of TSS parameter file.**

- \_\_\_ a) Review the system proclibs to locate the production TSS procedure. Select the production TSS procedure, and identify the TSS parmlib member to be copied for review.
- \_\_\_ b) Save a copy of the TSS parameter file in  
**SYS3.FSO.xxxx.mmmyyy.TSSCMD.S.RPT(TSSPRMFL).**

\_\_\_ 5. Collect TSS facility and mode information.

*NOTE: Due to the TSS authorizations required to collect facility and mode information, site security personnel must submit the TSSCMD2 and TSSCMD3 jobs.*

- \_\_\_ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.xxxx.mmmmyyyy.CNTL(TSSCMD2)** following the instructions within the comment block at the beginning of the JCL.
- \_\_\_ b) Copy **SYS3.FSO.xxxx.mmmmyyyy.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.
- \_\_\_ c) Review **SYS3.FSO.xxxx.mmmmyyyy.TSSCMDS.RPT** for member STATUS, WHOOMODE, and WHOHMODE. If the members are found with the appropriate results, delete the step that creates the report. STEP2, STEP3, and STEP4 respectively.
- \_\_\_ d) **TSSCMD2** should be submitted by the site security personnel (e.g., IAO). After the job has ended, review error messages to ensure successful execution.

The TSSCMD2 job will create one to four new members in **SYS3.FSO.xxxx.mmmmyyyy.TSSCMDS.RPT**. These members are FACALL, STATUS, WHOOMODE, and WHOHMODE.

- \_\_\_ e) Upon successful completion of **TSSCMD2**, review the JCL, edit, and make changes where necessary to **SYS3.FSO.xxxx.mmmmyyyy.CNTL(TSSCMD3)** using the following instructions by reviewing:
  - 1) **SYS3.FSO.xxxx.mmmmyyyy.TSSCMDS.RPT(FACALL)** and add the following **MODIFY** statement to **TSSCMD3** for each facility listed. For example:

**TSS MODIFY(FAC(facility name))**

- 2) **SYS3.FSO.xxxx.mmmmyyy.TSSCMD3.RPT(TSSPRMFL)** and add the following **MODIFY** statement to **TSSCMD3** for each CICS facility defined. CICS facilities are identified by the control option **'INITPGM=DFH'**. For example:

**TSS MODIFY(FAC(CICS facility name=BYPLIST))**

***NOTE:** CICS facilities require both **MODIFY** statements to collect the required data.*

- \_\_\_ f) Copy **SYS3.FSO.xxxx.mmmmyyy.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.
- \_\_\_ g) Have the site security personnel (e.g., IAO) submit **TSSCMD3**. After the job has ended, review error messages to ensure successful execution.

The **TSSCMD3** job will create a member in **SYS3.FSO.xxxx.mmmmyyy.TSSCMD3.RPT**. This member is named **FACLIST**. This information will be referenced in the z/OS STIG under the Vulnerability Checks for subsequent analysis.

**NOTE:** The following steps are an alternative process for collecting the TSS Facility information. This JCL does not have to be submitted by the site's security personnel.

- \_\_\_ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.xxxx.mmmmyyy.CNTL(TSSCMD4)** following the instructions within the comment block at the beginning of the JCL.
- \_\_\_ b) Copy **SYS3.FSO.xxxx.mmmmyyy.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.
- \_\_\_ c) Submit **TSSAUDIT** for execution. Review the job for error messages to ensure successful execution.

The **TSSCMD4** job will create the following data set member:  
**SYS3.FSO.xxxx.mmmmyyy.TSSCMD3.RPT(FACALLA)**  
**SYS3.FSO.xxxx.mmmmyyy.TSSCMD3.RPT(FACLISTA)**  
FACALLA can be used as a substitute for FACALL.  
FACLISTA can be used as a substitute for FACLIST.  
This information will be referenced in the z/OS STIG under the Vulnerability Checks for subsequent analysis.

\_\_\_ **6. Evaluate TSS Configuration.**

- \_\_\_ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.xxxx.mmmmyyyy.CNTL(CATJ0002)**.
- \_\_\_ b) Copy **SYS3.FSO.xxxx.mmmmyyyy.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.
- \_\_\_ c) Submit **CATJ0002** for execution. Review each of the job steps for error messages to ensure successful execution, particularly the following:

**NOTE:** If this job is submitted using the MSCA's ACID, the PDI member TSS0750 will be generated.

- \_\_\_ 1) The ISPLOG and SYSTSPRT output files of each step.
- \_\_\_ 2) The JOBLOG or JESLOG files.

The **CATJ0002** job will create members the following data set:

**SYS3.FSO.xxxx.mmmmyyyy.PDI** - Finding Analysis Detail reports.



## CA 1 Data Collection

```
*****
*   IF THE RETURN CODE FROM CA100 OF JOB CACJ0005   *
*           HAS A RC=4 THIS PRODUCT CAN BE SKIPPED   *
*****
```

**NOTE: The information that is collected for this product has already been collected and processed in CACJ0005. The instructions specified in this section do not need to be performed.**

CA 1 report utilities and IBM's IDCAMS program will be used to collect the CA 1 data necessary to conduct the Security Readiness Review (SRR).

The data gathered will be saved in the following partitioned data sets:

- 1) **SYS3.FSO.xxxx.mmmmyyyy.CA1.RPT** - CA 1 utility reports
- 2) **SYS3.FSO.xxxx.mmmmyyyy.CA1.RPT2** - IDCAMS report

These permanent data sets must be located on a domain accessible to the reviewing personnel and will be required for follow-up SRR data analysis. The data sets should be backed up and retained by the site for future reference.

\_\_\_ 1. Submit JCL to execute the batch CA 1 data collection job.

- \_\_\_ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.xxxx.mmmmyyyy.CNTL(CA1UTIL)**. Ensure that the correct CA 1 load library is specified on the **STEPLIB** DD statement for Steps 3 and 4 and on the **CAILIB** DD statement for Step 5.
- \_\_\_ b) Copy **SYS3.FSO.xxxx.mmmmyyyy.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.
- \_\_\_ c) Submit **CA1UTIL** for execution. Review the job for error messages to ensure successful execution.

The **CA1UTIL** job will create the data sets:

**SYS3.FSO.xxxx.mmmmyyyy.CA1.RPT**

**SYS3.FSO.xxxx.mmmmyyyy.CA1.RPT2**

They will be referenced in the CA 1 Data Analysis.

---

\_\_\_ **2. Collect data using the CA 1 on-line ISPF application.**

- \_\_\_ a) CA 1 does not have a batch facility to report on internal passwords. Therefore, this information must be collected interactively using the CA 1 ISPF application. Before invoking the CA 1 ISPF application, you must obtain an internal password from the CA 1 systems programmer with the authority to view the CA 1 security table.
- \_\_\_ b) Invoke the CA 1 application, and select *Option 3, MAINTENANCE*, from the **CA 1 Primary Option Menu**. On the next menu, **CA 1 CONFIGURATION TABLES MAINTENANCE**, select *Option 1, CA 1 SECURITY Table*. All CA 1 internal passwords and associated privileges are available from the **CA 1 SECURITY TABLE LISTING** menu.
- \_\_\_ c) CA 1 does not provide a convenient method to save this information. Use an available facility to save the internal password information. For example, most 3270 Terminal Host Emulation software offers a COPY/PASTE feature. Use this feature to copy the information to **SYS3.FSO.xxxx.mmmyyy.CA1.RPT**, creating a new member called **TMSPSWD**.

## CICS Data Collection

```
*****  
*   IF THE RETURN CODE FROM CICS00 OF JOB CACJ0005   *  
*           HAS A RC=4 THIS PRODUCT CAN BE SKIPPED   *  
*****
```

IBM's IDCAMS program will be used to collect the CICS data necessary to conduct the Security Readiness Review (SRR).

The data gathered will be saved in the following partitioned data set:

**SYS3.FSO.xxxx.mmmmyyyy.CICS.RPT - IDCAMS SIT dump reports**

This permanent data set must be located on a domain accessible to the reviewing personnel and will be required for follow-up SRR data analysis. This data set should be backed up and retained by the site for future reference.

---

\_\_\_ **1. Submit JCL to execute the batch IDCAMS CICS data collection job.**

- \_\_\_ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.xxxx.mmmmyyyy.CNTL(CICSSIT)**. Ensure the following items are specified:

- 1) CICS load library containing the CICS SIT is specified on the **SDFHAUTH DD** statement.
- 2) Repeat the dump step (i.e., Step 2) for each CICS SIT.

Ensure the PDS member name on the **SITDUMP DD** statement matches the actual SIT being dumped. This is helpful when matching dumps with specific CICS regions during the data analysis phase.

**NOTE:** The CICS startup parameter **SIT=** specifies the SIT suffix. For example, **SIT=6\$** indicates the SIT is named **DFHSIT6\$**. If no **SIT=** parameter is found in (1) the **PARM** parameter from the **EXEC PGM=DFHSIP** statement, or (2) in the **SYSIN** data set, CICS will use the unsuffixed module named **DFHSIT**.

- \_\_\_ b) Copy **SYS3.FSO.xxxx.mmmmyyyy.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the **JOB** statement.
- \_\_\_ c) Submit **CICSSIT** for execution. Review the job for error messages to ensure successful execution.

The **CICSSIT** job will create the partitioned data set:

**SYS3.FSO.xxxx.mmmmyyyy.CICS.RPT** - This file will save each SIT dump in individual members. This data set and its members will be referenced in the CICS Data Analysis.

## IBM Communications Server Data Collection

**NOTE:** The information that is collected for these products has already been collected and processed in CACJ0005. The instructions specified in this section do not need to be performed.

The IBM Communications Server Data Collection process provides Finding Details for the findings on the information collected. Additional analysis may be necessary for some of the findings. On the largest part, most of the information generated by this process can be entered directly into the SRRDB.

The data gathered will be saved in the following partitioned data sets:

- 1) **SYS3.FSO.xxxx.mmmyyy.TCPDATA** – Intermediate member data set
- 2) **SYS3.FSO.xxxx.mmmyyy.PDI** – Finding Analysis Detail reports.

These permanent data sets must be located on a domain accessible to the reviewing personnel and will be required for follow-up SRR data analysis. The data sets should be backed up and retained by the site for future reference.

## IDMS Data Collection

```
*****
*   IF THE RETURN CODE FROM IDMS00 OF JOB CACJ0005   *
*           HAS A RC=4 THIS PRODUCT CAN BE SKIPPED   *
*****
```

IBM's IDCAMS will be used to collect the IDMS data necessary to conduct the Security Readiness Review (SRR). The IDMS data collected will be dumps of program module RHDCSRTT. This module is generally found in the IDMS load library specified on the STEPLIB DD statement of each IDMS Central Version (CV) or region.

The data gathered will be saved in the following partitioned data set:

**SYS3.FS0.xxxx.mmmmyyyy.SRTTDUMP** – Member names will be **SRTTnn** (where **nn** is changed to a number whose value depends on the number of CVs to be examined).

This permanent data set must be located on a domain accessible to the reviewing personnel and will be required for follow-up SRR data analysis. The data set should be backed up and retained by the site for future reference.

\_\_\_ 1. **Submit JCL to execute the batch IDMS data collection job.**

- \_\_\_ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.xxxx.mmmmyyyy.CNTL(IDMSJCL)** following the instructions detailed within the comments of the job.

Repeat JS20 as many times as necessary to dump this module for each IDMS region or CV. Change the SRTTnn to reflect each occurrence of RHDCSRRT.

***NOTE:** The **RHDCSRTT** module will be located in a library allocated by the **STEPLIB** and/or **CDMSLIB** DD statements within the IDMS procedure. If this module is located in both DD statements, the module allocated by **CDMSLIB** takes precedence.*

- \_\_\_ b) Copy **SYS3.FSO.xxxx.mmmmyyyy.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.
- \_\_\_ c) Submit **IDMSJCL** for execution. After the job has ended, review the job for error messages to ensure successful execution.

Job step JS10 will create the PDS **SYS3.FSO.xxxx.mmmmyyyy.SRTTDUMP**.

Each occurrence of job step JS20 will dump the IDMS module **RHDCSRTT**. These members will be referenced in the IDMS Data Analysis during subsequent analysis.



## Integrated Operation Architecture (IOA) Data Collection

```
*****  
*   IF THE RETURN CODE FROM BMCIOA00 OF JOB CACJ0005   *  
*           HAS A RC=4 THIS PRODUCT CAN BE SKIPPED      *  
*****
```

IBM's IDCAMS program will be used to collect the IOA data necessary to conduct the Security Readiness Review (SRR).

The data gathered will be saved in the following partitioned data set:

**SYS3.FSO.xxxx.mmmyyy.IOA.RPT** - Members will be used to identify information pertaining to the configuration of the IOA product.

This permanent data set is created in Job CACJ0005 steps BMCIOA10, BMCCTD10, BMCCTM10, and/or BMCCTO10. This Job was submitted in STEP 5 of the z/OS Data Collection.

## WebSphere MQ Data Collection

```
*****
*   IF THE RETURN CODE FROM MQS00 OF JOB CACJ0005   *
*           HAS A RC=4 THIS PRODUCT CAN BE SKIPPED   *
*****
```

The WebSphere MQ report utility will be used to collect the WebSphere MQ data necessary to conduct the Security Readiness Review (SRR).

The data gathered will be saved in the following partitioned data set:

**SYS3.FSO.xxxx.mmmmyyyy.MQSRPT** - WebSphere MQ utility reports

This permanent data set is created in Job CACJ0005 step MQS20. This Job was submitted in STEP 5 of the z/OS Data Collection. This data set is the replacement for the data set created in the **MQSUTIL** job in **SYS3.FSO.xxxx.mmmmyyyy.CNTL**. Therefore, submitting **MQSUTIL** is no longer required. Ensure that the Subsystem Identifiers for WebSphere MQ are identified in the PRODUCTS function details identified in the *SRRAUDIT Dialog Management* document.

Review the **IEFSSNxx** member(s) in **SYS1.PARMLIB** to determine the WebSphere MQ subsystem names. These definitions are identified by the **INTRTN(CSQ3INI)** parameter entry. The value of the associated **SUBNAME** parameter is the WebSphere MQ subsystem name (a.k.a. queue manager name). In order for the collection to run correctly, each WebSphere MQ subsystem task must be active. Use SDSF to display all active started tasks. Each WebSphere MQ subsystem task, or queue manager STC, are named **ssidMSTR** (where **ssid** is the subsystem name). The individual submitting the **CACJ0005** job requires the following resource access authorizations:

<u>Resource Class</u>	<u>Entity</u>	<u>Access</u>
PROGRAM	CSQUTIL	EXECUTE
MQCONN	ssid.BATCH	READ
MQCMDS	ssid.DISPLAY.	READ
MQQUEUE	ssid.SYSTEM.COMMAND.INPUT	UPDATE
MQQUEUE	ssid.SYSTEM.COMMAND.REPLY	UPDATE
MQQUEUE	ssid.SYSTEM.CSQUTIL.-	UPDATE

If any WebSphere MQ subsystem tasks are inactive, ask the site to start these tasks before running the WebSphere MQ utility.

## UNIX System Services Data Collection

A script of UNIX commands will be used to collect the UNIX System Services data necessary to conduct the Security Readiness Review (SRR).

The data gathered will be saved in the following partitioned data set:

**SYS3.FSO.xxxx.mmmmyyy.USSCMDS.RPT** – USS command reports

This permanent data set must be located on a domain accessible to the reviewing personnel and will be required for follow-up SRR data analysis. The data set should be backed up and retained by the site for future reference.

\_\_\_ 1. Submit JCL to execute the batch UNIX System Services data collection job.

**NOTE:** *To execute the data collection job successfully, UNIX System Services must be running in full function mode. Use the following checks to determine the mode:*

- *If **OMVS=DEFAULT** is specified or if **OMVS=xx** is not coded in PARMLIB member IEASYSxx, the system is **not** running in full function mode.*
- *If PARMLIB member BPXPRMxx (or other member as specified by **OMVS=xx**) does not contain a ROOT FILESYSTEM statement, the system is **not** running in full function mode.*
- *If UNIX System Services is **not** executing in full function mode, **skip** the USS Data Collection. You will be able to perform some of the USS data analysis. These items are indicated in the USS Data Analysis.*

\_\_\_ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.xxxx.mmmyyy.CNTL(USSJCOL1)**.

- 1) Step STEP1 deletes the report data set so that the job can be restarted or rerun if desired.
- 2) Step STEP2 executes the Terminal Monitor Program in batch. The OCOPY command copies the data collection script to an HFS file. The BPXWUNIX function is invoked to execute the scripts. A series of OGET commands copies the individual HFS report files to PDS members in the reports data set. Also generates a status and error report of the data collection.

**CAUTION: DO NOT MODIFY THE USSICOLA AND USSICOLB CNTL MEMBERS!** *The UNIX commands in these members are case sensitive and contain control characters in specific columns.*

- \_\_\_ b) Copy **SYS3.FSO.xxxx.mmmmyyy.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.
- \_\_\_ c) Submit **USSJCOL1** for execution. Review the job for error messages to ensure successful execution. Pay particular attention to the SYSERR and SYMSG output of STEP2; it contains the status report (UNIX standard output and error messages) from the data collection script.

**NOTE:** *The ID under which the data collection job runs must have a valid UNIX UID and **one** of the following privileges to read all UNIX directories:*

- 1) READ access to the **SUPERUSER.FILESYS** resource in the **UNIXPRIV** resource class.*
- 2) READ access to the **BPX.SUPERUSER** resource in the **FACILITY** resource class.*
- 3) UID(0)*

The **USSJCOL1** job will create the partitioned data set **SYS3.FSO.xxxx.mmmmyyy.USSCMDS.RPT**. It will be referenced in the UNIX System Services Data Analysis.

## **Data Set and Resource Data Collection**

These instructions will use batch processing to collect the ACP and z/OS data necessary to conduct the Security Readiness Review (SRR).

The data gathered will be saved in the following partitioned data sets:

- 1) **SYS3.FSO.xxxx.mmmyyy.SENSITIVE.RPT** - Data set and resource access reports
- 2) **SYS3.FSO.xxxx.mmmyyy.PDI** – Finding Analysis Detail reports.

These permanent data sets must be located on a domain accessible to the reviewing personnel and will be required for follow-up SRR data analysis. The data sets should be backed up and retained by the site for future reference.

---

\_\_\_ **1. Create work data sets used for subsequent processing.**

- \_\_\_ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.xxxx.mmmmyyyy.CNTL(CACJ0002)**.
- \_\_\_ b) Copy **SYS3.FSO.xxxx.mmmmyyyy.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.

**NOTE: It is recommended that the user that the JOB runs under not utilize SDSF until the JOB completes.**

- \_\_\_ c) Submit **CACJ0002** for execution. Review the job for error messages to ensure successful execution, particularly the following:
  - \_\_\_ 1) The ISPLOG and SYSTSPRT output files of each step.
  - \_\_\_ 2) The JOBLLOG or JESLOG files.

The **CACJ0002** job will create the following work data sets:

- a) **SYS3.FSO.xxxx.mmmmyyyy.TEMP1** - A copy of selected CA Auditor reports with special editing.
- b) **SYS3.FSO.xxxx.mmmmyyyy.TEMP2** - A copy of the JES2 initialization parameters and a copy of your DSNLIST member.
- c) **SYS3.FSO.xxxx.mmmmyyyy.TEMP3** - A list of data set names from EXAMINE reports and the DSNLIST you created.

The **CACJ0002** job will create members in the following data set:

**SYS3.FSO.xxxx.mmmmyyyy.PDI** - Finding Analysis Detail reports.

## ACF2 Data Set and Resource Data Collection

```
*****
* Follow the instruction in this Section only if the *
*               System is running ACF2               *
*****
```

### \_\_\_ 1. Produce the SENSITIVE data set access reports.

**Note:** *This job will utilize the backup of the Primary security database to create its own security database for use within this job. Ensure that the system has successfully been able to back up the Primary security database.*

- \_\_\_ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.xxxx.mmmmyyyy.CNTL(CAAJ0001)**.
- \_\_\_ b) Copy **SYS3.FSO.xxxx.mmmmyyyy.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.
- \_\_\_ c) Change the **SET JCL** command for symbolic **SRRAUL** to specify the Dialog data set created using the instructions in the *SRRAUDIT Dialog Management* document.
- \_\_\_ d) Submit **CAAJ0001** for execution. Review each of the job steps for error messages to ensure successful execution, particularly the following:
  - \_\_\_ 1) The ISPLOG and SYSTSPRT output files of each step.
  - \_\_\_ 2) The JOBLOG or JESLOG files.

The **CAAJ0001** job will create the following data set:

**SYS3.FSO.xxxx.mmmmyyyy.SENSITIVE.RPT** - Data set access reports.

The **CAAJ0001** job will create members in the following data set:

**SYS3.FSO.xxxx.mmmmyyyy.PDI** - Finding Analysis Detail reports.

The files will be referenced in the z/OS STIG under the Vulnerability Checks for subsequent analysis.



---

\_\_\_ 2. Produce the SENSITIVE resource access reports.

**Note:** *This job will utilize the alternate security database, ensure that the system has successfully been able to back up the Primary database and create the alternate security database. The alternate database must be as current as of the last backup of the Primary database.*

- \_\_\_ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.xxxx.mmmmyyyy.CNTL(CAAJ0002)**.
- \_\_\_ b) Copy **SYS3.FSO.xxxx.mmmmyyyy.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.

**Note:** This process will not list logonids when the Type Code is SAF.

- \_\_\_ c) Submit **CAAJ0002** for execution. Review the job for error messages to ensure successful execution, particularly the following:
  - \_\_\_ 1) The ISPLOG and SYSTSPRT output files of each step.
  - \_\_\_ 2) The JOBLOG or JESLOG files.

The **CAAJ0002** job will create members in the following data set:

**SYS3.FSO.xxxx.mmmmyyyy.SENSITIVE.RPT** - Resource access reports.

This file will be referenced in the z/OS STIG under the Vulnerability Checks for subsequent analysis.

## RACF Data Set and Resource Data Collection

```
*****
* Follow the instruction in this Section only if the *
*               System is running RACF               *
*****
```

### \_\_\_ 1. Create specialized RACF reports necessary to produce the SENSITIVE REPORTS.

- \_\_\_ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.xxxx.mmmyyy.CNTL(CARJ0001)**.
- \_\_\_ b) Copy **SYS3.FSO.xxxx.mmmyyy.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.
- \_\_\_ c) Submit **CARJ0001** for execution. Review the job for error messages to ensure successful execution, particularly the following:
  - \_\_\_ 1) The ISPLOG and SYSTSPRT output files of each step.
  - \_\_\_ 2) The JOBLOG or JESLOG files.

The **CARJ0001** job will add a member to **SYS3.FSO.xxxx.mmmyyy.TEMP2** file.

---

\_\_\_ **2. Produce the SENSITIVE data set and resource access reports.**

- \_\_\_ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.xxxx.mmmmyyyy.CNTL(CARJ0002)**.
- \_\_\_ b) Copy **SYS3.FSO.xxxx.mmmmyyyy.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.
- \_\_\_ c) Change the **SET JCL** command for symbolic **SRRAUL** to specify the Dialog data set created using the instructions in the *SRRAUDIT Dialog Management* document.
- \_\_\_ d) Submit **CARJ0002** for execution. Review each of the job steps for error messages to ensure successful execution, particularly the following:
  - \_\_\_ 1) The ISPLOG and SYSTSPRT output files of each step.
  - \_\_\_ 2) The JOBLOG or JESLOG files.

The **CARJ0002** job will create the following data set:

**SYS3.FSO.xxxx.mmmmyyyy.SENSITIVE.RPT** - Data set and Resource access reports.

The **CARJ0002** job will create members in the following data set:

**SYS3.FSO.xxxx.mmmmyyyy.PDI** - Finding Analysis Detail reports.

The files will be referenced in the z/OS STIG under the Vulnerability Checks for subsequent analysis.

## TSS Data Set and Resource Data Collection

```
*****
* Follow the instruction in this Section only if the *
*               System is running TSS               *
*****
```

### \_\_\_ 1. Produce the SENSITIVE data set and resource access reports.

- \_\_\_ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.xxxx.mmmmyyyy.CNTL(CATJ0001)**.
- \_\_\_ b) Copy **SYS3.FSO.xxxx.mmmmyyyy.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.
- \_\_\_ c) Change the **SET** JCL command for symbolic **SRRAUL** to specify the Dialog data set created using the instructions in the *SRRAUDIT Dialog Management* document.
- \_\_\_ d) Submit **CATJ0001** for execution. Review each of the job steps for error messages to ensure successful execution, particularly the following:
  - \_\_\_ 1) The ISPLOG and SYSTSPRT files of each report step
  - \_\_\_ 2) The JOBLLOG or JESLOG files.

The **CATJ0001** job will create the following data set:

**SYS3.FSO.xxxx.mmmmyyyy.SENSITIVE.RPT** - Data set and Resource access reports.

The **CATJ0001** job will create members the following data set:

**SYS3.FSO.xxxx.mmmmyyyy.PDI** - Finding Analysis Detail reports.

The files will be referenced in the z/OS STIG under the Vulnerability Checks for subsequent analysis.

## SRRDB Data Collection

Individuals that use the SRRDB Desktop Edition or the Web based VMS application should perform this process. This process is part of the Automation Tools used for z/OS. This process will remain as the last step before individuals begin the Data Analysis.

The data gathered will be saved in the following data set:

**SYS3.FSO.xxxx.mmmmyyyy.XMLDATA** – SRRDB Import File (VMS 6.0 and above)

This permanent data set must be located on a domain accessible to the reviewing personnel. This data set should be backed up and retained by the site for future reference.

### VMS 6.0 and above Asset Registration Information:

Asset Type
Computing

Asset Fields	Example
Host Name:	TEST.DISA.MIL
IP Address:	127.0.0.1 ( <b>optional</b> )
SYSNAME:	TEST

Asset Posture	
Operating System	Application
MVS	ACPs
z/OS	ACF2
	RACF
	TSS

**Note:** In this document, Enclave Certification Team Lead is referred to as the Team Lead. Additional Asset Postures are dependent on z/OS Products installed and used on the system.

**Note:** Currently VMS has not made the changes to identify OS390 as SYSNAME. Until this change is made this document will identify SYSNAME as a key field, and it represents the field OS390.

\_\_\_ 1. Produce the SRRDB Import data sets.

- \_\_\_ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.xxxx.mmmmyyyy.CNTL(CACJ0004)**.
- \_\_\_ b) Copy **SYS3.FSO.xxxx.mmmmyyyy.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.
- \_\_\_ c) Submit **CACJ0004** for execution. Review each of the job steps for error messages to ensure successful execution, particularly the following:
  - \_\_\_ 1) The ISPLOG and SYSTSPRT output files of each step.
  - \_\_\_ 2) The JOBLOG or JESLOG files.

The **CACJ0004** job will create the following data sets:

**SYS3.FSO.xxxx.mmmmyyyy.XMLDATA** – SRRDB Import file for VMS 6.0 and above.

These files can be downloaded and used as the *Script Import* to the VMS application.

**NOTE:** If the above data sets are downloaded, it is recommended the each text file be reviewed after the data sets are downloaded. Delete the end-of-file indicator from each file. The end-of-file indicator is located at the end of the file and look like a square, (). Delete this character before importing file into VMS.

If these files are zipped using **SYS3.FSO.xxxx.mmmmyyyy.CNTL(ZIPJCL)** and the **SYS3.FSO.xxxx.mmmmyyyy.ZIP** is downloaded. The removal of the square () is not necessary.

---

**The remaining steps are instructions to import the finding details into VMS 6.0****\_\_\_ 2. Download information.**

**NOTE:** There are two (2) possible options on the process to download the information for VMS.

- \_\_\_ a) Using any 3270 Terminal Host Emulation or File Transfer Protocol software, establish a host connection.
- \_\_\_ b) Initiate the upload/download function of the 3270 Terminal Host Emulation or File Transfer Protocol software
  - \_\_\_ 1) Enter '**SYS3.FSO.xxxx.mmmmyyy.XMLDATA**' (ensure that the data set name is in quotes) for the Host File Name
  - \_\_\_ 2) Enter a drive, directory, and file name using **xml** extension for the PC File Name.  
(e.g. D:\directory\_name\xxxx.mmmmyyy.xmldata.xml)
  - \_\_\_ 3) Ensure that the Transfer Mode is set to **Text**.
  - \_\_\_ 4) Ensure that Transfer Options are set to **ASCII CRLF**.
  - \_\_\_ 5) Initiate the file transfer.

**NOTE:** The other option for downloading is to follow these steps:

- \_\_\_ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.xxxx.mmmmyyy.CNTL(ZIPJCL)**.
- \_\_\_ b) Copy **SYS3.FSO.xxxx.mmmmyyy.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement. This includes changes stated in the JCL comments.
- \_\_\_ c) Submit **ZIPJCL** for execution. Review each of the job steps for error messages to ensure successful execution, particularly the following:

The SYSPRINT output file.

The **ZIPJCL** job will create the following data set:

**SYS3.FSO.xxxx.mmmmyyy.ZIP** – Zip file that contains all data sets/members process during the Data Collection Process.

- \_\_\_ d) establish a host connection using any 3270 Terminal Host Emulation or File Transfer Protocol software.
- \_\_\_ e) Initiate the upload/download function of the 3270 Terminal Host Emulation or File Transfer Protocol software
  - \_\_\_ 1) Enter '**SYS3.FSO.xxxx.mmmmyyy.ZIP**' (ensure that the data set name is in quotes) for the Host File Name
  - \_\_\_ 2) Enter a drive, directory, and file name using **zip** extension for the PC File Name.  
(e.g. D:\directory\_name\xxxx.mmmmyyy.zip)
  - \_\_\_ 3) Ensure that the Transfer Mode is set to **Binary**.
  - \_\_\_ 4) Initiate the file transfer.



---

### 3. Modifications to XMLDATA file after download.

After downloading the SRRDB Import file for VMS 6.0 from instructions in the above step, ensure the following are performed on the text file. Confirm the asset information in VMS matches the asset information found in the XML import file. In this asset example, the **Host Name** is **TEST.DISA.MIL** and the **SYSNAME** is **TEST**. This information is found at the beginning of the XMLDATA text file:

- a) Obtain Asset information from one or both of the following locations:

The following information is found at the beginning of the downloaded XMLDATA text file (Use notepad to view this file):

```
<?xml version="1.0"?>
<IMPORT_FILE xmlns="urn:FindingImport">
<AUTHENTICATED>true</AUTHENTICATED>
<ASSET>
<ASSET_ID TYPE="ASSET NAME">TEST.DISA.MIL</ASSET_ID>
<ASSET_ID TYPE="HOST NAME">TEST.DISA.MIL</ASSET_ID>
<ASSET_ID TYPE="IP ADDRESS">127.0.0.1</ASSET_ID>
<ASSET_ID TYPE="SYSNAME">TEST</ASSET_ID>
<ASSET_TOOL>MVSSSCRIPTS</ASSET_TOOL>
<ASSET_TOOL_VERSION>5.12 042706_52</ASSET_TOOL_VERSION>
<ELEMENT><ELEMENT_KEY>106</ELEMENT_KEY>
<ELEMENT_DESCRIP>MVS z/OS</ELEMENT_DESCRIP></ELEMENT>
<ELEMENT><ELEMENT_KEY>197</ELEMENT_KEY>
<ELEMENT_DESCRIP>ACPs RACF</ELEMENT_DESCRIP></ELEMENT>
```

This information is also found in the output from DD SYSTSPRT of STEP4 in job CACJ0004. The following is an example:

```
CACC1000 04/27/06 Security Readiness Review Self-Auditing Version 5.12 Rel...
CACC1000 04/27/06 MVS System z/OS Version 1.04 Running on system TEST/TESTPLEX
CACC1000 04/27/06 RACF Version 7.707 is running on this system.
CACC1000 04/27/06 The system has a HOST name of TEST.DISA.MIL.
CACC1000 04/27/06 The system has the following IP Addresses assigned:
CACC1000 04/27/06 127.0.0.1
CACC1000 04/27/06 end of messages.
```

**Note:** Information marked in **bold/underline** in the above examples will be used in later steps to determine the Asset Identification and Posture. Make note of the operating system and the ACP (e.g., z/OS and RACF). Also make note of the HOST NAME, SYSNAME, and optional IP ADDRESS entries (e.g., TEST.DISA.MIL, TEST, and 127.0.0.1).

- \_\_\_ b) Ensure the white square (□) has been removed from the end of XMLDATA file.

```
</IMPORT_FILE>  
□
```

**Note:** Delete the end-of-file indicator from each file. The end-of-file indicator is located at the end of the file and look like a white square, (□). If the XMLDATA file is zipped using **SYS3.FSO.xxxx.mmmyyyy.CNTL(ZIPJCL)** and the **SYS3.FSO.xxxx.mmmyyyy.ZIP** is downloaded. The removal of the white square (□) is not necessary.

- \_\_\_ c) Save all resulting changes.

---

## Navigating through the VMS Web Application.

### \_\_\_ 4. Selecting Asset for Verification.

**Note:** In this document, Enclave Certification Team Lead is referred to as the Team Lead.

- \_\_\_ a) Access VMS 6.0 Web Application.
- \_\_\_ b) Click 'Asset Finding Maint.' in left column and Click 'Assets / Findings'.
- \_\_\_ c) Expand 'Visits' (Reviewers will navigate to the vulnerabilities through the visit.).

Note: If the visit is not visible contact the Team Lead. The MVS reviewer has not been designated at the visit level as a reviewer.

- \_\_\_ d) Expand the Visit name, Summary Form identifier, and owner name (e.g., 'GO4-Field Security Operations').

**Note:** The Visit name and Summary Form identifier are identified during the creation of the visit. The Team lead will have the information pertaining to these entries.

- \_\_\_ e) Expand 'Computing', then 'Must Review'.

The Team Lead has designated assets under 'Must Review', 'Reviewed', or 'Not Selected for Review'. If the asset is not visible contact the Team Lead, the MVS reviewers will not create an asset.

- \_\_\_ f) Click the asset to be reviewed. This will display the asset information entries on the right side of the screen.

## \_\_\_ 5. Verify Asset Information.

This step will require information collected in step 3. The information will ensure that the XMLDATA file will import correctly into the VMS application.

### VMS 6.0 and above Asset Registration Information:

Asset Type
Computing

The following fields are the key fields used in the script import process to determine the asset for z/OS assets. If these asset fields are not properly completed, the import process will fail to locate the asset. This will prevent the automated vulnerabilities from being reported on in the VMS application.

Asset Fields	Example
Host Name:	TEST.DISA.MIL
IP Address:	127.0.0.1 ( <b>optional</b> )
SYSNAME:	TEST

- \_\_\_ a) Click the 'General' tab, ensure the asset is registered in VMS under the correct organization and to confirm the 'Host Name' entry to the HOST NAME collected in Step 3 (e.g., TEST.DISA.MIL). Make changes as necessary.
- \_\_\_ b) Click the 'Asset Identification' tab to confirm the SYSNAME entry to the SYSNAME entry collected in Step 3 (e.g., TEST). Make changes as necessary.

Asset Posture	
Operating System	Application
MVS	ACPs
z/OS	ACF2
	RACF
	TSS

- \_\_\_ c) Click the 'Asset Posture' tab:

In the 'Selected:' box, expand the Host Name on the right side of the screen and confirm that the correct Operating System (e.g. z/OS) and Application (ACP) associated with this asset (e.g., ACF2, RACF, or TSS) are listed.

**Note:** The Operating System and ACP were identified above in step 2. (e.g., z/OS and RACF)

If the Operating System and/or Application are incorrect or not specified, use the double arrow buttons to remove (<<) and add (>>) checked elements in the asset.

- \_\_\_ d) Click the 'Systems / Enclaves' tab:

Insure that the Selected Systems and/or Enclaves specify one or more entries. If nothing is specified, contact team lead to determine which Available Systems and/or Enclaves are to be added to the asset.

If the Selected Systems and/or Enclaves are incorrect or not specified, use the double arrow buttons to remove (<<) and add (>>) selected Systems and/or Enclaves to the asset.

- \_\_\_ e) If any changes are made to the asset, click the 'Save' icon at bottom of screen.

\_\_\_ **6. Import the XMLDATA file into VMS.**

To import the *script import* file, select the XML icon next to Computing.

- \_\_\_ a) Click the Browse button and locate the modified XMLDATA file. This file was modified in Step 3 above.
- \_\_\_ b) Click the Submit button.
- \_\_\_ c) Review the Script Results from the Script Import.