z/OS
SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG)
INSTRUCTION

Version 6, Release 35

26 January 2018

Developed by DISA for the DoD

TABLE OF CONTENTS

Page

Summary of Changes

Revision Number	Document Revised	Description of Change	Release Date
V6R34	V6R33 (27 Oct 2017)	No changes made to this document.	17 November 2017
V6R33	V6R32 (28 July 2017	Added SMTSTC entries for DSNLIST	27 October 2017
V6R32	V6R31 (28 April 2017)	Added CASECAUT resource for TSS for resources Auditors may require. Updated list of Authorized User Groups.	28 July 2017
V6R30	V6R29 (28 Oct 2016)	Removed unnecessary product instructions. Added CA1STC to DSNLIST instructions.	27 January 2017
V6R29	V6R28 (22 July 2016)	Added RACFREXX and SYSREXX entries to the Dataset Group table.	28 October 2016

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 U_zOS_V*x*R*xx*_SRR.zip to the host.**

___ a) Allocate two 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.V*vrr*.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.V*vrr*.JCL(RESTJCL).** Ensure that Transfer Options are set to **ASCII CRLF**.

___ 2) Perform a **Binary** transfer of **V*x*R*xx*.DUMP.xmi** to create **SYS3.FSO.V*vrr*.DUMP.XMI.** 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.V*vrr*.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.V*vrr*.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.V*vrr*.DUMP
SYS3.FSO.V*vrr*.DUMP.XMI
SYS3.FSO.V*vrr*.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:	**SRR - site *name* - *xxxx***
Maximum lines per page:	**55** (suggested)
Report destination:	**LOCAL**
Sysout class:	**X** (must be a JES held output class)
Upper case:	**YES** (suggested)
Allocated hold:	**YES**

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:

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

___ b) Ensure that all Products are identified.

___ c) Ensure that all Vulnerability Questions are answered.

___ d) Ensure that the Asset Definition 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 resources 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		
General	FACILITY	IRR.DIGTCERT.LIST	CONTROL	No
RACF	OPERCMDS	MVS.MODIFY.STC.AXR.*	UPDATE	Yes
RACF	OPERCMDS	MVS.SYSREXX.EXECUTE.*	READ	No
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
TSS	CASECAUT	TSSCMD.ADMIN.MODIFY	USE	No
WebSphere MQ	PROGRAM	CSQUTIL	EXECUTE	No
WebSphere MQ	MQCONN	*ssid*.BATCH	READ	No
WebSphere MQ	MQCMDS	s*sid*.DISPLAY.	READ	No
WebSphere MQ	MQQUEUE	s*sid*.SYSTEM.COMMAND.INPUT	UPDATE	No
WebSphere MQ	MQQUEUE	s*sid*.SYSTEM.COMMAND.REPLY	UPDATE	No
WebSphere MQ	MQQUEUE	s*sid*.SYSTEM.CSQUTIL.-	UPDATE	No
Unix System Services	UNIXPRIV	SUPERUSER.FILESYS	READ	No
Unix System Services	FACILITY	BPX.SUPERUSER	READ	No
CA Auditor	FACILITY	CSVDYNEX.LIST	READ	No
CA Auditor	PROGRAM	LTDMMAIN	EXECUTE	No

___ **7. Modify members in SYS3.FSO.*xxxx.mmmyyyy*.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.mmmyyyy*.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 CICS regions:

```
CA CICSJ1    CICS                        ZCICR010  ZCICT010  ZCICA010
CA DFHSTART  CICS                        ZCICR010  ZCICT010  ZCICA010
CA CICST1    CICS                        ZCICR010  ZCICT010  ZCICA010
CA CICSP1    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 **SENSITVE.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*.*mmmyyyy*.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 **SENSITVE.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**.

Identifier Code	Dataset Group	Report Name	Note
AA	SYS1.PARMLIB (Logical Parmlib data sets)	PARMRPT	[1]
AB	SYS1.LINKLIB	LINKRPT	[2]
AC	SYS1.SVCLIB	SVCRPT	[2]
AD	SYS1.IMAGELIB	IMAGERPT	[2]
AE	SYS1.LPALIB	LPARPT	[2]
AF	SYS1.NUCLEUS	NUCLRPT	[2]
AG	SYS1.UADS	UADSRPT	[3]
AH	SYS1.DUMP	DUMPRPT	[3 4]
AI	SYS1.TRACE	TRACERPT	[2 4]
AJ	RACF REXX Exit Datasets	RACFREXX	[5]
AK	System REXX Datasets	SYSREXX	[5]
BA	APF-authorized	APFXRPT	[6]
BB	LINKLIST	LNKXRPT	[6]
BC	LPA	LPAXRPT	[6]
BD	Libraries containing PPT modules	PPTXRPT	[6]
BE	Libraries containing system exits	MVSXRPT	[6]
BF	TSO APF-authorized	APFTRPT	[6]
BG	SMF collection (i.e., SYS1.MAN)	SMFXRPT	[3 6]
BH	JES2 procedures	PROCRPT	[3 7]
BI	Master System catalog	CATMRPT	[3]
BJ	System User catalogs	CATURPT	[3 6]
BK	SMP/E installation (i.e., CSIs)	SMPERPT	[6]
BL	System PAGE	PGXXRPT	[3]
BM	JES2 System data sets	JES2RPT	[6]
BN	SMF dump/backup	SMFBKRPT	[4 8]
BO	System DASD backup	BKUPRPT	[4 8]
BP	ACP and security-related	ACPRPT	[3 9]
BQ	System-level product installation	PRODRPT	
BR	FDR Installation Datasets	FDRRPT	[8]
BS	IBM Health Checker STC Data Sets	HCKSTC	[8]
C0	Compuware Abend-Aid User Data Sets	AIDUSER	[8]
C1	CA VTAPE Installation Data Sets	VTAPERPT	[8]
C2	BMC MAINVIEW for z/OS STC Data Sets	MVZSTC	[8]
C3	BMC MAINVIEW for z/OS Installation Data Sets	MVZRPT	[8]
C4	Compuware Abend-Aid STC Data Sets	AIDSTC	[8]

[1] SYS1.PARMLIB and/or Logical Parmlib obtained from System Control Blocks that are set during an IPL.
[2] Datasets are hard coded within the script.
[3] Datasets obtained from commands and/or System Control Blocks available to the system.
[4] Additional data sets can be obtains from detailed instructions.
[5] Data sets enqueued to ARX Started Tasks.
[6] The data sets for this group are obtained from SYS3.FSO.xxxx.mmmyyyy.EXAM.RPT data set.
[7] The data sets for this group are obtained from the STC's JCL.
[8] Data sets obtained from information requested in the Dialog Process.
[9] Data sets obtained from Product reports and/or within data sets.

Identifier Code	Dataset Group	Report Name	Note
C5	Compuware Abend-Aid Installation Data Sets	AIDRPT	8
C6	CA MIM STC Data Sets	MIMSTC	8
C7	CA MIM Installation Data Sets	MIMRPT	8
C8	CA MICS User Data Sets	MICSUSER	8
C9	CA MICS Installation Data Sets	MICSRPT	8
CA	CICS STC Data Sets	CICSSTC	4 8
CB	FEP/NCP	NCPRPT	4 8
CC	VTAM	VTAMRPT	8
CD	NC-PASS STC Data Sets	NCPASSTC	8
CE	UNIX HFS Files	HFSRPT	3
CF	UNIX System Services	USSRPT	4
CG	UNIX STEPLIBLIST	STLLRPT	3
CH	CL/SuperSession STC Data Sets	KLSSTC	8
CI	DFSMS	SMSRPT	4 9
CJ	CA 1 (TMC, AUDIT, and optional RDS and VPD data sets)	CA1RPT	9
CK	CA 1 Started Task data sets	CA1STC	8
CL	WebSphere MQ	MQSRPT	4
CM	TCPIP	TCPRPT	4
CN	CA Auditor (CA Examine) User Data Sets	ADTUSER	8
CO	CA Auditor (CA Examine) Installation Data Sets	ADTRPT	8
CP	HTTP	HTTPRPT	4
CQ	CICS Installation Data Sets	CICSRPT	4 8
CR	FTP	FTPRPT	4 9
CS	WebSphere Application Service	WASRPT	4
CT	SDSF	ISFRPT	8
CU	HASPINDX	SDSFRPT	3
CV	NETVIEW STC Data Sets	NETVSTC	8
CW	NETVIEW Installation Data Sets	NETVRPT	8
CX	TADz STC Data Sets	TADZSTC	8
CY	TADz Installation Data Sets	TADZRPT	8
CZ	CA VTAPE STC Data Sets	VTAPESTC	8
D0	CONTROL-M/Restart Installation/Operations Data Sets	CTRRPT	8
D1	CONTROL-O User Data Sets	CTOSTC	8
D2	CONTROL-O Install/Operations Data Sets	CTORPT	8
DA	CA 1 Installation Data Sets	CA1PROD	8
DB	Catalog Solution Installation Data Sets	CSLPROD	8
DC	CL/SuperSession Installation Data Sets	KLSRPT	8
DD	NC-PASS Installation Data Sets	NCPASRPT	8
DE	SRRAUDIT User Data Sets	SRRUSER	8
DF	SRRAUDIT Installation Data Sets	SRRPROD	8
DG	ROSCOE STC Data Sets	ROSCSTC	8
DH	ROSCOE Installation Data Sets	ROSCRPT	8

Identifier Code	Dataset Group	Report Name	Note
DI	TDMF Installation Data Sets	TDMFRPT	8
DJ	VSS User Data Sets	VSSUSER	8
DK	VSS Installation Data Sets	VSSRPT	8
DL	HCD User Data Sets	HCDUSER	8
DM	HCD Installation Data Sets	HCDRPT	8
DN	ICSF STC Data Sets	ICSFSTC	8
DO	ICSF Installation Data Sets	ICSFRPT	8
DP	INCONTROL (IOA) User Data Sets	IOAUSER	8
DQ	INCONTROL (IOA) STC Data Sets	IOASTC	8
DR	INCONTROL (IOA) Installation Data Sets	IOARPT	8
DS	CONTROL-D User Data Sets	CTDUSER	8
DT	CONTROL-D STC Data Sets	CTDSTC	8
DU	CONTROL-D Installation Data Sets	CTDRPT	8
DV	CONTROL-M User/Application JCL Data Sets	CTMJCL	8
DW	CONTROL-M User Data Sets	CTMUSER	8
DX	CONTROL-M STC Data Sets	CTMSTC	8
DY	CONTROL-M Installation Data Sets	CTMRPT	8
DZ	CONTROL-M/Restart User Data Sets	CTRUSER	8
EA	CA Common Services Installation Data Sets	CCSRPT	8
EB	CSSMTP STC Datasets	SMTSTC	8

Note: All references for data set masks are used to collect data sets that may be associated with the Dataset Group. The list of data sets should be reviewed to ensure that the data sets collected are associated to the Dataset Group.

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

Example: Additional data set masks (such as ****.*BPX***, ****BPA***, ****CMX***, ****OMVS***, ****.*FOM***.) are used to collect data sets associated with the Dataset Group. The list of data sets should be reviewed to ensure that the data sets collected are associated to the Executive software being reviewed and not data sets 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.

Additional Trace data sets 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 **HSMPARM** 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(CICSPROC)**. CICS system data set names are identified by DD names beginning with **DFH**. These data sets 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.

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

➔ 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***.
➔ 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* JESMSGLG. 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***.

➔ TCPIP – 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**.

➔ 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 are maintained by the system programming personnel. These data sets 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.SCEEOBJ**.

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

___ a) Review, edit, and make changes where necessary to **SYS3.FSO.*xxxx.mmmyyyy*.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-character Resource Class name, **starting in column 1**, and a three-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 and 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 online 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.mmmyyyy*.EXAM.RPT** – CA Auditor reports
2) **SYS3.FSO.*xxxx.mmmyyyy*.PARMLIB** – Copies of various system parmlib members
3) **SYS3.FSO.*xxxx.mmmyyyy*.PARMLIB.ACCESS** – Inaccessible data sets referred to in SYS1.PARMLIB
4) **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. Submit JCL to execute the batch CA Auditor job.**

___ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.*xxxx.mmmyyyy*.CNTL(EXAMJOB)**.

___ b) Copy **SYS3.FSO.*xxxx.mmmyyyy*.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.mmmyyyy*.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 online 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 online.

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*.*mmmyyyy*.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*.*mmmyyyy*.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.mmmyyyy*.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.mmmyyyy*.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.mmmyyyy*.CNTL(CACJ0001)**.

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

The following is an example:

ISPSTART CMD(%CACC0003 TERMMSGS(ON) +
PARMDSN(SYS2.PARMLIB))

Or

ISPSTART CMD(%CACC0003 TERMMSGS(ON) +
PARMDSN('SYS2.PARMLIB SYS1.PARMLIB'))

___ b) Copy **SYS3.FSO.*xxxx.mmmyyyy*.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 JOBLOG or JESLOG files

The **CACJ0001** job will create the data sets **SYS3.FSO.*xxxx.mmmyyyy*.PARMLIB.ACCESS** and **SYS3.FSO.xxxx.mmmyyyy.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	*ssid*.BATCH	READ
MQCMDS	s*sid*.DISPLAY.	READ
MQQUEUE	s*sid*.SYSTEM.COMMAND.INPUT	UPDATE
MQQUEUE	s*sid*.SYSTEM.COMMAND.REPLY	UPDATE
MQQUEUE	s*sid*.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 on the products used on the system.

___ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.*xxxx*.*mmmyyyy*.CNTL(CACJ0005)**.

___ b) Copy **SYS3.FSO.*xxxx*.*mmmyyyy*.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.mmmyyyy.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.mmmyyyy*.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.mmmyyyy*.CA1RPT – CA 1 utility reports
SYS3.FSO.*xxxx.mmmyyyy*.CONSOLE – CA Examine Console report
SYS3.FSO.*xxxx.mmmyyyy*.MQSRPT – WebSphere MQ utility reports
SYS3.FSO.*xxxx.mmmyyyy*.IOA.RPT – IOA product configuration data
SYS3.FSO.*xxxx.mmmyyyy*.SMFOPTS – CA Examine SMF Options report
SYS3.FSO.*xxxx.mmmyyyy*.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.mmmyyyy*.CNTL(ACF2CMDS)**.

___ b) Copy **SYS3.FSO.*xxxx.mmmyyyy*.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 JOBLOG or JESLOG files

The **ACF2CMDS** job will create the PDS **SYS3.FSO.*xxxx.mmmyyyy*.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.mmmyyyy*.CNTL(ACFLSTA)**.

___ b) Copy **SYS3.FSO.*xxxx.mmmyyyy*.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 JOBLOG or JESLOG files

The **ACFLSTA** job will create the data set **SYS3.FSO.*xxxx.mmmyyyy*.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*.*mmmyyyy*.ALIAS.RPT** – Master Catalog aliases
2) **SYS3.FSO.*xxxx*.*mmmyyyy*.DSMON.RPT** – RACF DSMON reports
3) **SYS3.FSO.*xxxx*.*mmmyyyy*.RACFCMDS.RPT** – RACF command reports
4) **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 RACF command reports.**

___ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.*xxxx.mmmyyyy*.CNTL(RACFCMD1)**.

___ b) Copy **SYS3.FSO.*xxxx.mmmyyyy*.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.mmmyyyy*.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.mmmyyyy*.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.mmmyyyy*.CNTL(RACFCMD2)**.

___ b) Copy **SYS3.FSO.*xxxx.mmmyyyy*.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.mmmyyyy*.ALIAS.RPT – A list of Master Catalog aliases

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

SYS3.FSO.*xxxx.mmmyyyy*.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*.*mmmyyyy*.CNTL(CARJ0003)**.

___ b) Copy **SYS3.FSO.*xxxx*.*mmmyyyy*.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*.*mmmyyyy*.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.mmmyyyy*.TSSCMDS.RPT** – TSS command reports
2) **SYS3.FSO.*xxxx.mmmyyyy*.TSSDUMP.RPT** – IDCAMS report
3) **SYS3.FSO.*xxxx.mmmyyyy*.ALIAS.RPT** – Master Catalog aliases
4) **SYS3.FSO.*xxxx.mmmyyyy*.TSSPRIV.RPT** – TSS privileges (short) report
5) **SYS3.FSO.*xxxx.mmmyyyy*.TSSCHNGS.RPT** – TSS changes report
6) **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. 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.mmmyyyy*.CNTL(TSSCMDS)**. Change the SET JCL statement for TSSINSTX to specify the data set that contains the **TSSINSTX** load module. Refer to comments in the JCL on determining the data set that contains the **TSSINSTX** load module.

___ b) Copy **SYS3.FSO.*xxxx.mmmyyyy*.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.mmmyyyy*.TSSCMDS.RPT, SYS3.FSO.*xxxx.mmmyyyy*.TSSDUMP.RPT**, and **SYS3.FSO.*xxxx.mmmyyyy*.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.mmmyyyy*.CNTL(TSSLSTA)**.

___ b) Copy **SYS3.FSO.*xxxx.mmmyyyy*.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 JOBLOG or JESLOG files

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

SYS3.FSO.*xxxx.mmmyyyy*.ALIAS.RPT, which contains a list of Master Catalog aliases.
SYS3.FSO.*xxxx.mmmyyyy*.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.mmmyyyy*.CNTL(TSSAUDIT)**.

___ b) Copy **SYS3.FSO.*xxxx.mmmyyyy*.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.mmmyyyy*.TSSPRIV.RPT, saving a report on special privileges.
SYS3.FSO.*xxxx.mmmyyyy*.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*.*mmmyyyy*.TSSCMDS.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.mmmyyyy*.CNTL(TSSCMD2),** following the instructions within the comment block at the beginning of the JCL.

___ b) Copy **SYS3.FSO.*xxxx.mmmyyyy*.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.

___ c) Review **SYS3.FSO.*xxxx.mmmyyyy*.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., ISSO). 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.mmmyyyy*.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.mmmyyyy*.CNTL(TSSCMD3)** using the following instructions by reviewing:

1) **SYS3.FSO.*xxxx.mmmyyyy*.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.mmmyyyy*.TSSCMDS.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.mmmyyyy*.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.

___ g) Have the site security personnel (e.g., ISSO) 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.mmmyyyy*.TSSCMDS.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.mmmyyyy*.CNTL(TSSCMD4),** following the instructions within the comment block at the beginning of the JCL.

___ b) Copy **SYS3.FSO.*xxxx.mmmyyyy*.CNTL(JOBCARD)** to the beginning of member and make any changes needed to the JOB statement.

___ c) Submit **TSSCMD4** 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.mmmyyyy*.TSSCMDS.RPT(FACALL)
SYS3.FSO.*xxxx.mmmyyyy*.TSSCMDS.RPT(FACLIST)
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.mmmyyyy*.CNTL(CATJ0002)**.

___ b) Copy **SYS3.FSO.*xxxx.mmmyyyy*.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.mmmyyyy*.PDI – Finding Analysis Detail reports

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.mmmyyyy*.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.mmmyyyy*.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) the SYSIN data set, CICS will use the unsuffixed module named **DFHSIT**.

___ b) Copy **SYS3.FSO.*xxxx.mmmyyyy*.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.mmmyyyy*.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.

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*.*mmmyyyy*.SENSITVE.RPT** – Data set and resource access reports
2)**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. Create work data sets used for subsequent processing.**

___ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.*xxxx.mmmyyyy*.CNTL(CACJ0002)**.

___ b) Copy **SYS3.FSO.*xxxx.mmmyyyy*.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 JOBLOG or JESLOG files

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

a) **SYS3.FSO.*xxxx.mmmyyyy*.TEMP1** – A copy of selected CA Auditor reports with special editing

b) **SYS3.FSO.*xxxx.mmmyyyy*.TEMP2** – A copy of the JES2 initialization parameters and a copy of your DSNLIST member

c) **SYS3.FSO.*xxxx.mmmyyyy*.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.mmmyyyy*.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 SENSITVE data set access reports.**

Note: This job will use 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.mmmyyyy*.CNTL(CAAJ0001)**.

___ b) Copy **SYS3.FSO.*xxxx.mmmyyyy*.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.mmmyyyy*.SENSITVE.RPT – Data set access reports

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

SYS3.FSO.*xxxx.mmmyyyy*.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 SENSITVE resource access reports.**

Note: This job will use 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.mmmyyyy*.CNTL(CAAJ0002)**.

___ b) Copy **SYS3.FSO.*xxxx.mmmyyyy*.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.mmmyyyy*.SENSITVE.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.mmmyyyy*.CNTL(CARJ0001)**.

___ b) Copy **SYS3.FSO.*xxxx.mmmyyyy*.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.mmmyyyy*.TEMP2** file.

___ **2. Produce the SENSITVE data set and resource access reports.**

___ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.*xxxx.mmmyyyy*.CNTL(CARJ0002)**.

___ b) Copy **SYS3.FSO.*xxxx.mmmyyyy*.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.mmmyyyy*.SENSITVE.RPT – Data set and Resource access reports

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

SYS3.FSO.*xxxx.mmmyyyy*.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 SENSITVE data set and resource access reports.**

___ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.*xxxx*.*mmmyyyy*.CNTL(CATJ0001)**.

___ b) Copy **SYS3.FSO.*xxxx*.*mmmyyyy*.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 JOBLOG or JESLOG files

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

SYS3.FSO.*xxxx*.*mmmyyyy*.SENSITVE.RPT – Data set and Resource access reports

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

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

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

XMLDATA Data Collection

Individuals that use a Web-based vulnerability tracking 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.mmmyyyy*.XMLDATA – XMLDATA Import File

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.

___ **1. Produce the XMLDATA Import data sets.**

___ a) Review the JCL, edit, and make changes where necessary to **SYS3.FSO.*xxxx.mmmyyyy*.CNTL(CACJ0004)**.

___ b) Copy **SYS3.FSO.*xxxx.mmmyyyy*.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.mmmyyyy*.XMLDATA** – SRRDB Import file

Note: If the above data set can be downloaded, it is recommended the each text file be reviewed after the data set is downloaded. Delete the end-of-file indicator from each file. The end-of-file indicator is located at the end of the file and looks like a square, (). Delete this character.

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

___ 2. Download information.

Note: There are two possible options on the process to download the information to a PC.

___ 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*.*mmmyyyy*.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*.*mmmyyyy*.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.mmmyyyy*.CNTL(ZIPJCL)**.

___ b) Copy **SYS3.FSO.*xxxx.mmmyyyy*.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.mmmyyyy*.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.mmmyyyy*.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.mmmyyyy*.**zip**).

___ 3) Ensure that the Transfer Mode is set to **Binary**.

___ 4) Initiate the file transfer.

___ **3. Importing XMLDATA file into web-based vulnerability tracking application.**

To be determined.