zSecure 3.2

Compliance Standards

September 2025

This edition applies to the zSecure 3.2 lists of controls for September 2025.

Contents

Chapter 1. About zSecure controls

This document provides an overview of the compliance standards that are available in zSecure 3.2. These standards are included with the zSecure 3.2 code that became available on 30 September 2025.

The versions listed in this document represent the latest versions at the time of publication of this document.

In the following chapters, "Not supported" means that the control is not supported within zSecure; therefore, there is no CARLa member.

Summary of changes since zSecure 3.1 (July 2025)

Versions of the standards were updated. You can view the updated version at “Compliance standards categories and versions” on page 2.

- Automation for the following DISA controls introduced in z/OS® STIG 9.05 is added:

RACF®-IC-000060	ICSF resource class(es) must be active in accordance with security requirements.
ACF2-IC-000050	ICSF resource class(es) must be defined to the ACF2 GSO CLASMAP record in accordance with security requirements.
RACF-ZO-000010 ACF2-ZO-000010	z/OSMF resource class(es) must be active in accordance with security requirements.

- Automation for the following existing but previously not supported z/OS DISA STIG controls is added:

RACF-SH-000060 ACF2-OS-000330 TSS0-ES-000100	IBM® z/OS for PKI-based authentication must use the ICSF or ESM for key management.
RACF-OS-000240 ACF2-OS-000240 TSS0-OS-000100	The IBM z/OS Policy Agent must be configured to deny-all, allow-by-exception firewall policy for allowing connections to other systems.
RACF-OS-000370 ACF2-OS-000370 TSS0-OS-000150	The IBM z/OS Policy Agent must contain a policy that manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of Denial of Service (DoS) attacks.
RACF-OS-000140 ACF2-OS-000110 TSS0-OS-000240	IBM z/OS SMF collection files (system MANx data sets or LOGSTREAM DASD) must have storage capacity to store at least one week of audit data.
RACF-OS-000360 ACF2-OS-000360 TSS0-OS-000300	The IBM z/OS Policy Agent must contain a policy that protects against or limits the effects of Denial of Service (DoS) attacks by ensuring IBM z/OS is implementing rate-limiting measures on impacted network interfaces.
RACF-OS-000320 ACF2-OS-000340 TSS0-OS-000320	The IBM z/OS systems requiring data-at-rest protection must properly employ IBM DS8880 or equivalent hardware solutions for full disk encryption.

RACF-SM-000040	IBM z/OS DFSMS resources must be protected in accordance with the proper security requirements.
ACF2-US-000040	IBM z/OS UNIX resources must be protected in accordance with security requirements.
RACF-US-000070	IBM z/OS UNIX resources must be protected in accordance with security requirements.

- Automation for the following IBM zSecure for ACF2 STIG control is added:

ZSEC-00-000100	Started tasks for IBM zSecure products must be properly defined.

- Automation for the following CIS IBM z/OS RACF Benchmark controls is added:

CIS-OS-6.2.3	Ensure FTP.DATA configuration statements enforce secure configuration.
CIS-OS-6.4.2	Ensure Syslog daemon is secured.
CIS-OS-6.5.4	Ensure PROFILE.TCPIP configuration statements for the TCP/IP stack are defined.
CIS-OS-6.5.8	Ensure started tasks for the base TCP/IP component are defined securely in RACF.
CIS-OS-6.6.1	Ensure configuration statements for the TN3270E Telnet server are configured.
CIS-OS-9.1	Ensure that z/OS UNIX SURROGAT resources are protected.

- Automation for the following CIS IBM Db2® for z/OS Benchmark controls is added:

CIS-DB2®-2.1.6	Secure connections by using trusted contexts.
CIS-DB2-2.1.7	Secure object ownership by using Db2 roles.
CIS-DB2-3.1.5	Enable auditing of system administrator access.
CIS-DB2-3.1.6	Enable auditing of database administrator access.

- Automation for the following DB2 control is added in ACF2 and the CARLa member that stores the control is renamed from CKAHD213 to C2RHD213:

CIS-DB2-2.1.3	Secure access by using IBM Z® Multi-Factor Authentication (MFA).

The updates are indicated by revision bars in the left margin of the PDF file for this version. The PDF files of this and previous versions of this document are included in technote IBM zSecure 3.2 Compliance Standards (September 2025).

Compliance standards categories and versions

The US Defense Information Systems Agency Security Technical Implementation Guide (DISA STIG) controls are divided into the following standards categories and versions:

This table outlines the categories of DISA STIG controls and related security standards for IBM z/OS environments.

	Version RACF	**Version ACF2**	**Version Top Secret**
“CIS IBM z/OS RACF Benchmark” on page 5	1.1.0		
“CIS IBM Db2 for z/OS Benchmark (RACF)” on page 12[1]	1.0.0		
“CIS IBM Db2 for z/OS Benchmark (ACF2)” on page 37[1]		1.0.0	

This table outlines the categories of DISA STIG controls and related security standards for IBM z/OS environments. *(continued)*			
	Version RACF	**Version ACF2**	**Version Top Secret**
"CIS IBM Db2 for z/OS Benchmark (Top Secret)" on page 61[1]			1.0.0
"IBM z/OS RACF STIG" on page 15	9.05		
"IBM z/OS ACF2 STIG" on page 39		9.05	
"IBM z/OS TSS STIG" on page 63			9.05
"IBM zSecure for RACF STIG" on page 33	1.03		
"IBM zSecure for ACF2 STIG" on page 57		1.03	
"PCI-DSS for RACF" on page 34	4.0		
"PCI-DSS for ACF2" on page 58		4.0	
[1]: Using this standard requires a Z Security and Compliance Center license.			

"IBM z/OS RACF Products STIG" on page 26 "IBM z/OS ACF2 Products STIG" on page 50 "IBM z/OS TSS Products STIG" on page 74	**Version RACF**	**Version ACF2**	**Version Top Secret**
z/OS BMC CONTROL-D STIG	7.01	7.01	7.01
z/OS BMC CONTROL-M/Restart	7.01	7.01	7.01
z/OS BMC CONTROL-M STIG	7.01	7.01	7.01
z/OS BMC CONTROL-O STIG	7.01	7.01	7.01
z/OS BMC Integrated Operations Architecture (IOA) STIG	7.01	7.01	7.01
z/OS BMC MainView Systems Management STIG	7.01	7.01	7.01
z/OS CA Auditor STIG	7.01	7.01	7.01
z/OS CA Common Services STIG	7.01	7.01	7.01
z/OS CA Management Information Control System (MICS) Resource Management STIG	7.01	7.01	7.01
z/OS CA Multi-image Manager (MIM) Resource Sharing STIG	7.01	7.01	7.01
z/OS CA Roscoe Interactive Environment STIG	7.01	7.01	7.01
z/OS CA Vtape Virtual Tape System STIG	7.01	7.01	7.01
z/OS CA 1 Tape Management STIG	7.01	7.01	7.01
z/OS Catalog Solutions STIG	7.01	7.01	7.01
z/OS Compuware Abend-AID STIG	7.01	7.01	7.01
z/OS Fast Dump Restore (FDR) STIG	7.01	7.01	7.01
z/OS Front End Processor (FEP) STIG	7.01	7.01	7.01
z/OS IBM CL/SuperSession STIG	7.01	7.01	7.01
z/OS IBM Communications Server Simple Mail Transfer Protocol (CSSMTP) STIG	7.01	7.01	7.01

“IBM z/OS RACF Products STIG” on page 26 **“IBM z/OS ACF2 Products STIG” on page 50** **“IBM z/OS TSS Products STIG” on page 74**	**Version RACF**	**Version ACF2**	**Version Top Secret**
z/OS IBM Customer Information Control System (CICS®) Transaction Server STIG	7.01	7.01	7.01
z/OS IBM Hardware Configuration Definition (HCD) STIG	7.01	7.01	7.01
z/OS IBM Health Checker STIG	7.01	7.01	7.01
z/OS IBM MQ STIG	7.02	7.01	7.01
z/OS IBM System Display and Search Facility (SDSF) STIG	7.01	7.01	7.01
z/OS IBM Tivoli® Asset Discovery (TADz) STIG	7.01	7.01	7.01
z/OS IBM Transparent Data Migration Facility (TDMF) STIG	7.01	7.01	7.01
z/OS IBM WebSphere® Application Server (WAS) STIG	7.01	7.01	7.01
z/OS Quest NC-Pass STIG	7.01	7.01	7.01
IBM Z NetView	7.01	7.01	7.01
z/OS SRRAUDIT STIG	7.01	7.01	7.01
z/OS Vanguard Security Solutions (VSS) STIG	7.01		

Chapter 2. zSecure compliance standards for RACF

CIS IBM z/OS RACF Benchmark

Table 1. CIS IBM z/OS RACF Benchmark

CIS Control ID	CARLa member	Rule Title
CIS-OS-1.1.1	CKAHR111	Ensure that the PASSWORD(INTERVAL) SETROPTS value is set to no longer than 90 daays.
CIS-OS-1.1.2	CKAHR112	Ensure that the PASSWORD(HISTORY) SETROPTS value is set to at least 4.
CIS-OS-1.1.3	CKAHR113	Ensure that the PASSWORD(RULEn) SETROPTS value(s) is set.
CIS-OS-1.1.4	CKAHR114	Ensure that SETROPTS PASSWORD(MINCHANGE(n)) specifies a value greater than zero((0).
CIS-OS-1.1.5	CKAHR115	Ensure that the PASSWORD(REVOKE) SETROPTS value is specified.
CIS-OS-1.1.6	CKAHR116	Ensure that the KDFAES algorithm is used to protect passwords in the security daatabase.
CIS-OS-1.1.7	CKAHR117	Ensure that the PASSWORD(WARNING) SETROPTS value is set.
CIS-OS-1.2.1	CKAHR121	Ensure that Inactive users are revoked.
CIS-OS-1.2.2	CKAHR122	Ensure that STARTED class is used to assign users to started tasks.
CIS-OS-1.2.3	CKAHR123	Ensure user propagation is protected with the PROPCNTL class.
CIS-OS-1.2.4	CKAHR124	Ensure that Job wait time option is set.
CIS-OS-1.2.5	CKAHR125	Ensure that started tasks defined with the trusted attribute are justified.
CIS-OS-1.2.6	CKAHR126	Ensure that the OPERCMDS resource class is ACTIVE and RACLISTed.
CIS-OS-1.2.7	CKAHR127	Ensure that CONSOLE resource class is ACTIVE and RACLISTED.
CIS-OS-1.2.8	CKAHR128	Ensure that FACILITY resource class is ACTIVE and RACLISTED.
CIS-OS-1.2.9	CKAHR129	Ensure that inapplicable PPT entries have been invalidated.
CIS-OS-1.2.10	CKAHR12A	Ensure that LNKAUTH=APFTAB is specified in the IEASYSxx member(s) currently active parmlib data set(s).
CIS-OS-1.2.11	CKAHR12B	Ensure that the CONSOLxx members are configured.
CIS-OS-1.2.12	CKAHR12C	Ensure that no expired digital certificates are used.
CIS-OS-1.2.13	CKAHR12D	Ensure that RACF RVARYPW are set to non-default values.
CIS-OS-1.3.1	CKAHR131	Ensure that the use of RACF SPECIAL attribute is justified.
CIS-OS-1.3.2	CKAHR132	Ensure that SYS1.UADS contains only emergency user IDs.
CIS-OS-1.3.3	CKAHR133	Ensure that MCS console user IDs are protected.
CIS-OS-1.3.4	CKAHR134	Ensure that all STARTED class profiles specify PROTECTED user IDs.

Table 1. CIS IBM z/OS RACF Benchmark (continued)		
CIS Control ID	**CARLa member**	**Rule Title**
CIS-OS-2.1.1	CKAHR211	Ensure that maintenance user IDs are protected.
CIS-OS-2.1.2	CKAHR212	Ensure that access to active SMF collection files is controlled.
CIS-OS-2.1.3	CKAHR213	Ensure that the WHEN(PROGRAM) SETROPTS value is active.
CIS-OS-2.1.4	CKAHR214	Ensure that the ICHDSM00 program is protected.
CIS-OS-2.1.5	Not supported	Ensure that the IRRDPI00 program is protected
CIS-OS-2.1.6	CKAHR216	Ensure that the SETROPTS ERASE value is set to ERASE(ALL) on all systems.
CIS-OS-2.1.7	CKAHR217	Ensure that the TEMPDSN class is active.
CIS-OS-2.1.8	CKAHR218	Ensure the RACF security data sets and all copies are protected.
CIS-OS-2.1.9	CKAHR219	Ensure the RACF remote sharing facility files are protected.
CIS-OS-2.1.10	CKAHR21A	Ensure the RACF parameter library file is protected.
CIS-OS-2.1.11	CKAHR21B	Ensure that RACF remote sharing connections use the TCP/IP protocol.
CIS-OS-2.1.12	CKAHR21C	Ensure that memory and privileged program dumps are protected.
CIS-OS-2.1.13	CKAHR21D	Ensure that access to system trace datasets is controlled.
CIS-OS-2.1.14	CKAHR21E	Ensure that access to system backup data sets is controlled.
CIS-OS-2.1.15	CKAHR21F	Ensure that access to SYSTEM DUMP data sets is controlled.
CIS-OS-2.1.16	CKAHR21G	Ensure that access to SMF collection offload data sets is controlled.
CIS-OS-2.1.17	Not supported	Ensure that Temporary Data Sets are protected.
CIS-OS-2.2.1	CKAHR221	Ensure that the ability to update system dynamic lists are protected.
CIS-OS-2.2.2	CKAHR222	Ensure that IEASYMUP resource is protected.
CIS-OS-2.2.3	CKAHR223	Ensure that PASSWORD protection for data sets is not used.
CIS-OS-2.2.4	CKAHR224	Ensure that access to datasets in the PARMLIB concatenation is controlled.
CIS-OS-2.2.5	CKAHR225	Ensure that access to all LPA libraries is controllled.
CIS-OS-2.2.6	CKAHR226	Ensure that access to the system Master Catalog is controlled.
CIS-OS-2.2.7	CKAHR227	Ensure that access to all APF-authorized objects is controlled.
CIS-OS-2.2.8	CKAHR228	Ensure that access to SYS1.SVCLIB is controlled.
CIS-OS-2.2.9	CKAHR229	Ensure that access to SYS1.IMAGELIB is controlled.
CIS-OS-2.2.10	CKAHR22A	Ensure that access to libraries that contain PPT modules is controlled.
CIS-OS-2.2.11	CKAHR22B	Ensure that access to SYS1.NUCLEUS is controlled.
CIS-OS-2.2.12	CKAHR22C	Ensure that access to all system PROCLIB data sets is controlled.
CIS-OS-2.2.13	CKAHR22D	Ensure that system REXX data set is protected.
CIS-OS-2.2.14	CKAHR22E	Ensure that Access to SYS1.LINKLIB is protected.

Table 1. CIS IBM z/OS RACF Benchmark (continued)

CIS Control ID	CARLa member	Rule Title
CIS-OS-2.2.15	CKAHR22F	Ensure that access to all system-level product installation libraries is controlled.
CIS-OS-2.3.1	CKAHR231	Ensure that the TERMINAL SETROPTS value is set to NONE.
CIS-OS-2.3.2	CKAHR232	Ensure that the GENERIC SETROPTS value is enabled for required classes.
CIS-OS-2.3.3	CKAHR233	Ensure that the PROTECTALL SETROPTS value is set to FAIL.
CIS-OS-2.4.1	CKAHR241	Ensure that the assignment of the RACF OPERATIONS attribute is tightly controlleed.
CIS-OS-2.4.2	CKAHR242	Ensure that TSOAUTH resources are restricted to authorized users.
CIS-OS-2.4.3	CKAHR243	Ensure that access for surrogate users is controlled.
CIS-OS-2.4.4	CKAHR244	Ensure that UID 0 is only assigned to PROTECTED STC IDs.
CIS-OS-2.4.5	CKAHR245	Ensure that started tasks requiring exceptional access rights use the TRUSTED atttribute.
CIS-OS-2.4.6	CKAHR246	Ensure that access to Libraries containing EXIT modules is controlled (Level 1).
CIS-OS-2.4.7	CKAHR247	Ensure that access to LINKLIST libraries is controlled.
CIS-OS-2.4.8	CKAHR248	Ensure that access to SYS1.UADS is maintained.
CIS-OS-2.4.9	CKAHR249	Ensure that access to system page data sets (i.e., PLPA, COMMON, and LOCALx) is controlled.
CIS-OS-2.4.10	CKAHR24A	Ensure that MCS consoles access is protected through CONSOLE class profile.
CIS-OS-2.4.11	Not supported	Ensure that access to system user catalogs is controlled.
CIS-OS-2.4.12	CKAHR24C	Ensure that access to Libraries containing EXIT modules is controlled (Level 2).
CIS-OS-3.1	CKAHR31	Ensure that the command violations are being logged.
CIS-OS-3.2	CKAHR32	Ensure that activity of SPECIAL users are being logged.
CIS-OS-3.3	CKAHR33	Ensure that the AUDIT SETROPTS value is set for all classes.
CIS-OS-3.4	CKAHR34	Ensure that activities of users with the OPERATIONS attribute are logged.
CIS-OS-3.5	CKAHR35	Ensure that Logon statistics are recorded.
CIS-OS-3.6	CKAHR36	Ensure RACF AUDITOR or ROAUDIT privilege is assigned only to users with auditing mission.
CIS-OS-3.7	CKAHR37	Ensure that effective SMF records collection options are set.
CIS-OS-3.8	CKAHR38	Ensure that an automated process is in place to collect and retain SMF data.
CIS-OS-3.9	CKAHR39	Ensure that required SMF record types are collected.
CIS-OS-3.10	CKAHR3A	Ensure that RACF audit logs are reviewed on a regular basis.
CIS-OS-3.11	CKAHR3B	Ensure regular audit of AC=1 modules in APF authorized libraries are conducted.

Table 1. CIS IBM z/OS RACF Benchmark (continued)		
CIS Control ID	**CARLa member**	**Rule Title**
CIS-OS-3.12	CKAHR3C	Ensure that only supported (vendor) system software is installed and active on the system.
CIS-OS-3.13	CKAHR3D	Ensure all software on your system is supported.
CIS-OS-3.14	CKAHR3E	Implement sensitive z/OS data sets monitoring.
CIS-OS-4.1	CKAHR41	Ensure that the RACF database is backed up on a scheduled basis.
CIS-OS-4.2	CKAHR42	Ensure that RACF primary and backup databases are isolated.
CIS-OS-4.3	CKAHR43	Ensure sensitive data is encrypted.
CIS-OS-5.1	CKAHR51	Ensure that DFSMS is configured.
CIS-OS-5.2	CKAHR52	Ensure that a very limited number of users can use the Tape Bypass Label Processing (BLP).
CIS-OS-5.3	CKAHR53	Ensure that Automatic Data Set Protection (ADSP) SETROPTS value is set to NOADSP
CIS-OS-5.4	CKAHR54	Ensure that DFSMS control data sets are protected.
CIS-OS-6.1.1	CKAHR611	Ensure CSSMTP started task name is configured.
CIS-OS-6.1.2	CKAHR612	Ensure CSSMTP started task(s) is defined to the STARTED resource class.
CIS-OS-6.1.3	Not supported	Ensure AT-TLS protection is enabled for CSSMTP.
CIS-OS-6.1.4	CKAHR614	Ensure CSSMTP STC data sets are protected.
CIS-OS-6.2.1	CKAHR621	Ensure FTP server daemon is configured with proper security parameters.
CIS-OS-6.2.2	CKAHR622	Ensure startup parameters for the FTP daemon do not allow ANONYMOUS or INACTIVE keywords.
CIS-OS-6.2.3	CKAHR623	Ensure FTP.DATA configuration statements enforce secure configuration.
CIS-OS-6.2.4	CKAHR624	Ensure AT-TLS protection is enabled for the FTP daemon.
CIS-OS-6.2.5	CKAHR625	Ensure user exits for the FTP server are not used without approval.
CIS-OS-6.2.6	CKAHR626	Ensure warning banner for the FTP server is specified.
CIS-OS-6.2.7	CKAHR627	Ensure SMF recording options for the FTP server are configured.
CIS-OS-6.2.8	CKAHR628	Ensure permission and user audit bits for FTP server are configured.
CIS-OS-6.2.9	CKAHR629	Ensure MVS data sets for the FTP server are protected.
CIS-OS-6.2.10	CKAHR62A	Ensure FTP Control cards are stored in a secure PDS file.
CIS-OS-6.3.1	CKAHR631	Ensure SSH daemon is configured to only use the SSHv2 protocol.
CIS-OS-6.3.2	CKAHR632	Ensure SSH daemon is configured to use FIPS 140-2 compliant cryptographic provider where required.
CIS-OS-6.3.3	CKAHR633	Ensure SSH daemon is configured with the logon banner.
CIS-OS-6.3.4	CKAHR634	Ensure SMF recording options for the SSH daemon are configured.

Table 1. CIS IBM z/OS RACF Benchmark (continued)

CIS Control ID	CARLa member	Rule Title
CIS-OS-6.3.5	CKAHR635	Ensure SSH daemon is configured to use SAF keyrings for key storage.
CIS-OS-6.4.1	CKAHR641	Ensure Syslog daemon is started at z/OS initialization.
CIS-OS-6.4.2	CKAHR642	Ensure Syslog daemon is secured.
CIS-OS-6.4.3	CKAHR643	Ensure permission and user audit bits for syslog daemon component are configured
CIS-OS-6.4.4	Not supported	Ensure syslogd archive data sets are protected
CIS-OS-6.5.1	CKAHR651	Ensure configuration files for the TCP/IP stack are explicitly specified.
CIS-OS-6.5.2	CKAHR652	Ensure TCP/IP stack configuration is defined in TCPIP.DATA.
CIS-OS-6.5.3	CKAHR653	Ensure Hosts identified by the NSINTERADDR statement are protectted.
CIS-OS-6.5.4	CKAHR654	Ensure PROFILE.TCPIP configuration statements for the TCP/IP stack are defined.
CIS-OS-6.5.5	CKAHR655	Ensure permission and user audit bits for z/OS Unix file system objects that are part of the Base TCP/IP component are configured.
CIS-OS-6.5.6	CKAHR656	Ensure access to TCP/IP SAF resources.
CIS-OS-6.5.6-1	CKAHR656	TCP/IP stack resources used by IBM Communications Server Simple Mail Transfer Protocol (CSSMTP) must be protected in accordance with security requirements.
CIS-OS-6.5.7	CKAHR657	Ensure RACF SERVAUTH resource class is active for TCP/IP resources.
CIS-OS-6.5.8	CKAHR658	Ensure started tasks for the base TCP/IP component are defined securely in RACF.
CIS-OS-6.5.9	CKAHR659	Ensure MVS data sets for the Base TCP/IP component are protected.
CIS-OS-6.6.1	CKAHR661	Ensure configuration statements for the TN3270E Telnet server are configured.
CIS-OS-6.6.2	CKAHR662	Ensure VTAM® session setup controls for the TN3270E Telnet server are configured.
CIS-OS-6.6.3	CKAHR663	Ensure warning banner for the TN3270 Telnet server is configured.
CIS-OS-6.6.4	CKAHR664	Ensure AT-TLS protection is enabled for the TN3270 Telnet server.
CIS-OS-6.6.5	CKAHR665	Ensure SMF recording options for the TN3270 Telnet server are configured.
CIS-OS-6.6.6	Not supported	Ensure Startup user account for the z/OS UNIX Telnet server is defined.
CIS-OS-6.7.1	CKAHR671	Ensure VTAM USSTAB definitions are being used for secured terminals.
CIS-OS-6.7.2	CKAHR672	Ensure system data sets used to support the VTAM network are secured.

Table 1. CIS IBM z/OS RACF Benchmark (continued)		
CIS Control ID	**CARLa member**	**Rule Title**
CIS-OS-7.1.1	CKAHR711	Ensure that all ICSF installation data sets are protected.
CIS-OS-7.1.2	CKAHR712	Ensure that the ICSF Started Task is protected.
CIS-OS-7.1.3	Not supported	Ensure CSFINPV2 requires signature verification
CIS-OS-7.1.4	CKAHR714	Ensure ICSF is configured to start during IPL.
CIS-OS-7.2.1	CKAHR721	Ensure Crypto Usage Statistics are enabled.
CIS-OS-7.2.2	CKAHR722	Ensure Crypto key lifecycle auditing is enabled.
CIS-OS-7.2.3	CKAHR723	Ensure crypto key usage auditing is enabled.
CIS-OS-7.2.4	CKAHR724	Ensure ICSF Key Data Sets have a system backup.
CIS-OS-7.2.5	CKAHR725	Ensure ICSF Master Keys have a backup procedure.
CIS-OS-7.2.6	Not supported	Ensure all ICSF Key Data Sets are in Common Record Format.
CIS-OS-7.2.7	CKAHR727	Ensure all ICSF Key Data Sets are enabled for sysplex sharing.
CIS-OS-7.2.8	CKAHR728	Ensure ICSF is running with FIPSMODE enabled.
CIS-OS-7.2.9	CKAHR729	Ensure CCA operational keys are created with WRAPENH3 key wrapping.
CIS-OS-7.3.1	CKAHR731	Ensure that the CSFSERV class is active.
CIS-OS-7.3.2	CKAHR732	Ensure that the CSFKEYS class is active.
CIS-OS-7.3.3	CKAHR733	Ensure that the CRYPTOZ class is active.
CIS-OS-7.3.4	CKAHR734	Ensure that the XCSFKEY class is active.
CIS-OS-7.3.5	CKAHR735	Ensure ICSF Key Store Policy controls are enabled.
CIS-OS-7.3.6	CKAHR736	Ensure ICSF Key Datasets are protected.
CIS-OS-7.3.7	Not supported	Ensure ICSF administrative services are protected.
CIS-OS-7.3.8	CKAHR738	Ensure ICSF operator commands are protected.
CIS-OS-8.1.1	CKAHR811	Ensure that JES2 system commands are protected.
CIS-OS-8.2.1	CKAHR821	Ensure that JESSPOOL CLASS is active.
CIS-OS-8.2.2	CKAHR822	CKAHR822 Ensure that JES2 spool resources are protected.
CIS-OS-8.2.3	CKAHR823	CKAHR823 Ensure that JES2 trace resources are protected.
CIS-OS-8.2.4	CKAHR824	CKAHR824 Ensure that JESNEWS resources are protected.
CIS-OS-8.3.1	CKAHR831	CKAHR831 Ensure that JESJOBS class is set up.
CIS-OS-8.3.2	CKAHR832	CKAHR832 Ensure CANCEL JESJOBS profiles are protected.
CIS-OS-8.3.3	CKAHR833	CKAHR833 Awareness of the ENCRYPT JESJOBS profiles.
CIS-OS-8.3.4	CKAHR834	CKAHR834 Ensure GROUPREG JESJOBS profiles are protected.
CIS-OS-8.3.5	CKAHR835	CKAHR835 Ensure HOLD JESJOBS profiles are protected.
CIS-OS-8.3.6	CKAHR836	CKAHR836 Ensure JOBCLASS JESJOBS profiles are protected.
CIS-OS-8.3.7	CKAHR837	CKAHR837 Ensure JOBNFY JESJOBS profiles are protected.
CIS-OS-8.3.8	CKAHR838	CKAHR838 Ensure MODIFY JESJOBS profiles are protected.

Table 1. CIS IBM z/OS RACF Benchmark (continued)

CIS Control ID	CARLa member	Rule Title
CIS-OS-8.3.9	CKAHR839	CKAHR839 Ensure PURGE JESJOBS profiles are protected.
CIS-OS-8.3.10	CKAHR83A	CKAHR83A Ensure RELEASE JESJOBS profiles are protected.
CIS-OS-8.3.11	CKAHR83B	CKAHR83B Ensure REROUTE JESJOBS profiles are protected.
CIS-OS-8.3.12	CKAHR83C	CKAHR83C Ensure SPIN JESJOBS profiles are protected.
CIS-OS-8.3.13	CKAHR83D	CKAHR83D Ensure SPOOLIO JESJOBS profiles are protected.
CIS-OS-8.3.14	CKAHR83E	CKAHR83E Ensure START JESJOBS profiles are protected.
CIS-OS-8.3.15	CKAHR83F	CKAHR83F Ensure SUBMIT JESJOBS profiles are protected.
CIS-OS-8.4.1	CKAHR841	Ensure that data sets on SPOOL are encrypted as required.
CIS-OS-8.5.1	CKAHR851	Ensure that the JES(BATCHALLRACF) SETROPTS value is set to JES(BATCHALLRACF).
CIS-OS-8.5.2	CKAHR852	Ensure that the JES(XBMALLRACF) SETROPTS value is set to JES(XBMALLRACF).
CIS-OS-8.6.1	CKAHR861	Ensure that access to the data sets used by JES2 is controlled.
CIS-OS-8.6.2	CKAHR22C	Ensure that access to any PROCLIB data sets used by JES2 is protected from unintended updates.
CIS-OS-8.6.3	CKAHR863	Ensure that RACF is called for data sets opened by JES2.
CIS-OS-8.7.1	CKAHR871	Ensure that JES2 output devices are controlled.
CIS-OS-8.7.2	CKAHR872	Ensure that bypass label processing (BLP=) is not set on any JOBCLASS.
CIS-OS-8.7.3	CKAHR873	Ensure that use of JES2 input sources are controlled.
CIS-OS-8.8.1	CKAHR881	Ensure that RJE workstations and NJE nodes are controlled.
CIS-OS-8.8.2	CKAHR882	Ensure that RJE workstations and NJE nodes are controlled.
CIS-OS-9.1	CKAHR91	Ensure that z/OS UNIX SURROGAT resources are protected.
CIS-OS-9.2	CKAHR92	Ensure that resources protecting superuser capabilities in the UNIXPRIV class are protected.
CIS-OS-9.3	CKAHR93	Ensure that general users are not allowed to change their file ownership.
CIS-OS-9.4	CKAHR94	Ensure that RESTRICTED users cannot access UNIX files to which they are not explicitly permitted
CIS-OS-9.5	CKAHR95	Ensure that newly assigned UIDs and GIDs are unique values.
CIS-OS-9.6	CKAHR96	Ensure that z/OS UNIX user accounts are defined.
CIS-OS-9.7	CKAHR97	Ensure that RACF classes required to secure the z/OS UNIX environment are active.
CIS-OS-9.8	CKAHR98	Ensure that RACF Classes required to secure the z/OS UNIX environment are RACLISTed.
CIS-OS-9.9	Not supported	Ensure that the user account for the z/OS UNIX kernel (OMVS) is defined to the security database.
CIS-OS-9.10	CKAHR9A	Ensure that z/OS UNIX automount configuration files are protected.

Table 1. CIS IBM z/OS RACF Benchmark (continued)		
CIS Control ID	**CARLa member**	**Rule Title**
CIS-OS-9.11	CKAHR9B	Ensure that z/OS UNIX security parameters in /etc/inetd.conf are configured.
CIS-OS-9.12	CKAHR9C	Ensure that z/OS UNIX OMVS parameters in IEASYSxx are configured.
CIS-OS-9.13	CKAHR9D	Ensure that z/OS UNIX BPXPRMxx parameters in PARMLIB are set for security.
CIS-OS-9.14	CKAHR9E	Ensure that z/OS UNIX permission bits and audit bits are configured to audit sensitive file access.
CIS-OS-9.15	CKAHR9F	Ensure that BPX resources are protected.
CIS-OS-9.16	CKAHR9G	Ensure that security parameters in etc/profile are configured.
CIS-OS-9.17	CKAHR9H	Ensure that security commands in /etc/rc are safe.
CIS-OS-9.18	CKAHR9I	Ensure that the BPXROOT user account is configured.
CIS-OS-9.19	CKAHR9J	Ensure that each RACF group for UNIX is defined with a unique GID.
CIS-OS-9.20	CKAHR9K	Ensure that data sets used as step libraries in /etc/steplib are configured.
CIS-OS-9.21	CKAHR9L	Ensure that ability to switch into superuser mode is restricted.
CIS-OS-9.22	CKAHR9M	Ensure file permission for universal write is restricted.
CIS-OS-9.23	CKAHR9N	Ensure USS Telnet server is not active.
CIS-OS-9.24	CKAHR9O	Ensure rlogin is not active.
CIS-OS-9.25	CKAHR9P	Ensure changes to UNIX file security are logged.
CIS-OS-9.26	CKAHR9Q	Ensure that programs cannot execute from the /tmp directory.
CIS-OS-9.27	CKAHR9R	Ensure that data sets containing user file systems do not have the user ID as the high-level qualifier.
CIS-OS-9.28	CKAHR9S	Ensure that daemons are running with z/OS UNIX level security.
CIS-OS-9.29	CKAHR9T	Ensure that servers are running with z/OS UNIX level security.
CIS-OS-9.30	Not supported	Ensure that file systems containing critical data are protected from access using profiles in the FSACCESS class.
CIS-OS-9.31	CKAHR9U	Ensure that file systems are mounted read-only wherever possible.
CIS-OS-9.32	CKAHR9V	Ensure that file systems are mounted with set-id files disabled wherever possible.
CIS-OS-9.33	CKAHR9X	Ensure that no file systems are mounted with security disabled.

CIS IBM Db2 for z/OS Benchmark (RACF)

This standard is available only if your organization has a license for Z Security and Compliance Center.

zSecure has added the CIS-DB2 prefix to the control number to help distinguish between CIS IBM z/OS RACF Benchmark control numbers and CIS IBM Db2 for z/OS Benchmark control numbers.

Table 2. CIS IBM Db2 for z/OS Benchmark (RACF)		
CIS Db2 Control ID	**CARLa member**	**Rule Title**
CIS-DB2-1.1.1	CKAHD111	Ensure that Db2 system data sets are protected
CIS-DB2-1.1.2	C2RHD112	Ensure that Db2 USS file system is protected
CIS-DB2-1.1.3	C2RHD113	Secure installation process
CIS-DB2-1.2.1	C2RHD121	Ensure that RACF changes are accepted immediately
CIS-DB2-1.2.2	C2RHD122	Ensure that authorization is enabled
CIS-DB2-1.2.3	CKAHD123	Ensure that the default authorization IDs are changed from the installation defined
CIS-DB2-1.2.4	C2RHD124	Ensure that generic error codes are returned for remote security errors
CIS-DB2-1.2.5	C2RHD125	Separate security administration from system administration
CIS-DB2-2.1.1	Not supported	Ensure subsystem access is protected
CIS-DB2-2.1.2	C2RHD212	Ensure secure authentication is enabled for remote access
CIS-DB2-2.1.3	C2RHD213	Secure access by using IBM Z Multi-Factor Authentication (MFA)
CIS-DB2-2.1.4	C2RHD214	Secure all remote connections by using SSL
CIS-DB2-2.1.5	Not supported	Secure remote connections by using TCP/IP Network Access control with the RACF SERVAUTH class
CIS-DB2-2.1.6	CKCHD216	Secure connections by using trusted contexts
CIS-DB2-2.1.7	CKCHD217	Secure object ownership by using Db2 roles
CIS-DB2-2.1.8	Not supported	Secure application access by using package controls
CIS-DB2-2.1.9	CKCHD219	Ensure that grant authorization IDs are defined in RACF
CIS-DB2-2.2.1	CKCHD221	Ensure that access to the catalog tables in the communications database (CDB) is restricted
CIS-DB2-2.2.2	CKCHD222	Ensure that access to SYSIBM.SYSAUDITPOLICIES is restricted
CIS-DB2-2.2.3	CKCHD223	Ensure that access to SYSIBM.SYSAUDITPOLICIES is restricted
CIS-DB2-2.2.4	CKCHD224	Ensure that access to SYSIBM.SYSCOLUMNS is restricted
CIS-DB2-2.2.5	CKCHD225	Ensure that access to trusted context tables is restricted
CIS-DB2-2.2.6	CKCHD226	Ensure that access to SYSIBM.SYSCONTROLS is restricted
CIS-DB2-2.2.7	CKCHD227	Ensure that access to SYSIBM.SYSDATABASE is restricted
CIS-DB2-2.2.8	CKCHD228	Ensure that access to SYSIBM.SYSDBAUTH is restricted
CIS-DB2-2.2.9	CKCHD229	Ensure that access to dynamic query-related tables is restricted
CIS-DB2-2.2.10	CKCHD22A	Ensure that access to SYSIBM.SYSINDEXES is restricted (Manual)
CIS-DB2-2.2.11	CKCHD22B	Ensure that access to SYSIBM.SYSOBJROLEDEP is restricted
CIS-DB2-2.2.12	CKCHD22C	Ensure that access to package-related tables is restricted
CIS-DB2-2.2.13	CKCHD22D	Ensure that access to SYSIBM.SYSPACKAUTH is restricted
CIS-DB2-2.2.14	CKCHD22E	Ensure that access to SYSIBM.SYSPARMS is restricted
CIS-DB2-2.2.15	CKCHD22F	Ensure that access to SYSIBM.SYSPLAN is restricted

Table 2. CIS IBM Db2 for z/OS Benchmark (RACF) (continued)		
CIS Db2 Control ID	**CARLa member**	**Rule Title**
CIS-DB2-2.2.16	CKCHD22G	Ensure that access to SYSIBM.SYSPLANAUTH is restricted
CIS-DB2-2.2.17	CKCHD22H	Ensure that access to SYSIBM.SYSQUERY is restricted
CIS-DB2-2.2.18	CKCHD22I	Ensure that access to SYSIBM.SYSRESAUTH is restricted
CIS-DB2-2.2.19	CKCHD22J	Ensure that access to SYSIBM.SYSROLES is restricted
CIS-DB2-2.2.20	CKCHD22K	Ensure that access to SYSIBM.SYSROUTINEAUTH is restricted
CIS-DB2-2.2.21	CKCHD22L	Ensure that access to SYSIBM.SYSROUTINES is restricted
CIS-DB2-2.2.22	CKCHD22M	Ensure that access to SYSIBM.SYSROUTINESTEXT is restricted
CIS-DB2-2.2.23	CKCHD22N	Ensure that access to SYSIBM.SYSSCHEMAAUTH is restricted
CIS-DB2-2.2.24	CKCHD22O	Ensure that access to SYSIBM.SYSSEQUENCEAUTH is restricted
CIS-DB2-2.2.25	CKCHD22P	Ensure that access to SYSIBM.SYSSEQUENCES is restricted
CIS-DB2-2.2.26	CKCHD22Q	Ensure that access to SYSIBM.SYSSTMT is restricted
CIS-DB2-2.2.27	CKCHD22R	Ensure that access to SYSIBM.SYSSTOGROUP is restricted
CIS-DB2-2.2.28	CKCHD22S	Ensure that access to SYSIBM.SYSTABAUTH is restricted
CIS-DB2-2.2.29	CKCHD22T	Ensure that access to SYSIBM.SYSTABLES is restricted
CIS-DB2-2.2.30	CKCHD22U	Ensure that access to SYSIBM.SYSTABLESPACE is restricted
CIS-DB2-2.2.31	CKCHD22V	Ensure that access to SYSIBM.SYSTRIGGERS is restricted
CIS-DB2-2.2.32	CKCHD22W	Ensure that access to SYSIBM.SYSUSERAUTH is restricted
CIS-DB2-2.2.33	CKCHD22X	Ensure that access to variable-related tables is restricted
CIS-DB2-2.2.34	CKCHD22Y	Ensure that access to SYSIBM.SYSVARIABLEAUTH is restricted
CIS-DB2-2.2.35	CKCHD22Z	Ensure that access to SYSIBM.SYSVIEWS is restricted
CIS-DB2-2.3.1	CKCHD231	Ensure that access to the program authorization table is restricted
CIS-DB2-2.3.2	CKCHD232	Ensure that access to the REST services definition table is restricted
CIS-DB2-2.3.3	CKCHD233	Ensure that access to the query accelerator tables is restricted
CIS-DB2-2.3.4	CKCHD234	Ensure that access to profile tables is restricted
CIS-DB2-2.3.5	CKCHD235	Ensure that access to SQL Data Insights tables is restricted
CIS-DB2-2.4.1	CKCHD241	Secure SYSADM authority access
CIS-DB2-2.4.2	CKCHD242	Secure SYSCTRL authority access
CIS-DB2-2.4.3	CKCHD243	Secure SYSOPR authority access
CIS-DB2-2.4.4	CKCHD244	Secure system DBADM authority access
CIS-DB2-2.4.5	CKCHD245	Secure DATAACCESS authority access
CIS-DB2-2.4.6	CKCHD246	Secure ACCESSCTRL authority access
CIS-DB2-2.4.7	CKCHD247	Secure PACKADM authority access
CIS-DB2-2.4.8	CKCHD248	Secure SQLADM authority access
CIS-DB2-2.4.9	CKCHD249	Secure database DBADM authority access

Table 2. CIS IBM Db2 for z/OS Benchmark (RACF) (continued)		
CIS Db2 Control ID	**CARLa member**	**Rule Title**
CIS-DB2-2.4.10	CKCHD24A	Secure database DBCTRL authority access
CIS-DB2-2.4.11	CKCHD24B	Secure database DBMAINT authority access
CIS-DB2-2.5.1	C2RHD251	Ensure that data is encrypted at rest and in-flight
CIS-DB2-2.5.2	Not supported	Secure sensitive data in memory
CIS-DB2-2.6.1	C2RHD261	Secure row access using row permit
CIS-DB2-2.6.2	C2RHD262	Secure column values using column mask
CIS-DB2-3.1.1	CKCHD311	Ensure that audit tracing is enabled during Db2 start up
CIS-DB2-3.1.2	CKCHD312	Ensure that critical audit traces are always enabled
CIS-DB2-3.1.3	C2RHD313	Ensure that authorization failures are audited
CIS-DB2-3.1.4	CKCHD314	Enable audit policies to audit installation system administrator and system operator access
CIS-DB2-3.1.5	CKCHD315	Enable auditing of system administrator access
CIS-DB2-3.1.6	CKCHD316	Enable auditing of database administrator access

IBM z/OS RACF STIG

Table 3. IBM z/OS RACF STIG		
STIG ID	**CARLa member**	**Rule Title**
RACF-CE-000010	CKAHCE10	Certificate Name Filtering must be implemented with appropriate authorization and documentation.
RACF-CE-000020	CKAHCE20	Expired digital certificates must not be used.
RACF-CE-000030	CKAHCE30	All digital certificates in use must have a valid path to a trusted Certification authority.
RACF-ES-000010	CKAHE010	IBM RACF must limit Write or greater access to SYS1.NUCLEUS to system programmers only.
RACF-ES-000020	CKAHE020	IBM RACF must limit Write or greater access to libraries that contain PPT modules to system programmers only.
RACF-ES-000030	CKAHE030	IBM RACF must limit WRITE or greater access to LINKLIST libraries to system programmers only
RACF-ES-000040	CKAHE040	IBM RACF emergency user IDs must be properly defined.
RACF-ES-000050	CKAHE050	IBM RACF SETROPTS LOGOPTIONS must be properly configured.
RACF-ES-000060	CKAHE060	IBM RACF must protect memory and privileged program dumps in accordance with proper security requirements.
RACF-ES-000070	CKAHE070	IBM z/OS system commands must be properly protected.
RACF-ES-000080	CKAHE080	IBM RACF must properly define users that have access to the CONSOLE resource in the TSOAUTH resource class.
RACF-ES-000090	CKAHE090	The IBM RACF FACILITY resource class must be active.
RACF-ES-000100	CKAHE100	The IBM RACF OPERCMDS resource class must be active.

Table 3. IBM z/OS RACF STIG (continued)

STIG ID	CARLa member	Rule Title
RACF-ES-000110	CKAHE110	The IBM RACF MCS consoles resource class must be active.
RACF-ES-000120	CKAHE120	IBM RACF CLASSACT SETROPTS must be specified for the TEMPDSN class.
RACF-ES-000130	CKAHE130	IBM RACF started tasks defined with the trusted attribute must be justified.
RACF-ES-000140	CKAHE140	IBM RACF user IDs possessing the Tape Bypass Label Processing (BLP) privilege must be justified.
RACF-ES-000150	CKAHE150	IBM RACF DASD volume-level protection must be properly defined.
RACF-ES-000160	CKAHE160	IBM Sensitive Utility Controls must be properly defined and protected.
RACF-ES-000170	CKAHE170	IBM RACF Global Access Checking must be restricted to appropriate classes and resources.
RACF-ES-000180	CKAHE180	IBM RACF access to the System Master Catalog must be properly protected.
RACF-ES-000190	CKAHE190	IBM RACF must limit Write or greater access to SYS1.UADS to system programmers only, and WRITE or greater access must be limited to system programmer personnel and/or security personnel.
RACF-ES-000200	CKAHE200	IBM z/OS must protect dynamic lists in accordance with proper security requirements.
RACF-ES-000210	CKAHE210	IBM RACF allocate access to system user catalogs must be properly protected.
RACF-ES-000220	CKAHE220	IBM RACF must limit WRITE or greater access to System backup files to system programmers and/or batch jobs that perform DASD backups.
RACF-ES-000230	CKAHE230	IBM RACF must limit access to SYS(x).TRACE to system programmers only.
RACF-ES-000240	CKAHE240	IBM RACF batch jobs must be properly secured.
RACF-ES-000250	CKAHE250	IBM RACF batch jobs must be protected with propagation control.
RACF-ES-000260	CKAHE260	IBM RACF must limit Write or greater access to SYS1.IMAGELIB to system programmers only.
RACF-ES-000270	CKAHE270	IBM RACF must limit Write or greater access to SYS1.SVCLIB to appropriate authorized users.
RACF-ES-000280	CKAHE280	IBM RACF must limit Write or greater access to SYS1.LPALIB to system programmers only.
RACF-ES-000290	CKAHE290	IBM z/OS libraries included in the system REXXLIB concatenation must be properly protected.
RACF-ES-000300	CKAHE300	IBM RACF must limit write or greater access to all LPA libraries to system programmers only.
RACF-ES-000310	CKAHE310	IBM RACF must limit Write or greater access to libraries containing EXIT modules to system programmers only.

Table 3. IBM z/OS RACF STIG (continued)

STIG ID	CARLa member	Rule Title
RACF-ES-000320	CKAHE320	IBM RACF must limit WRITE or greater access to all system-level product installation libraries to system programmers.
RACF-ES-000330	CKAHE330	IBM RACF must limit access to SYSTEM DUMP data sets to system programmers only.
RACF-ES-000340	CKAHE340	IBM RACF must limit WRITE or greater access to all APF-authorized libraries to system programmers only.
RACF-ES-000350	CKAHE350	IBM RACF access to SYS1.LINKLIB must be properly protected.
RACF-ES-000360	CKAHE360	The IBM RACF System REXX IRRPWREX security data set must be properly protected.
RACF-ES-000365	Not supported	The IBM RACF System REXX IRRPHREX security data set must be properly protected.
RACF-ES-000370	CKAHE370	IBM RACF security data sets and/or databases must be properly protected.
RACF-ES-000380	CKAHE380	IBM RACF must limit access to data sets used to back up and/or dump SMF collection files to appropriate users and/or batch jobs that perform SMF dump processing.
RACF-ES-000390	CKAHE390	IBM RACF must limit all system PROCLIB data sets to system programmers only.
RACF-ES-000400	CKAHE400	IBM RACF must limit access to System page data sets (that is, PLPA, COMMON, and LOCALx) to system programmers.
RACF-ES-000410	CKAHE410	IBM z/OS MCS consoles access authorization(s) for CONSOLE resource(s) must be properly protected.
RACF-ES-000420	CKAHE420	IBM RACF must limit WRITE or greater access to the JES2 System data sets (for example, Spool, Checkpoint, and Initialization parameters) to system programmers only.
RACF-ES-000430	CKAHE430	The IBM z/OS IEASYMUP resource must be protected in accordance with proper security requirements.
RACF-ES-000440	CKAHE440	The IBM RACF JES(BATCHALLRACF) SETROPTS value must be set to JES(BATCHALLRACF).
RACF-ES-000460	CKAHE460	The IBM z/OS JES(XBMALLRACF) SETROPTS value must be set to JES(XBMALLRACF).
RACF-ES-000470	CKAHE470	IBM RACF OPERAUDIT SETROPTS value must set to OPERAUDIT.
RACF-ES-000480	CKAHE480	The IBM RACF PASSWORD(REVOKE) SETROPTS value must be specified to revoke the user ID after three invalid logon attempts.
RACF-ES-000500	CKAHE500	IBM z/OS SYS1.PARMLIB must be properly protected.
RACF-ES-000520	CKAHE520	The IBM RACF SETROPTS SAUDIT value must be specified.
RACF-ES-000530	CKAHE530	The IBM RACF REALDSN SETROPTS value must be specified.
RACF-ES-000540	CKAHE540	IBM z/OS must limit access for SMF collection files (that is, SYS1.MANx) to appropriate users and/or batch jobs that perform SMF dump processing.
RACF-ES-000550	CKAHE550	IBM RACF SETROPTS RVARYPW values must be properly set.

Table 3. IBM z/OS RACF STIG (continued)		
STIG ID	**CARLa member**	**Rule Title**
RACF-ES-000560	CKAHE560	IBM RACF must define WARN = NO on all profiles.
RACF-ES-000570	CKAHE570	The IBM RACF PROTECTALL SETROPTS value specified must be properly set.
RACF-ES-000580	CKAHE580	The IBM RACF GRPLIST SETROPTS value must be set to ACTIVE.
RACF-ES-000590	CKAHE590	The IBM RACF RETPD SETROPTS value specified must be properly set.
RACF-ES-000600	CKAHE600	The IBM RACF TAPEDSN SETROPTS value specified must be properly set.
RACF-ES-000610	CKAHE610	The IBM RACF WHEN(PROGRAM) SETROPTS value specified must be active.
RACF-ES-000620	CKAHE620	IBM RACF use of the AUDITOR privilege must be justified.
RACF-ES-000630	CKAHE630	The IBM RACF database must be on a separate physical volume from its backup and recovery data sets.
RACF-ES-000640	CKAHE640	The IBM RACF database must be backed up on a scheduled basis.
RACF-ES-000650	CKAHE650	IBM z/OS Batch job user IDs must be properly defined.
RACF-ES-000660	CKAHE660	IBM RACF use of the RACF SPECIAL Attribute must be justified.
RACF-ES-000670	CKAHE670	IBM RACF assignment of the RACF OPERATIONS attribute to individual user IDs must be fully justified.
RACF-ES-000680	C2RHE680	IBM z/OS must properly configure CONSOLxx members.
RACF-ES-000690	CKAHE690	IBM z/OS must properly protect MCS console user ID(s).
RACF-ES-000700	CKAHE700	IBM RACF users must have the required default fields.
RACF-ES-000710	CKAHE710	IBM interactive user IDs defined to RACF must have the required fields completed.
RACF-ES-000720	CKAHE720	IBM z/OS Started Tasks must be properly identified and defined to RACF.
RACF-ES-000740	CKAHE740	The IBM RACF Automatic Data Set Protection (ADSP) SETROPTS value must be set to NOADSP.
RACF-ES-000750	CKAHE750	IBM RACF user accounts must uniquely identify system users.
RACF-ES-000760	CKAHE760	The IBM RACF INACTIVE SETROPTS value must be set to 35 days.
RACF-ES-000770	CKAHE770	IBM RACF PASSWORD(RULEn) SETROPTS value(s) must be properly set.
RACF-ES-000780	CKAHE780	IBM RACF exit ICHPWX01 must be installed and properly configured.
RACF-ES-000785	CKAHE785	IBM RACF exit ICHPWX11 must be installed and properly configured.
RACF-ES-000790	CKAHE790	The IBM RACF SETROPTS PASSWORD(MINCHANGE) value must be set to 1.
RACF-ES-000800	CKAHE800	IBM RACF SETROPTS PASSWORD(INTERVAL) must be set to 60 days.

Table 3. IBM z/OS RACF STIG (continued)

STIG ID	CARLa member	Rule Title
RACF-ES-000810	CKAHE810	The IBM RACF PASSWORD(HISTORY) SETROPTS value must be set to 5 or more.
RACF-ES-000820	CKAHE820	NIST FIPS-validated cryptography must be used to protect passwords in the security database.
RACF-ES-000840	CKAHE840	The IBM RACF ERASE ALL SETROPTS value must be set to ERASE(ALL) on all systems.
RACF-ES-000850	CKAHE850	IBM RACF DASD Management user IDs must be properly controlled.
RACF-ES-000860	CKAHE860	IBM Passtickets must be configured to be KeyEncrypted
RACF-FT-000010	C2RHF010	IBM z/OS SMF recording options for the FTP Server must be configured to write SMF records for all eligible events
RACF-FT-000020	C2RHF020	IBM RACF permission bits and user audit bits for HFS objects that are part of the FTP server component must be properly configured.
RACF-FT-000030	CKAHF030	IBM z/OS data sets for the FTP server must be properly protected.
RACF-FT-000040	C2RHF040	IBM z/OS FTP.DATA configuration statements must indicate a BANNER statement with the proper content.
RACF-FT-000050	C2RHF050	IBM z/OS FTP.DATA configuration statements for the FTP server must specify the BANNER statement.
RACF-FT-000065	CKAHF065	IBM z/OS FTP control cards must be properly stored in a secure PDS file.
RACF-FT-000070	C2RHF070	IBM z/OS FTP.DATA configuration statements for the FTP Server must be specified in accordance with requirements.
RACF-FT-000080	CKAHF080	The IBM z/OS TFTP server program must be properly protected.
RACF-FT-000090	C2RHF090	IBM z/OS user exits for the FTP server must not be used without proper approval and documentation.
RACF-FT-000100	CKAHF100	The IBM z/OS FTP server daemon must be defined with proper security parameters.
RACF-FT-000110	C2RHF110	IBM FTP.DATA configuration for the FTP server must have the INACTIVE statement properly set.
RACF-FT-000120	C2RHF120	IBM z/OS startup parameters for the FTP server must have the INACTIVE statement properly set.
RACF-IC-000010	C2RHIC10	IBM Integrated Crypto Service Facility (ICSF) Configuration parameters must be correctly specified.
RACF-IC-000020	CKAHIC20	IBM Integrated Crypto Service Facility (ICSF) install data sets are not properly protected.
RACF-IC-000030	CKAHIC30	IBM Integrated Crypto Service Facility (ICSF) STC data sets must be properly protected.
RACF-IC-000040	CKAHIC40	IBM Integrated Crypto Service Facility (ICSF) Started Task name is not properly identified / defined to the system ACP.
RACF-IC-000050	CKAHIC50	IBM Integrated Crypto Service Facility (ICSF) Started task(s) must be properly defined to the STARTED resource class for RACF.

Table 3. IBM z/OS RACF STIG (continued)

STIG ID	CARLa member	Rule Title
RACF-IC-000060	CKAHIC60	The ICSF resource class(es) must be active in accordance with security requirements.
RACF-IC-000070	Not supported	ICSF resources must be protected in accordance with security requirements.
RACF-JS-000010	CKAHJ010	IBM z/OS RJE workstations and NJE nodes must be defined to the FACILITY resource class.
RACF-JS-000020	CKAHJ020	IBM z/OS JES2 input sources must be controlled in accordance with the proper security requirements.
RACF-JS-000030	CKAHJ030	IBM z/OS JES2 input sources must be properly controlled.
RACF-JS-000040	CKAHJ040	IBM z/OS JES2 output devices must be controlled in accordance with the proper security requirements.
RACF-JS-000050	CKAHJ050	IBM z/OS JES2 output devices must be properly controlled for classified systems.
RACF-JS-000060	CKAHJ060	IBM z/OS JESSPOOL resources must be protected in accordance with security requirements.
RACF-JS-000070	CKAHJ070	IBM z/OS JESNEWS resources must be protected in accordance with security requirements.
RACF-JS-000080	CKAHJ080	IBM z/OS JESTRACE and/or SYSLOG resources must be protected in accordance with security requirements.
RACF-JS-000090	CKAHJ090	IBM z/OS JES2 spool resources must be controlled in accordance with security requirements.
RACF-JS-000100	CKAHJ100	IBM z/OS JES2 system commands must be protected in accordance with security requirements.
RACF-JS-000110	CKAHJ110	IBM z/OS surrogate users must be controlled in accordance with proper security requirements.
RACF-JS-000120	CKAHJ120	IBM z/OS RJE workstations and NJE nodes must be controlled in accordance with security requirements.
RACF-OS-000010	C2RHO010	IBM z/OS must configure system wait times to protect resource availability based on site priorities.
RACF-OS-000020	Not supported	The IBM z/OS BPX.SMF resource must be properly configured.
RACF-OS-000030	C2RHO030	IBM z/OS SMF recording options for the TN3270 Telnet Server must be properly specified.
RACF-OS-000040	CKAHO040	IBM RACF must be installed and active on the system.
RACF-OS-000050	C2RHO050	The IBM z/OS System Administrator (SA) must develop a process to disable emergency accounts after the crisis is resolved or 72 hours.
RACF-OS-000060	C2RHO060	The IBM z/OS System Administrator (SA) must develop a process to notify appropriate personnel when accounts are created.
RACF-OS-000070	C2RHO070	The IBM z/OS System Administrator (SA) must develop a process to notify appropriate personnel when accounts are modified.
RACF-OS-000080	C2RHO080	The IBM z/OS System Administrator (SA) must develop a process to notify appropriate personnel when accounts are deleted.

Table 3. IBM z/OS RACF STIG (continued)

STIG ID	CARLa member	Rule Title
RACF-OS-000090	C2RHO090	The IBM z/OS System Administrator (SA) must develop a process to notify appropriate personnel when accounts are removed.
RACF-OS-000100	C2RHO100	The IBM z/OS System Administrator (SA) must develop a process to notify Information System Security Officers (ISSOs) of account enabling actions.
RACF-OS-000110	C2RHO110	IBM z/OS required SMF data record types must be collected.
RACF-OS-000120	CKAHO120	IBM z/OS must employ a session manager to manage display of the Standard Mandatory Department of Defense (DoD) Notice and Consent Banner.
RACF-OS-000130	C2RHO130	IBM z/OS must specify SMF data options to assure appropriate activation.
RACF-OS-000140	C2RHO140	IBM z/OS SMF collection files (system MANx data sets or LOGSTREAM DASD) must have storage capacity to store at least one week of audit data.
RACF-OS-000150	C2RHO150	IBM z/OS system administrators must develop an automated process to collect and retain SMF data.
RACF-OS-000160	C2RHO160	IBM z/OS BUFUSEWARN in the SMFPRMxx must be properly set.
RACF-OS-000170	C2RHO170	IBM z/OS NOBUFFS in SMFPRMxx must be properly set (default is MSG).
RACF-OS-000180	C2RHO180	The IBM z/OS SNTP daemon (SNTPD) must be active.
RACF-OS-000190	C2RHO190	IBM z/OS SNTP daemon (SNTPD) permission bits must be properly configured.
RACF-OS-000200	C2RHO200	IBM z/OS PARMLIB CLOCKxx must have the Accuracy PARM properly coded.
RACF-OS-000210	CKAHO210	IBM RACF must define UACC of NONE on all profiles.
RACF-OS-000220	C2RHO220	IBM z/OS PASSWORD data set and OS passwords must not be used.
RACF-OS-000240	C2RHO240	The IBM z/OS Policy Agent must employ a deny-all, allow-by-exception firewall policy for allowing connections to other systems.
RACF-OS-000250	C2RHO250	Unsupported system software must not be installed and/ or active on the system.
RACF-OS-000260	C2RHO260	IBM z/OS must not allow nonexistent or inaccessible LINKLIST libraries.
RACF-OS-000270	C2RHO270	IBM z/OS must not allow nonexistent or inaccessible Link Pack Area (LPA) libraries.
RACF-OS-000280	C2RHO280	IBM z/OS must not have inaccessible APF libraries defined.
RACF-OS-000290	C2RHO290	IBM z/OS inapplicable PPT entries must be invalidated.
RACF-OS-000300	C2RHO300	IBM z/OS LNKAUTH=APFTAB must be specified in the IEASYSxx member(s) in the currently active parmlib data set(s).
RACF-OS-000310	C2RHO310	IBM z/OS must not have duplicated sensitive utilities and/or programs existing in APF libraries.

Table 3. IBM z/OS RACF STIG (continued)

STIG ID	CARLa member	Rule Title
RACF-OS-000320	C2RHO320	The IBM z/OS systems requiring data-at-rest protection must properly employ IBM DS8880 or equivalent hardware solutions for full disk encryption.
RACF-OS-000350	C2RHO350	IBM z/OS sensitive and critical system data sets must not exist on shared DASDs.
RACF-OS-000360	C2RHO360	The IBM z/OS Policy Agent must contain a policy that protects against or limits the effects of Denial of Service (DoS) attacks by ensuring the operating system is implementing rate-limiting measures on impacted network interfaces.
RACF-OS-000370	C2RHO370	The IBM z/OS Policy Agent must contain a policy that manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of Denial of Service (DoS) attacks.
RACF-OS-000400	C2RHO400	The IBM z/OS must employ a session manager that conceals, via the session lock, information previously visible on the display with a publicly viewable image.
RACF-OS-000410	C2RHO410	IBM z/OS must employ a session manager to manage session lock after a 15-minute period of inactivity.
RACF-OS-000420	C2RHO420	IBM z/OS must employ a session for users to directly initiate a session lock for all connection types.
RACF-OS-000430	C2RHO430	IBM z/OS must employ a session manager to manage retaining a users session lock until that user reestablishes access using established identification and authentication procedures.
RACF-OS-000440	C2RHO440	IBM z/OS system administrator must develop a procedure to remove or disable temporary user accounts after 72 hours.
RACF-OS-000460	C2RHO460	IBM z/OS system administrator must develop a procedure to notify designated personnel if baseline configurations are changed in an unauthorized manner.
RACF-OS-000470	CKAHO470	IBM z/OS system administrator must develop a procedure to provide an audit reduction capability that supports on-demand reporting requirements.
RACF-OS-000480	C2RHO480	IBM z/OS system administrator must develop a procedure to terminate all sessions and network connections related to non-local maintenance when non-local maintenance is completed. Removed starting with z/OS RACF STIG version 9.1.
RACF-OS-000490	C2RHO490	IBM z/OS system administrator must develop a procedure to remove all software components after updated versions have been installed.
RACF-OS-000500	C2RHO500	IBM z/OS must shut down the information system, restart the information system, and/or notify the system administrator when anomalies in the operation of any security functions are discovered.
RACF-OS-000510	C2RHO510	IBM z/OS system administrator must develop a procedure to offload SMF files to a different system or media than the system being audited.
RACF-SH-000010	C2RHSH10	IBM z/OS SMF recording options for the SSH daemon must be configured to write SMF records for all eligible events.

Table 3. IBM z/OS RACF STIG (continued)

STIG ID	CARLa member	Rule Title
RACF-SH-000020	C2RHSH20	The IBM RACF SSH daemon must be configured to use a FIPS 140-2 compliant cryptographic algorithm to protect confidential information and remote access sessions.
RACF-SH-000040	C2RHSH40	The SSH daemon must be configured with the Standard Mandatory DoD Notice and Consent Banner.
RACF-SH-000050	C2RHSH50	IBM z/OS SSH daemon must be configured to only use the SSHv2 protocol.
RACF-SH-000060	C2RHSH60	IBM z/OS for PKI-based authentication must use the ICSF or ESM for key management.
RACF-SL-000010	CKAHSL10	IBM z/OS permission bits and user audit bits for HFS objects that are part of the Syslog daemon component must be properly configured.
RACF-SL-000020	C2RHSL20	The IBM z/OS Syslog daemon must be started at z/OS initialization.
RACF-SL-000030	CKAHSL30	The IBM z/OS Syslog daemon must be properly defined and secured.
RACF-SM-000010	CKAHSM10	IBM z/OS DFSMS Program Resources must be properly defined and protected.
RACF-SM-000020	CKAHSM20	IBM z/OS DFSMS control data sets must be protected in accordance with security requirements.
RACF-SM-000030	CKAHSM30	IBM z/OS DFSMS-related RACF classes must be active.
RACF-SM-000040	CKAHSM40	IBM z/OS DFSMS resources must be protected in accordance with the proper security requirements.
RACF-SM-000050	C2RHSM50	IBM z/OS using DFSMS must properly specify SYS(x).PARMLIB(IGDSMSxx), SMS parameter settings.
RACF-SM-000060	C2RHSM60	IBM z/OS DFSMS control data sets must reside on separate volumes.
RACF-TC-000010	C2RHT010	IBM z/OS PROFILE.TCPIP configuration statements for the TCP/IP stack must be coded properly.
RACF-TC-000020	Not supported	IBM z/OS must be configured to restrict all TCP/IP ports to ports, protocols, and/or services as defined in the PPSM CAL and vulnerability assessments.
RACF-TC-000030	C2RHT030	IBM z/OS permission bits and user audit bits for HFS objects that are part of the Base TCP/IP component must be properly configured.
RACF-TC-000040	CKAHT040	IBM z/OS TCP/IP resources must be properly protected.
RACF-TC-000050	CKAHT050	The IBM RACF SERVAUTH resource class must be active for TCP/IP resources.
RACF-TC-000065	CKAHT065	IBM z/OS started tasks for the Base TCP/IP component must be defined in accordance with security requirements.
RACF-TC-000070	CKAHT070	IBM z/OS data sets for the Base TCP/IP component must be properly protected.

Table 3. IBM z/OS RACF STIG (continued)

STIG ID	CARLa member	Rule Title
RACF-TC-000080	C2RHT080	IBM z/OS Configuration files for the TCP/IP stack must be properly specified.
RACF-TC-000100	C2RHT100	The IBM z/OS TCPIP.DATA configuration statement must contain the DOMAINORIGIN or DOMAIN specified for each TCP/IP defined.
RACF-TC-000110	Not supported	IBM z/OS TCP/IP AT-TLS policy must be properly configured in Policy Agent.
RACF-TN-000020	C2RHTN20	IBM z/OS SSL encryption options for the TN3270 Telnet Server must be specified properly for each statement that defines a SECUREPORT or within the TELNETGLOBALS.
RACF-TN-000040	C2RHTN40	The IBM z/OS warning banner for the TN3270 Telnet server must contain the proper content of the Standard Mandatory DoD Notice and Consent Banner.
RACF-TN-000050	C2RHTN50	IBM z/OS VTAM session setup controls for the TN3270 Telnet server must be properly specified.
RACF-TN-000060	C2RHTN60	The IBM z/OS PROFILE.TCPIP configuration for the TN3270 Telnet server must have the INACTIVE statement properly specified.
RACF-TS-000010	CKAHTS10	IBM Z/OS TSOAUTH resources must be restricted to authorized users.
RACF-TS-000020	C2RHTS20	IBM RACF logonids must not be defined to SYS1.UADS for non-emergency use.
RACF-US-000010	CKAHU010	The IBM z/OS UNIX SUPERUSER resources must be protected in accordance with guidelines.
RACF-US-000020	CKAHU020	IBM z/OS BPX resource(s) must be protected in accordance with security requirements.
RACF-US-000030	C2RHU030	IBM z/OS UNIX MVS HFS directories with other write permission bit set must be properly defined.
RACF-US-000050	C2RHU050	IBM z/OS UNIX security parameters in etc/profile must be properly specified.
RACF-US-000060	C2RHU060	IBM z/OS UNIX security parameters in /etc/rc must be properly specified.
RACF-US-000070	CKAHU070	IBM z/OS UNIX resources must be protected in accordance with security requirements.
RACF-US-000080	CKAHU080	IBM z/OS UNIX MVS data sets or HFS objects must be properly protected.
RACF-US-000090	CKAHU090	IBM z/OS UNIX MVS data sets WITH z/OS UNIX COMPONENTS must be properly protected.
RACF-US-000100	C2RHU100	IBM z/OS UNIX HFS permission bits and audit bits for each directory must be properly protected.
RACF-US-000110	C2RHU110	IBM z/OS UNIX SYSTEM FILE SECURITY SETTINGS must be properly protected or specified.
RACF-US-000120	CKAHU120	IBM z/OS UNIX MVS data sets used as step libraries in /etc/steplib must be properly protected.

Table 3. IBM z/OS RACF STIG (continued)

STIG ID	CARLa member	Rule Title
RACF-US-000130	CKAHU130	The IBM RACF classes required to properly secure the z/OS UNIX environment must be ACTIVE.
RACF-US-000140	C2RHU140	IBM z/OS UNIX OMVS parameters in PARMLIB must be properly specified.
RACF-US-000150	C2RHU150	IBM z/OS UNIX BPXPRMxx security parameters in PARMLIB must be properly specified.
RACF-US-000160	CKAHU160	IBM z/OS default profiles must be defined in the corresponding FACILITY Class Profile for classified systems.
RACF-US-000170	C2RHU170	IBM z/OS UNIX HFS MapName files security parameters must be properly specified.
RACF-US-000180	C2RHU180	IBM z/OS UNIX security parameters for restricted network service(s) in /etc/inetd.conf must be properly specified.
RACF-US-000190	CKAHU190	IBM z/OS UID(0) must be properly assigned.
RACF-US-000200	CKAHU200	IBM z/OS UNIX groups must be defined with a unique GID.
RACF-US-000220	CKAHU220	The IBM z/OS user account for the UNIX kernel (OMVS) must be properly defined to the security database.
RACF-US-000230	CKAHU230	The IBM z/OS user account for the z/OS UNIX SUPERUSER user ID must be properly defined.
RACF-US-000240	CKAHU240	The IBM z/OS user account for the UNIX (RMFGAT) must be properly defined.
RACF-US-000250	CKAHU250	IBM z/OS UNIX user accounts must be properly defined.
RACF-US-000260	CKAHU260	IBM z/OS attributes of UNIX user accounts used for account modeling must be defined in accordance with security requirements.
RACF-UT-000010	C2RHUT10	The IBM z/OS startup user account for the z/OS UNIX Telnet Server must be properly defined.
RACF-UT-000020	C2RHUT20	IBM z/OS HFS objects for the z/OS UNIX Telnet Server must be properly protected.
RACF-UT-000030	C2RHUT30	The IBM z/OS UNIX Telnet Server etc/banner file must have the Standard Mandatory DoD Notice and Consent Banner.
RACF-UT-000040	C2RHUT40	IBM z/OS UNIX Telnet server Startup parameters must be properly specified.
RACF-UT-000050	C2RHUT50	The IBM z/OS UNIX Telnet server warning banner must be properly specified.
RACF-VT-000010	CKAHVT10	IBM z/OS System data sets used to support the VTAM network must be properly secured.
RACF-VT-000020	C2RHVT20	IBM z/OS VTAM USSTAB definitions must not be used for unsecured terminals.
RACF-ZO-000010	CKAHZO10	z/OSMF resource class(es) must be active in accordance with security requirements.
RACF-ZO-000020	Not supported	z/OSMF resources must be protected in accordance with security requirements.

IBM z/OS RACF Products STIG

Table 4. IBM z/OS RACF Products STIG

STIG ID	CARLa member	Rule Title
ZADTR000	CKAHAU00	CA Auditor installation data sets are not properly protected.
ZADTR002	CKAHAU02	CA Auditor User data sets are not properly protected.
ZADTR020	CKAHAU20	CA Auditor resources are not properly defined and protected.
ZAID0040	C2RHAA40	Compuware Abend-AID external security options must be specified properly.
ZAIDR000	CKAHAA00	Compuware Abend-AID installation data sets will be properly protected.
ZAIDR001	CKAHAA01	Compuware Abend-AID STC data sets must be properly protected.
ZAIDR002	CKAHAA02	Compuware Abend-AID user data sets must be properly protected.
ZAIDR020	CKAHAA20	Compuware Abend-AID resources must be properly defined and protected.
ZAIDR030	CKAHAA30	Compuware Abend-AID Started Task name will be properly identified and/or defined to the system ACP.
ZAIDR032	CKAHAA32	Compuware Abend-AID Started task will be properly defined to the STARTED resource class for RACF.
ZCA10041	C2RHTM41	CA 1 Tape Management system password will be changed from the default.
ZCA10060	C2RHTM60	CA 1 Tape Management user exits, when in use, must be reviewed and/or approved.
ZCA1R000	CKAHTM00	CA 1 Tape Management installation data sets must be properly protected.
ZCA1R001	CKAHTM01	CA-1 Tape Management STC data sets must be properly protected.
ZCA1R003	CKAHTM03	CA 1 Tape Management TMC, AUDIT and optional RDS and VPD data sets will be properly protected.
ZCA1R020	CKAHTM20	CA 1 Tape Management command resources must be properly defined and protected.
ZCA1R021	CKAHTM21	CA 1 Tape Management function and password resources must be properly defined and protected.
ZCA1R030	CKAHTM30	CA 1 Tape Management Started Task name will be properly identified and/or defined to the system ACP.
ZCA1R032	CKAHTM32	CA 1 Tape Management Started task will be properly defined to the STARTED resource class for RACF.
ZCA1R038	CKAHTM38	CA 1 Tape Management Resource Class will be defined or active in the ACP.
ZCA1R040	CKAHTM40	CA 1 Tape Management external security options must be specified properly.
ZCCSR000	CKAHCS00	CA Common Services installation data sets will be properly protected.

Table 4. IBM z/OS RACF Products STIG (continued)

STIG ID	CARLa member	Rule Title
ZCCSR030	CKAHCS30	CA Common Services Started Task name will be properly identified and/or defined to the system ACP.
ZCCSR032	CKAHCS32	CA Common Services Started task will be properly defined to the STARTED resource class for RACF.
ZCIC0010	CKAHCI10	CICS system data sets are not properly protected.
ZCIC0020	CKAHCI20	Sensitive CICS transactions are not protected in accordance with security requirements.
ZCIC0030	C2RHCI30	CICS System Initialization Table (SIT) parameter values must be specified in accordance with proper security requirements.
ZCIC0040	CKAHCI40	CICS region logonid(s) must be defined and/or controlled in accordance with the security requirements.
ZCIC0041	CKAHCI41	CICS default logonid(s) must be defined and/or controlled in accordance with the security requirements.
ZCIC0042	CKAHCI42	CICS logonid(s) must have time-out limit set to 15 minutes.
ZCICR021	CKAHCC21	IBM CICS Transaction Server SPI command resources must be properly defined and protected.
ZCICR038	CKAHCI38	External RACF Classes are not active for CICS transaction checking.
ZCICR041	CKAHCC41	CICS regions are improperly protected to prevent unauthorized propagation of the region user ID.
ZCLS0040	C2RHSS40	CL/SuperSession profile options are set improperly.
ZCLS0041	C2RHSS41	CL/SuperSession is not properly configured to generate SMF records for audit trail and accounting reports.
ZCLSR000	CKAHSS00	CL/SuperSession Install data sets must be properly protected.
ZCLSR001	CKAHSS01	CL/SuperSession STC data sets must be properly protected.
ZCLSR030	CKAHSS30	CL/SuperSession Started Task name is not properly identified / defined to the system ACP.
ZCLSR032	CKAHSS32	CL/SuperSession Started task(s) must be properly defined to the STARTED resource class for RACF.
ZCLSR038	CKAHSS38	CL/SuperSession's Resource Class will be defined or active in the ACP.
ZCLSR042	CKAHSS42	CL/SuperSession KLVINNAM member must be configured in accordance to security requirements.
ZCLSR043	CKAHSS43	CL/SuperSession APPCLASS member is not configured in accordance with the proper security requirements.
ZCSLR000	CKAHCT00	Catalog Solutions Install data sets are not properly protected.
ZCSLR020	CKAHCT20	Catalog Solutions resources must be properly defined and protected.
ZCTD0040	C2RHCD40	BMC CONTROL-D configuration/parameter values are not specified properly.

Table 4. IBM z/OS RACF Products STIG (continued)		
STIG ID	**CARLa member**	**Rule Title**
ZCTD0060	C2RHCD60	BMC CONTROL-D security exits are not installed or configured properly.
ZCTDR000	CKAHCD00	BMC CONTROL-D installation data sets will be properly protected.
ZCTDR001	CKAHCD01	BMC CONTROL-D STC data sets must be properly protected.
ZCTDR002	CKAHCD02	BMC CONTROL-D user data sets must be properly protected.
ZCTDR020	CKAHCD20	BMC CONTROL-D resources must be properly defined and protected.
ZCTDR030	CKAHCD30	BMC CONTROL-D Started Task name is not properly identified / defined to the system ACP.
ZCTDR032	CKAHCD32	BMC CONTROL-D Started task(s) must be properly defined to the STARTED resource class for RACF.
ZCTM0060	C2RHCM60	BMC CONTROL-M security exits are not installed or configured properly.
ZCTMR000	CKAHCM00	BMC CONTROL-M installation data sets will be properly protected.
ZCTMR001	CKAHCM01	BMC CONTROL-M STC data sets will be properly protected.
ZCTMR002	CKAHCM02	BMC CONTROL-M User data sets will be properly protected.
ZCTMR003	CKAHCM03	BMC CONTROL-M User/Application JCL data sets must be properly protected.
ZCTMR020	CKAHCM20	BMC C0NTROL-M resources must be properly defined and protected.
ZCTMR030	CKAHCM30	BMC CONTROL-M Started Task name is not properly identified / defined to the system ACP.
ZCTMR032	CKAHCM32	BMC CONTROL-M Started task(s) must be properly defined to the STARTED resource class for RACF.
ZCTMR040	CKAHCM40	BMC CONTROL-M configuration/parameter values must be specified properly.
ZCTO0040	C2RHCO40	BMC CONTROL-O configuration/parameter values are not specified properly.
ZCTO0041	C2RHCO41	BMC CONTROL-O configuration/parameter values are not specified properly.
ZCTO0060	C2RHCO60	BMC CONTROL-O security exits are not installed or configured properly.
ZCTOR000	CKAHCO00	BMC CONTROL-O installation data sets will be properly protected.
ZCTOR001	CKAHCO01	BMC CONTROL-O STC data sets must be properly protected.
ZCTOR020	CKAHCO20	BMC CONTROL-O resources must be properly defined and protected.
ZCTOR030	CKAHCO30	BMC CONTROL-O Started Task name is not properly identified / defined to the system ACP.
ZCTOR032	CKAHCO32	BMC CONTROL-O Started task(s) must be properly defined to the STARTED resource class for RACF.

Table 4. IBM z/OS RACF Products STIG (continued)		
STIG ID	**CARLa member**	**Rule Title**
ZCTRR000	CKAHCR00	BMC CONTROL-M/Restart installation data sets will be not properly protected.
ZCTRR002	CKAHCR02	BMC CONTROL-M/Restart Archived Sysout data sets must be properly protected.
ZFDR0040	C2RHFD40	FDR (Fast Dump Restore) security options are improperly specified.
ZFDRR000	CKAHFD00	Fast Dump Restore (FDR) install data sets are not properly protected.
ZFEP0011	C2RHFE11	All hardware components of the FEPs are not placed in secure locations where they cannot be stolen, damaged, or disturbed
ZFEP0013	C2RHFE13	A documented procedure is not available instructing how to load and dump the FEP NCP (Network Control Program).
ZFEP0014	C2RHFE14	An active log is not available to keep track of all hardware upgrades and software changes made to the FEP (Front End Processor).
ZFEP0015	CKAHFE15	NCP (Net Work Control Program) Data set access authorization does not restricts UPDATE and/or ALLOCATE access to appropriate personnel.
ZFEP0016	C2RHFE16	A password control is not in place to restrict access to the service subsystem via the operator consoles (local and/or remote) and a key-lock switch is not used to protect the modem supporting the remote console of the service subsystem.
ZHCDR000	CKAHHD00	IBM Hardware Configuration Definition (HCD) install data sets are not properly protected.
ZHCDR002	CKAHHD02	IBM Hardware Configuration Definition (HCD) User data sets are not properly protected.
ZHCDR020	CKAHHD20	IBM Hardware Configuration Definition (HCD) resources are not properly defined and protected.
ZHCKR001	CKAHHC01	IBM Health Checker STC data sets will be properly protected.
ZHCKR030	CKAHHC30	IBM Health Checker Started Task name will be properly identified and/or defined to the system ACP.
ZHCKR032	CKAHHC32	IBM Health Checker Started task will be properly defined to the STARTED resource class for RACF.
ZIOA0060	C2RHOA60	BMC IOA security exits are not installed or configured properly.
ZIOAR000	CKAHOA00	BMC IOA installation data sets will be properly protected.
ZIOAR001	CKAHOA01	BMC IOA STC data sets must be properly protected.
ZIOAR002	CKAHOA02	BMC IOA User data sets will be properly protected.
ZIOAR020	CKAHOA20	BMC IOA resources must be properly defined and protected.
ZIOAR030	CKAHOA30	BMC IOA Started Task name must be properly identified and defined to the system ACP.
ZIOAR032	CKAHOA32	BMC IOA Started task(s) must be properly defined to the STARTED resource class for RACF.

Table 4. IBM z/OS RACF Products STIG (continued)		
STIG ID	**CARLa member**	**Rule Title**
ZIOAR040	CKAHOA40	BMC IOA configuration/parameter values are not specified properly.
ZISF0040	C2RHSF40	IBM System Display and Search Facility (SDSF) Configuration parameters must be correctly specified.
ZISFR000	CKAHSF00	IBM System Display and Search Facility (SDSF) installation data sets will be properly protected.
ZISFR002	CKAHSF02	IBM System Display and Search Facility (SDSF) HASPINDX data set identified in the INDEX parameter must be properly protected.
ZISFR020	CKAHSF20	IBM System Display and Search Facility (SDSF) resources will be properly defined and protected.
ZISFR021	CKAHSF21	IBM System Display and Search Facility (SDSF) resources will be properly defined and protected.
ZISFR030	CKAHSF30	IBM System Display and Search Facility (SDSF) Started Task name will be properly identified and/or defined to the system ACP.
ZISFR032	CKAHSF32	IBM System Display and Search Facility (SDSF) Started task will be properly defined to the STARTED resource class for RACF.
ZISFR038	CKAHSF38	IBM System Display and Search Facility (SDSF) Resource Class will be active in the RACF.
ZMICR000	CKAHMC00	CA MICS Resource Management installation data sets must be properly protected.
ZMICR002	CKAHMC02	CA MICS Resource Management User data sets must be properly protected.
ZMIM0040	C2RHMI40	CA MIM Resource Sharing external security options must be specified properly.
ZMIMR000	CKAHMI00	CA MIM Resource Sharing installation data sets will be properly protected.
ZMIMR001	CKAHMI01	CA MIM Resource Sharing STC data sets will be properly protected.
ZMIMR020	CKAHMI20	CA MIM Resource Sharing resources will be properly defined and protected.
ZMIMR030	CKAHMI30	CA MIM Resource Sharing Started Task name will be properly identified and/or defined to the system ACP.
ZMIMR032	CKAHMI32	CA MIM Resource Sharing Started task will be properly defined to the STARTED resource class for RACF.
ZMVZR000	CKAHMV00	BMC MAINVIEW for z/OS installation data sets are not properly protected.
ZMVZR001	CKAHMV01	BMC MAINVIEW for z/OS STC data sets are not properly protected.
ZMVZR020	CKAHMV20	BMC MAINVIEW resources must be properly defined and protected.
ZMVZR030	CKAHMV30	BMC Mainview for z/OS Started Task name is not properly identified and/or defined to the system ACP.
ZMVZR032	CKAHMV32	BMC Mainview for z/OS Started task(s) must be properly defined to the STARTED resource class for RACF.

Table 4. IBM z/OS RACF Products STIG (continued)

STIG ID	CARLa member	Rule Title
ZMVZR038	CKAHMV38	BMC Mainview for z/OS Resource Class will be defined or active in the ACP.
ZMVZR040	CKAHMV40	BMC MAINVIEW for z/OS configuration/parameter values are not specified properly.
ZNCPR000	CKAHNC00	Quest NC-Pass installation data sets will be properly protected.
ZNCPR001	CKAHNC01	Quest NC-Pass STC data sets will be properly protected.
ZNCPR020	CKAHNC20	Quest NC-Pass will be used by Highly-Sensitive users.
ZNCPR030	CKAHNC30	Quest NC-Pass Started Task name will be properly identified and/or defined to the system ACP.
ZNCPR032	CKAHNC32	Quest NC-Pass Started task will be properly defined to the STARTED resource class for RACF.
ZNET0040	C2RHNV40	NetView configuration/parameter values must be specified properly.
ZNETR000	CKAHNV00	NetView install data sets are not properly protected.
ZNETR001	CKAHNV01	NetView STC data sets are not properly protected.
ZNETR020	CKAHNV20	NetView resources must be properly defined and protected.
ZNETR030	CKAHNV30	NetView Started Task name(s) is not properly identified / defined to the system ACP.
ZNETR032	CKAHNV32	IBM Z NetView Started task(s) must be properly defined to the STARTED resource class for RACF.
ZROSR000	CKAHRS00	ROSCOE Install data sets are not properly protected.
ZROSR001	CKAHRS01	ROSCOE STC data sets are not properly protected.
ZROSR020	CKAHRS20	ROSCOE resources must be properly defined and protected.
ZROSR030	CKAHRS30	ROSCOE Started Task name is not properly identified / defined to the system ACP.
ZROSR032	CKAHRS32	ROSCOE Started task(s) must be properly defined to the STARTED resource class for RACF.
ZROSR038	CKAHRS38	The Roscoe Resource Class will be defined or active in the ACP.
ZROSR040	CKAHRS40	Product configuration/parameter values are not specified properly.
ZSMTR001	CKAHMT01	IBM Communications Server Simple Mail Transfer Protocol (CSSMTP) STC data sets must be properly protected.
ZSMTR030	CKAHMT30	IBM CSSMTP Started Task name is not properly identified and/or defined to the system ACP.
ZSMTR032	CKAHMT32	IBM CSSMTP Started task(s) must be properly defined to the STARTED resource class for RACF.
ZSRRR000	CKAHSR00	SRRAUDIT installation data sets must be properly protected.
ZSRRR002	CKAHSR02	SRRAUDIT User data sets are not properly protected.
ZTADR000	CKAHAD00	Tivoli Asset Discovery for z/OS (TADz) Install data sets are not properly protected.

Table 4. IBM z/OS RACF Products STIG (continued)		
STIG ID	**CARLa member**	**Rule Title**
ZTADR001	CKAHAD01	Tivoli Asset Discovery for z/OS (TADz) STC and/or batch data sets are not properly protected.
ZTADR030	CKAHAD30	Tivoli Asset Discovery for z/OS (TADz) Started Task name(s) must be properly identified / defined to the system ACP.
ZTADR032	CKAHAD32	IBM Tivoli Asset Discovery for z/OS (TADz) Started task(s) must be properly defined to the STARTED resource class for RACF.
ZTDM0040	C2RHDM40	Transparent Data Migration Facility (TDMF) configuration/ parameter/option values are not specified properly.
ZTDMR000	CKAHDM00	Transparent Data Migration Facility (TDMF) installation data sets will be not properly protected.
ZVSSR000	CKAHVS00	Vanguard Security Solutions (VSS) Install data sets are not properly protected.
ZVSSR002	CKAHVS02	Vanguard Security Solutions (VSS) User data sets are not properly protected.
ZVSSR020	CKAHVS20	Vanguard Security Solutions resources must be properly defined and protected.
ZVTAR000	CKAHVA00	CA VTAPE installation data sets are not properly protected.
ZVTAR001	CKAHVA01	CA VTAPE STC data sets will be properly protected.
ZVTAR030	CKAHVA30	CA VTAPE Started Task name is not properly identified/defined to the system ACP.
ZVTAR032	CKAHVA32	CA VTAPE Started task(s) must be properly defined to the STARTED resource class for RACF.
ZWAS0010	CKAHWS10	MVS data sets for the WebSphere Application Server must be protected in accordance with the proper security requirements.
ZWAS0020	C2RHWS20	HFS objects for the WebSphere Application Server must be protected in accordance with the proper security requirements.
ZWAS0030	CKAHWS30	The CBIND Resource Class for the WebSphere Application Server is not configured in accordance with security requirements.
ZWAS0040	C2RHWS40	Vendor-supplied user accounts for the WebSphere Application Server must be defined to the ACP.
ZWAS0050	C2RHWS50	The WebSphere Application Server plug-in is not specified in accordance with the proper security requirements.
ZWMQ0011	C2RHWM11	IBM MQ for z/OS channel security must be implemented in accordance with security requirements.
ZWMQ0012	C2RHWM12	IBM MQ for z/OS channel security must be implemented in accordance with security requirements.
ZWMQ0014	C2RHWM14	Production IBM MQ for z/OS remote subsystems must utilize Certified Name Filters (CNF).
ZWMQ0020	C2RHWM20	User timeout parameter values for IBM MQ for z/OS queue managers must be specified in accordance with security requirements.

Table 4. IBM z/OS RACF Products STIG (continued)		
STIG ID	**CARLa member**	**Rule Title**
ZWMQ0030	CKAHWM30	IBM MQ for z/OS started tasks must be defined in accordance with the proper security requirements.
ZWMQ0040	CKAHWM40	IBM MQ for z/OS all UPDATE and higher access to MQSeries®/ WebSphere MQ product and system data sets must be properly restricted.
ZWMQ0049	CKAHWM49	IBM MQ for z/OS resource classes must be properly activated for security checking by the ESM.
ZWMQ0051	C2RHWM51	IBM MQ for z/OS switch profiles must be properly defined to the appropriate ADMIN class.
ZWMQ0052	CKAHWM52	IBM MQ for z/OS connection class resource definitions must be protected in accordance with security.
ZWMQ0053	C2RHWM53	IBM MQ for z/OS dead-letter and alias dead-letter queues must be properly defined.
ZWMQ0054	CKAHWM54	IBM MQ for z/OS MQQUEUE queue resource profiles defined to the appropriate class must be protected in accordance with security requirements.
ZWMQ0055	CKAHWM55	IBM MQ for z/OS process resource profiles defined in the appropriate class must be protected in accordance with security requirements.
ZWMQ0056	CKAHWM56	IBM MQ for z/OS namelist resource profiles defined in the appropriate class must be protected in accordance with security requirements.
ZWMQ0057	CKAHWM57	IBM MQ for z/OS alternate user resources defined to appropriate ADMIN resource class must be protected in accordance with security requirements.
ZWMQ0058	CKAHWM58	IBM MQ for z/OS context resources defined to the appropriate ADMIN resource class must be protected in accordance with security requirements.
ZWMQ0059	CKAHWM59	IBM MQ for z/OS command resources defined to MQCMDS resource class are protected in accordance with security requirements.
ZWMQ0060	CKAHWM60	IBM MQ for z/OS RESLEVEL resources in the appropriate ADMIN resource class must be protected in accordance with security requirements.

IBM zSecure for RACF STIG

Table 5. IBM zSecure for RACF STIG		
STIG ID	**CARLa member**	**Rule Title**
ZSEC-00-000040	CKAHZ040	Access to zSecure installation data must be properly restricted and logged.
ZSEC-00-000060	CKAHZ060	Access to IBM zSecure STC data sets must be properly restricted and logged.

Table 5. IBM zSecure for RACF STIG (continued)		
STIG ID	**CARLa member**	**Rule Title**
ZSEC-00-000080	CKAHZ080	IBM zSecure access to user data sets must be properly restricted and logged.
ZSEC-00-000100	CKAHZ100	Started tasks for zSecure products must be properly defined.
ZSEC-00-000120	CKAHZ120	Access to IBM zSecure program resources must be limited to authorized users.
ZSEC-00-000140	CKAHZ140	zSecure must prevent non-privileged users from executing privileged zSecure functions.
ZSEC-00-000160	CKAHZ160	The zSecure programs CKFCOLL and CKGRACF, and the APF-authorized version of program CKRCARLA, must be restricted to security administrators, security batch jobs performing External Security Manager (ESM) maintenance, auditors, and systems programmers, and audited.
ZSEC-00-000200	CKAHZ200	IBM zSecure must implement organization-defined automated security responses if baseline zSecure configurations are changed in an unauthorized manner.
ZSEC-00-000220	CKAHZ220	IBM zSecure must remove all upgraded/replaced zSecure software components that are no longer required for operation after updated versions have been installed.
ZSEC-00-000240	CKAHZ240	IBM zSecure system administrators must install security-relevant zSecure software updates within the time period directed by an authoritative source (for example, IAVMs, CTOs, DTMs, and STIGs).
ZSEC-00-000260	CKAHZ260	XFACILIT class, or alternate class if specified in module CKRSITE, must be active.

PCI-DSS for RACF

The following table lists the Payment Card Industry Data Security Standard (PCI-DSS) standards that zSecure Audit supports. zSecure Audit does not support any other PCI-DSS requirements.

Table 6. PCI DSS for RACF		
PCI-DSS ID	**CARLa member**	**Rule Title**
PCI-DSS-1.2.5	C2RHP125	All services, protocols, and ports allowed are identified, approved, and have a defined business need.
PCI-DSS-1.2.6	C2RHP126	Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.
PCI-DSS-3.5.1	C2RHP351	PCI-PAN-clr classified data sets must be encrypted.
PCI-DSS-7.2.1	CKAHP721	Access rights for privileged user IDs must be restricted to least privileges to perform job responsibilities.
PCI-DSS-7.2.6	CKAHP726	All user access to query repositories of stored cardholder data is restricted.
PCI-DSS-7.3.3	CKAHP733	The access control system(s) is set to deny all by default.
PCI-DSS-8.2.1	CKAHP821	All users are assigned a unique ID before access to system components or cardholder data is allowed.

Table 6. PCI DSS for RACF (continued)

PCI-DSS ID	CARLa member	Rule Title
PCI-DSS-8.2.6	CKAHP826	Inactive user accounts are removed or disabled within 90 days of inactivity.
PCI-DSS-8.3.2	CKAHP832	Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.
PCI-DSS-8.3.4	CKAHP834	Invalid authentication attempts are limited by locking out the user ID after not more than 10 attempts.
PCI-DSS-8.3.7	CKAHP837	Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.
PCI-DSS-8.3.9	CKAHP839	User passwords must be changed at least every 90 days.
PCI-DSS-8.4.6	CKAHP846	User password length must be at least eight characters.
PCI-DSS-10.2.1.2	CKAHPA2C	Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts.

Chapter 3. zSecure compliance standards for ACF2

CIS IBM Db2 for z/OS Benchmark (ACF2)

This standard is available only if your organization has a license for Z Security and Compliance Center.

zSecure has added the CIS-DB2 prefix to the control number to help distinguish between CIS IBM z/OS RACF Benchmark control numbers and CIS IBM Db2 for z/OS Benchmark control numbers.

Table 7. CIS IBM Db2 for z/OS Benchmark (ACF2)

CIS Db2 Control ID	CARLa member	Rule Title
CIS-DB2-1.1.1	Not supported	Ensure that Db2 system data sets are protected
CIS-DB2-1.1.2	C2RHD112	Ensure that Db2 USS file system is protected
CIS-DB2-1.1.3	C2RHD113	Secure installation process
CIS-DB2-1.2.1	C2RHD121	Ensure that RACF changes are accepted immediately
CIS-DB2-1.2.2	C2RHD122	Ensure that authorization is enabled
CIS-DB2-1.2.3	Not supported	Ensure that the default authorization IDs are changed from the installation defined
CIS-DB2-1.2.4	C2RHD124	Ensure that generic error codes are returned for remote security errors
CIS-DB2-1.2.5	C2RHD125	Separate security administration from system administration
CIS-DB2-2.1.1	Not supported	Ensure subsystem access is protected
CIS-DB2-2.1.2	C2RHD212	Ensure secure authentication is enabled for remote access
CIS-DB2-2.1.3	C2RHD213	Secure access by using IBM Z Multi-Factor Authentication (MFA)
CIS-DB2-2.1.4	C2RHD214	Secure all remote connections by using SSL
CIS-DB2-2.1.5	Not supported	Secure remote connections by using TCP/IP Network Access control with the RACF SERVAUTH class
CIS-DB2-2.1.6	CKCHD216	Secure connections by using trusted contexts
CIS-DB2-2.1.7	CKCHD217	Secure object ownership by using Db2 roles
CIS-DB2-2.1.8	Not supported	Secure application access by using package controls
CIS-DB2-2.1.9	CKCHD219	Ensure that grant authorization IDs are defined in RACF
CIS-DB2-2.2.1	CKCHD221	Ensure that access to the catalog tables in the communications database (CDB) is restricted
CIS-DB2-2.2.2	CKCHD222	Ensure that access to SYSIBM.SYSAUDITPOLICIES is restricted
CIS-DB2-2.2.3	CKCHD223	Ensure that access to SYSIBM.SYSAUDITPOLICIES is restricted
CIS-DB2-2.2.4	CKCHD224	Ensure that access to SYSIBM.SYSCOLUMNS is restricted
CIS-DB2-2.2.5	CKCHD225	Ensure that access to trusted context tables is restricted
CIS-DB2-2.2.6	CKCHD226	Ensure that access to SYSIBM.SYSCONTROLS is restricted
CIS-DB2-2.2.7	CKCHD227	Ensure that access to SYSIBM.SYSDATABASE is restricted

Table 7. CIS IBM Db2 for z/OS Benchmark (ACF2) (continued)		
CIS Db2 Control ID	**CARLa member**	**Rule Title**
CIS-DB2-2.2.8	CKCHD228	Ensure that access to SYSIBM.SYSDBAUTH is restricted
CIS-DB2-2.2.9	CKCHD229	Ensure that access to dynamic query-related tables is restricted
CIS-DB2-2.2.10	CKCHD22A	Ensure that access to SYSIBM.SYSINDEXES is restricted (Manual)
CIS-DB2-2.2.11	CKCHD22B	Ensure that access to SYSIBM.SYSOBJROLEDEP is restricted
CIS-DB2-2.2.12	CKCHD22C	Ensure that access to package-related tables is restricted
CIS-DB2-2.2.13	CKCHD22D	Ensure that access to SYSIBM.SYSPACKAUTH is restricted
CIS-DB2-2.2.14	CKCHD22E	Ensure that access to SYSIBM.SYSPARMS is restricted
CIS-DB2-2.2.15	CKCHD22F	Ensure that access to SYSIBM.SYSPLAN is restricted
CIS-DB2-2.2.16	CKCHD22G	Ensure that access to SYSIBM.SYSPLANAUTH is restricted
CIS-DB2-2.2.17	CKCHD22H	Ensure that access to SYSIBM.SYSQUERY is restricted
CIS-DB2-2.2.18	CKCHD22I	Ensure that access to SYSIBM.SYSRESAUTH is restricted
CIS-DB2-2.2.19	CKCHD22J	Ensure that access to SYSIBM.SYSROLES is restricted
CIS-DB2-2.2.20	CKCHD22K	Ensure that access to SYSIBM.SYSROUTINEAUTH is restricted
CIS-DB2-2.2.21	CKCHD22L	Ensure that access to SYSIBM.SYSROUTINES is restricted
CIS-DB2-2.2.22	CKCHD22M	Ensure that access to SYSIBM.SYSROUTINESTEXT is restricted
CIS-DB2-2.2.23	CKCHD22N	Ensure that access to SYSIBM.SYSSCHEMAAUTH is restricted
CIS-DB2-2.2.24	CKCHD22O	Ensure that access to SYSIBM.SYSSEQUENCEAUTH is restricted
CIS-DB2-2.2.25	CKCHD22P	Ensure that access to SYSIBM.SYSSEQUENCES is restricted
CIS-DB2-2.2.26	CKCHD22Q	Ensure that access to SYSIBM.SYSSTMT is restricted
CIS-DB2-2.2.27	CKCHD22R	Ensure that access to SYSIBM.SYSSTOGROUP is restricted
CIS-DB2-2.2.28	CKCHD22S	Ensure that access to SYSIBM.SYSTABAUTH is restricted
CIS-DB2-2.2.29	CKCHD22T	Ensure that access to SYSIBM.SYSTABLES is restricted
CIS-DB2-2.2.30	CKCHD22U	Ensure that access to SYSIBM.SYSTABLESPACE is restricted
CIS-DB2-2.2.31	CKCHD22V	Ensure that access to SYSIBM.SYSTRIGGERS is restricted
CIS-DB2-2.2.32	CKCHD22W	Ensure that access to SYSIBM.SYSUSERAUTH is restricted
CIS-DB2-2.2.33	CKCHD22X	Ensure that access to variable-related tables is restricted
CIS-DB2-2.2.34	CKCHD22Y	Ensure that access to SYSIBM.SYSVARIABLEAUTH is restricted
CIS-DB2-2.2.35	CKCHD22Z	Ensure that access to SYSIBM.SYSVIEWS is restricted
CIS-DB2-2.3.1	CKCHD231	Ensure that access to the program authorization table is restricted
CIS-DB2-2.3.2	CKCHD232	Ensure that access to the REST services definition table is restricted
CIS-DB2-2.3.3	CKCHD233	Ensure that access to the query accelerator tables is restricted
CIS-DB2-2.3.4	CKCHD234	Ensure that access to profile tables is restricted
CIS-DB2-2.3.5	CKCHD235	Ensure that access to SQL Data Insights tables is restricted
CIS-DB2-2.4.1	CKCHD241	Secure SYSADM authority access

Table 7. CIS IBM Db2 for z/OS Benchmark (ACF2) (continued)		
CIS Db2 Control ID	**CARLa member**	**Rule Title**
CIS-DB2-2.4.2	CKCHD242	Secure SYSCTRL authority access
CIS-DB2-2.4.3	CKCHD243	Secure SYSOPR authority access
CIS-DB2-2.4.4	CKCHD244	Secure system DBADM authority access
CIS-DB2-2.4.5	CKCHD245	Secure DATAACCESS authority access
CIS-DB2-2.4.6	CKCHD246	Secure ACCESSCTRL authority access
CIS-DB2-2.4.7	CKCHD247	Secure PACKADM authority access
CIS-DB2-2.4.8	CKCHD248	Secure SQLADM authority access
CIS-DB2-2.4.9	CKCHD249	Secure database DBADM authority access
CIS-DB2-2.4.10	CKCHD24A	Secure database DBCTRL authority access
CIS-DB2-2.4.11	CKCHD24B	Secure database DBMAINT authority access
CIS-DB2-2.5.1	C2RHD251	Ensure that data is encrypted at rest and in-flight
CIS-DB2-2.5.2	Not supported	Secure sensitive data in memory
CIS-DB2-2.6.1	C2RHD261	Secure row access using row permit
CIS-DB2-2.6.2	C2RHD262	Secure column values using column mask
CIS-DB2-3.1.1	CKCHD311	Ensure that audit tracing is enabled during Db2 start up
CIS-DB2-3.1.2	CKCHD312	Ensure that critical audit traces are always enabled
CIS-DB2-3.1.3	C2RHD313	Ensure that authorization failures are audited
CIS-DB2-3.1.4	CKCHD314	Enable audit policies to audit installation system administrator and system operator access
CIS-DB2-3.1.5	CKCHD315	Enable auditing of system administrator access
CIS-DB2-3.1.6	CKCHD316	Enable auditing of database administrator access

IBM z/OS ACF2 STIG

Table 8. IBM z/OS ACF2 STIG		
STIG ID	**CARLa member**	**Rule Title**
ACF2-CE-000010	C2AHCE10	IBM z/OS Certificate Name Filtering must be implemented with appropriate authorization and documentation.
ACF2-CE-000020	C2AHCE20	IBM z/OS must not use Expired Digital Certificates.
ACF2-CE-000030	C2AHCE30	All IBM z/OS digital certificates in use must have a valid path to a trusted Certification authority.
ACF2-ES-000010	C2AHE010	CA-ACF2 OPTS GSO record must be set to ABORT mode.
ACF2-ES-000020	C2AHE020	The number of ACF2 users granted the special privilege PPGM must be justified.
ACF2-ES-000030	C2AHE030	The number of ACF2 users granted the special privilege OPERATOR must be kept to a strictly controlled minimum.

Table 8. IBM z/OS ACF2 STIG (continued)

STIG ID	CARLa member	Rule Title
ACF2-ES-000040	C2AHE040	The number of ACF2 users granted the special privilege CONSOLE must be justified.
ACF2-ES-000050	C2AHE050	The number of ACF2 users granted the special privilege ALLCMDS must be justified.
ACF2-ES-000060	C2AHE060	IBM z/OS system commands must be properly protected.
ACF2-ES-000070	C2AHE070	IBM z/OS Sensitive Utility Controls must be properly defined and protected.
ACF2-ES-000080	C2AHE080	CA-ACF2 NJE GSO record value must indicate validation options that apply to jobs submitted through a network job entry subsystem (JES2, JES3, RSCS).
ACF2-ES-000090	C2AHE090	CA-ACF2 must protect Memory and privileged program dumps in accordance with proper security requirements.
ACF2-ES-000100	Not supported	CA-ACF2 must properly define users that have access to the CONSOLE resource in the TSOAUTH resource class.
ACF2-ES-000120	C2AHE120	CA-ACF2 must limit access to SYSTEM DUMP data sets to appropriate authorized users.
ACF2-ES-000130	C2AHE130	CA-ACF2 must limit access to SYS(x).TRACE to system programmers only.
ACF2-ES-000140	C2AHE140	CA-ACF2 allocate access to system user catalogs must be properly protected.
ACF2-ES-000150	C2AHE150	ACF2 Classes required to properly security the z/OS UNIX environment must be ACTIVE.
ACF2-ES-000160	C2AHE160	Access to IBM z/OS special privilege TAPE-LBL or TAPE-BLP must be limited and/or justified.
ACF2-ES-000170	C2AHE170	CA-ACF2 must limit access to System page data sets (that is, PLPA, COMMON, and LOCALx) to system programmers.
ACF2-ES-000180	C2AHE180	IBM z/OS must protect dynamic lists in accordance with proper security requirements.
ACF2-ES-000190	C2AHE190	IBM z/OS Libraries included in the system REXXLIB concatenation must be properly protected.
ACF2-ES-000200	C2AHE200	CA-ACF2 must limit Write or greater access to SYS1.UADS To system programmers only and read and update access must be limited to system programmer personnel and/or security personnel.
ACF2-ES-000210	C2AHE210	CA-ACF2 must limit all system PROCLIB data sets to appropriate authorized users.
ACF2-ES-000220	C2AHE220	CA-ACF2 access to the System Master Catalog must be properly protected.
ACF2-ES-000230	C2AHE230	IBM z/OS MCS consoles access authorization(s) for CONSOLE resource(s) must be properly protected.
ACF2-ES-000240	C2AHE240	CA-ACF2 must limit Write or greater access to SYS1.NUCLEUS to system programmers only.

Table 8. IBM z/OS ACF2 STIG (continued)

STIG ID	CARLa member	Rule Title
ACF2-ES-000250	C2AHE250	CA-ACF2 must limit Write or greater access to SYS1.LPALIB to system programmers only.
ACF2-ES-000260	C2AHE260	CA-ACF2 must limit Write or greater access to SYS1.IMAGELIB to system programmers.
ACF2-ES-000270	C2AHE270	CA-ACF2 must limit Write or greater access to Libraries containing EXIT modules to system programmers only.
ACF2-ES-000280	C2AHE280	CA-ACF2 must limit Update and Allocate access to all APF-authorized libraries to system programmers only.
ACF2-ES-000290	C2AHE290	CA-ACF2 must limit Write or greater access to all LPA libraries to system programmers only.
ACF2-ES-000300	C2AHE300	CA-ACF2 must limit Update and Allocate access to LINKLIST libraries to system programmers only.
ACF2-ES-000310	C2AHE310	CA-ACF2 must limit update and allocate access to all system-level product installation libraries to system programmers only.
ACF2-ES-000320	C2AHE320	CA-ACF2 must limit Write or greater access to SYS1.SVCLIB to system programmers only.
ACF2-ES-000330	C2AHE330	CA-ACF2 Access to SYS1.LINKLIB must be properly protected.
ACF2-ES-000340	C2AHE340	CA-ACF2 must limit access to data sets used to back up and/or dump SMF collection files to appropriate users and/or batch jobs that perform SMF dump processing.
ACF2-ES-000350	C2RHTS20	CA-ACF2 logonids must not be defined to SYS1.UADS for non-emergency use.
ACF2-ES-000370	C2AHE370	IBM z/OS IEASYMUP resource must be protected in accordance with proper security requirements.
ACF2-ES-000380	C2AHE380	CA-ACF2 must limit Update and Allocate access to system backup files to system programmers and/or batch jobs that perform DASD backups.
ACF2-ES-000390	C2AHE390	ACF2 PPGM GSO record value must specify protected programs that are only executed by privileged users.
ACF2-ES-000430	C2AHE430	The CA-ACF2 PSWD GSO record values for MAXTRY and PASSLMT must be properly set.
ACF2-ES-000440	C2AHE440	IBM z/OS SYS1.PARMLIB must be properly protected.
ACF2-ES-000450	C2AHE450	CA-ACF2 must be installed, functional, and properly configured.
ACF2-ES-000470	C2AHE470	CA-ACF2 must limit update and allocate access to the JES2 System data sets (for example, Spool, Checkpoint, and Initialization parameters) to system programmers only.
ACF2-ES-000480	C2AHE480	CA-ACF2 must limit Write or greater access to libraries that contain PPT modules to system programmers only.
ACF2-ES-000490	C2AHE490	The EXITS GSO record value must specify the module names of site written ACF2 exit routines.
ACF2-ES-000500	C2AHE500	The CA-ACF2 LOGONID with the REFRESH attribute must have procedures for utilization.

Table 8. IBM z/OS ACF2 STIG (continued)

STIG ID	CARLa member	Rule Title
ACF2-ES-000510	C2AHE510	IBM z/OS TSO GSO record values must be set to the values specified.
ACF2-ES-000520	C2AHE520	IBM z/OS procedures must restrict ACF2 logonids with the READALL attribute to auditors and/or authorized users.
ACF2-ES-000530	C2AHE530	IBM z/OS must have the RULEVLD and RSRCVLD attributes specified for logonids with the SECURITY attribute.
ACF2-ES-000540	C2AHE540	IBM z/OS logonids with the AUDIT or CONSULT attribute must be properly scoped.
ACF2-ES-000550	C2AHE550	IBM z/OS LOGONID with the ACCTPRIV attribute must be restricted to the ISSO.
ACF2-ES-000560	C2AHE560	IBM z/OS batch jobs with restricted ACF2 logonids must have the PGM(xxxxxxxx) and SUBAUTH attributes or the SOURCE(xxxxxxxx) attribute assigned to the corresponding logonids.
ACF2-ES-000570	C2AHE570	CA-ACF2 RULEOPTS GSO record values must be set to the values specified.
ACF2-ES-000580	C2AHE580	The CA-ACF2 GSO OPTS record value must be properly specified.
ACF2-ES-000590	C2AHE590	CA-ACF2 must prevent the use of dictionary words for passwords.
ACF2-ES-000600	C2AHE600	CA-ACF2 database must be on a separate physical volume from its backup and recovery data sets.
ACF2-ES-000610	C2AHE610	CA-ACF2 database must be backed up on a scheduled basis.
ACF2-ES-000620	C2AHE620	ACF2 REFRESH attribute must be restricted to security administrators only.
ACF2-ES-000630	C2AHE630	ACF2 maintenance logonids must have corresponding GSO MAINT records.
ACF2-ES-000640	C2AHE640	ACF2 logonids with the NON-CNCL attribute specified in the associated LOGONID record must be listed as trusted and must be specifically approved.
ACF2-ES-000650	C2AHE650	ACF2 logonids with the ACCOUNT, LEADER, or SECURITY attribute must be properly scoped.
ACF2-ES-000660	C2AHE660	ACF2 logonids associated with started tasks that have the MUSASS attribute and the requirement to submit jobs on behalf of its users must have the JOBFROM attribute as required.
ACF2-ES-000670	C2AHE670	ACF2 logonids assigned for started tasks must have the STC attribute specified in the associated LOGONID record.
ACF2-ES-000680	C2AHE680	ACF2 emergency logonids with the REFRESH attribute must have the SUSPEND attribute specified.
ACF2-ES-000690	C2AHE690	ACF2 BACKUP GSO record must be defined with a TIME value specifies greater than 00 unless the database is shared and backed up on another system.
ACF2-ES-000700	C2AHE700	ACF2 APPLDEF GSO record if used must have supporting documentation indicating the reason it was used.

Table 8. IBM z/OS ACF2 STIG (continued)

STIG ID	CARLa member	Rule Title
ACF2-ES-000710	C2AHE710	ACF2 MAINT GSO record value if specified must be restricted to production storage management user.
ACF2-ES-000720	C2AHE720	ACF2 LINKLST GSO record if specified must only contains trusted system data sets.
ACF2-ES-000730	C2AHE730	IBM z/OS must properly protect MCS console user ID(s).
ACF2-ES-000740	C2AHE740	ACF2 BLPPGM GSO record must not be defined.
ACF2-ES-000750	C2AHE750	IBM z/OS UID(0) must be properly assigned.
ACF2-ES-000760	C2AHE760	IBM z/OS user account for the UNIX kernel (OMVS) must be properly defined to the security database.
ACF2-ES-000770	C2AHE770	IBM z/OS user account for the UNIX (RMFGAT) must be properly defined.
ACF2-ES-000780	C2AHE780	ACF2 logonids must be defined with the required fields completed.
ACF2-ES-000790	C2AHE790	CA-ACF2 defined user accounts must uniquely identify system users.
ACF2-ES-000800	C2AHE800	CA-ACF2 user ids found inactive for more than 35 days must be suspended.
ACF2-ES-000810	C2AHE810	CA-ACF2 PWPHRASE GSO record must be properly defined.
ACF2-ES-000820	C2AHE820	CA-ACF2 must enforce password complexity by requiring that at least one special character be used.
ACF2-ES-000840	C2AHE840	ACF2 PSWD GSO record value must be set to require at least one uppercase character be used.
ACF2-ES-000850	C2AHE850	ACF2 PSWD GSO record value must be set to require at least one numeric character be used.
ACF2-ES-000860	C2AHE860	ACF2 PSWD GSO record value must be set to require at least one lowercase character be used.
ACF2-ES-000870	C2AHE870	ACF2 PSWD GSO record value must be set to require the change of at least 50% of the total number of characters when passwords are changed.
ACF2-ES-000880	C2AHE880	ACF2 must use NIST FIPS-validated cryptography to protect passwords in the security database.
ACF2-ES-000890	C2AHE890	ACF2 PSWD GSO record value must be set to require a 60-day maximum password lifetime restriction.
ACF2-ES-000900	C2AHE900	ACF2 PSWD GSO record value must be set to require 24 hours/1 day as the minimum password lifetime.
ACF2-ES-000910	C2AHE910	ACF2 PSWD GSO record value must be set to prohibit password reuse for a minimum of five generations or more.
ACF2-ES-000920	C2AHE920	ACF2 TSOTWX GSO record values must be set to obliterate the logon password on TWX devices.
ACF2-ES-000930	C2AHE930	ACF2 TSOCRT GSO record values must be set to obliterate the logon to ASCII CRT devices.

Table 8. IBM z/OS ACF2 STIG (continued)

STIG ID	CARLa member	Rule Title
ACF2-ES-000940	C2AHE940	ACF2 TSO2741 GSO record values must be set to obliterate the logon password on 2741 devices.
ACF2-ES-000950	C2AHE950	ACF2 SECVOLS GSO record value must be set to VOLMASK(). Any local changes are justified and documented with the ISSO.
ACF2-ES-000960	C2AHE960	ACF2 RESVOLS GSO record value must be set to Volmask(-). Any other setting requires documentation justifying the change.
ACF2-ES-000970	C2AHE970	ACF2 security data sets and/or databases must be properly protected.
ACF2-ES-000980	C2AHE980	ACF2 AUTOERAS GSO record value must be set to indicate that ACF2 is controlling the automatic physical erasure of VSAM or non VSAM data sets.
ACF2-ES-000990	C2AHE990	The operating system must enforce a minimum 8-character password length.
ACF2-FT-000010	C2RHF010	IBM z/OS SMF recording options for the FTP Server must be configured to write SMF records for all eligible events.
ACF2-FT-000020	C2AHF020	IBM z/OS data sets for the FTP Server must be properly protected.
ACF2-FT-000030	C2RHF020	IBM z/OS permission bits and user audit bits for HFS objects that are part of the FTP Server component must be properly configured.
ACF2-FT-000040	C2RHF040	IBM z/OS FTP.DATA configuration statements must have a proper BANNER statement with the Standard Mandatory Department of Defense (DoD) Notice and Consent Banner.
ACF2-FT-000060	C2RHF050	IBM z/OS FTP.DATA configuration statements for the FTP Server must specify the BANNER statement.
ACF2-FT-000070	C2AHF070	IBM z/OS FTP Control cards must be properly stored in a secure PDS file.
ACF2-FT-000080	C2AHF080	The IBM z/OS TFTP Server program must be properly protected.
ACF2-FT-000090	C2AHF090	IBM z/OS FTP Server daemon must be defined with proper security parameters.
ACF2-FT-000100	Not supported	IBM z/OS startup parameters for the FTP Server must be defined in the SYSTCPD and SYSFTPD DD statements for configuration files.
ACF2-FT-000110	C2RHF110	IBM z/OS FTP.DATA configuration for the FTP Server must have INACTIVE statement properly set.
ACF2-FT-000120	C2RHF070	IBM z/OS FTP.DATA configuration statements for the FTP Server must be specified in accordance with requirements
ACF2-IC-000010	C2RHIC10	IBM Integrated Crypto Service Facility (ICSF) Configuration parameters must be correctly specified.
ACF2-IC-000020	C2AHIC20	IBM Integrated Crypto Service Facility (ICSF) install data sets must be properly protected.
ACF2-IC-000030	C2AHIC30	IBM Integrated Crypto Service Facility (ICSF) STC data sets must be properly protected.
ACF2-IC-000040	C2AHIC40	IBM Integrated Crypto Service Facility (ICSF) Started Task name must be properly identified / defined to the system ACP.

Table 8. IBM z/OS ACF2 STIG (continued)

STIG ID	CARLa member	Rule Title
ACF2-IC-000050	C2AHIC50	ICSF resource class(es) must be defined to the ACF2 GSO CLASMAP record in accordance with security requirements.
ACF2-IC-000060	Not supported	ICSF resources must be protected in accordance with security requirements.
ACF2-JS-000010	C2AHJ010	IBM z/OS JESTRACE and/or SYSLOG resources must be protected in accordance with security requirements.
ACF2-JS-000020	C2AHJ020	IBM z/OS JESSPOOL resources must be protected in accordance with security requirements.
ACF2-JS-000030	C2AHJ030	IBM z/OS JESNEWS resources must be protected in accordance with security requirements.
ACF2-JS-000040	C2AHJ040	IBM z/OS JES2 system commands must be protected in accordance with security requirements.
ACF2-JS-000050	C2AHJ050	IBM z/OS JES2 spool resources must be controlled in accordance with security requirements.
ACF2-JS-000060	C2AHJ060	IBM z/OS JES2 output devices must be properly controlled for Classified Systems.
ACF2-JS-000070	Not supported	IBM z/OS JES2 output devices must be controlled in accordance with the proper security requirements.
ACF2-JS-000080	C2AHJ080	IBM z/OS JES2 input sources must be controlled in accordance with the proper security requirements.
ACF2-JS-000090	Not supported	IBM z/OS Surrogate users must be controlled in accordance with proper security requirements.
ACF2-JS-000100	Not supported	IBM z/OS JES2 system commands must be protected in accordance with security requirements.
ACF2-OS-000010	Not supported	The IBM z/OS BPX.SMF resource must be properly configured.
ACF2-OS-000030	C2RHO290	IBM z/OS Inapplicable PPT entries must be invalidated.
ACF2-OS-000040	C2RHO090	IBM z/OS system administrator must develop a process notify appropriate personnel when accounts are removed.
ACF2-OS-000050	C2RHO070	IBM z/OS system administrator must develop a process notify appropriate personnel when accounts are modified.
ACF2-OS-000060	C2RHO080	IBM z/OS system administrator must develop a process notify appropriate personnel when accounts are deleted.
ACF2-OS-000070	C2RHO060	IBM z/OS system administrator must develop a process notify appropriate personnel when accounts are created.
ACF2-OS-000080	C2RH0110	IBM z/OS Required SMF data record types must be collected.
ACF2-OS-000090	C2AHO090	IBM z/OS special privileges must be assigned on an as-needed basis to logonids associated with STCs and logonids that need to execute TSO in batch.
ACF2-OS-000100	C2RHO130	IBM z/OS must specify SMF data options to assure appropriate activation.

Table 8. IBM z/OS ACF2 STIG (continued)

STIG ID	CARLa member	Rule Title
ACF2-OS-000110	C2RHO140	IBM z/OS SMF collection files (system MANx data sets or LOGSTREAM DASD) must have storage capacity to store at least one weeks worth of audit data.
ACF2-OS-000120	C2RHO150	IBM z/OS system administrators must develop an automated process to collect and retain SMF data.
ACF2-OS-000130	C2RHO160	IBM z/OS BUFUSEWARN in the SMFPRMxx must be properly set.
ACF2-OS-000140	C2RHO170	IBM z/OS NOBUFFS SMF parameter must be properly set (default is MSG).
ACF2-OS-000150	C2RHO190	IBM z/OS SNTP daemon (SNTPD) permission bits must be properly configured.
ACF2-OS-000160	C2RHO180	IBM z/OS SNTP daemon (SNTPD) must be active.
ACF2-OS-000170	C2RHO200	IBM z/OS PARMLIB CLOCKxx must have the Accuracy PARM coded properly.
ACF2-OS-000180	C2AHO180	IBM z/OS SMF collection files (that is, SYS1.MANx) access must be limited to appropriate users and/or batch jobs that perform SMF dump processing.
ACF2-OS-000200	C2RHO220	IBM z/OS PASSWORD data set and OS passwords must not be used.
ACF2-OS-000210	C2RHO010	IBM z/OS must configure system wait times to protect resource availability based on site priorities.
ACF2-OS-000220	C2AHO220	IBM z/OS Emergency logonids must be properly defined.
ACF2-OS-000240	C2RHO240	The IBM z/OS Policy Agent must employ a deny-all, allow-by-exception firewall policy for allowing connections to other systems.
ACF2-OS-000250	C2RHO250	Unsupported IBM z/OS system software must not be installed and/or active on the system.
ACF2-OS-000260	C2RHO260	IBM z/OS must not allow non-existent or inaccessible LINKLIST libraries.
ACF2-OS-000270	C2RHO270	IBM z/OS must not allow non-existent or inaccessible Link Pack Area (LPA) libraries.
ACF2-OS-000280	C2RHO280	IBM z/OS must not have inaccessible APF libraries defined.
ACF2-OS-000290	C2RHO300	IBM z/OS LNKAUTH=APFTAB must be specified in the IEASYSxx member(s) in the currently active parmlib data set(s).
ACF2-OS-000310	C2RHO310	Duplicated IBM z/OS sensitive utilities and/or programs must not exist in APF libraries.
ACF2-OS-000320	C2RHE680	IBM z/OS must properly configure CONSOLxx members.
ACF2-OS-000330	C2RHSH60	IBM z/OS for PKI-based authentication must use the ICSF or ESM for key management.
ACF2-OS-000340	C2RHO320	The IBM z/OS systems requiring data-at-rest protection must properly employ IBM DS8880 or equivalent hardware solutions for full disk encryption.
ACF2-OS-000350	C2RHO350	IBM z/OS sensitive and critical system data sets must not exist on shared DASD.

Table 8. IBM z/OS ACF2 STIG (continued)

STIG ID	CARLa member	Rule Title
ACF2-OS-000360	C2RHO360	IBM z/OS Policy Agent must contain a policy that protects against or limits the effects of Denial of Service (DoS) attacks by ensuring the operating system is implementing rate-limiting measures on impacted network interfaces.
ACF2-OS-000370	C2RHO370	The IBM z/OS Policy Agent must contain a policy that manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of Denial of Service (DoS) attacks.
ACF2-OS-002240	C2RHO430	IBM z/OS must employ a session manager to manage retaining a users session lock until that user reestablishes access using established identification and authentication procedures.
ACF2-OS-002330	C2RHO460	IBM z/OS system administrator must develop a procedure to notify designated personnel if baseline configurations are changed in an unauthorized manner.
ACF2-OS-002350	C2RHO400	IBM z/OS must employ a session manager that conceal, via the session lock, information previously visible on the display with a publicly viewable image.
ACF2-OS-002360	C2RHO410	IBM z/OS must employ a session manager to manage session lock after a 15-minute period of inactivity.
ACF2-OS-002370	C2RHO440	IBM z/OS System Administrator must develop a procedure to automatically remove or disable temporary user accounts after 72 hours.
ACF2-OS-002380	C2RHO450	IBM z/OS system administrator must develop a procedure to automatically remove or disable emergency accounts after the crisis is resolved or 72 hours.
ACF2-OS-002390	Not supported	IBM z/OS system administrator must develop a procedure to notify system administrators and ISSOs of account enabling actions.
ACF2-OS-002410	C2RHO480	IBM z/OS system administrator must develop a procedure to terminate all sessions and network connections related to non-local maintenance when non-local maintenance is completed. Removed starting with z/OS ACF2 STIG version 9.1.
ACF2-OS-002420	C2RHO490	IBM z/OS system administrator must develop a procedure to remove all software components after updated versions have been installed.
ACF2-OS-002430	C2RHO500	IBM z/OS system administrator must develop a procedure to shut down the information system, restart the information system, and/or notify the system administrator when anomalies in the operation of any security functions are discovered.
ACF2-OS-002440	C2RHO420	IBM z/OS must employ a session manager configured for users to directly initiate a session lock for all connection types.
ACF2-OS-002470	C2AHO470	ACF2 system administrator must develop a procedure to disable account identifiers (individuals, groups, roles, and devices) after 35 days of inactivity.
ACF2-OS-003430	C2RHO510	IBM z/OS system administrator must develop a procedure to offload SMF files to a different system or media than the system being audited.

Table 8. IBM z/OS ACF2 STIG (continued)		
STIG ID	**CARLa member**	**Rule Title**
ACF2-SH-000010	C2RHSH10	IBM z/OS SMF recording options for the SSH daemon must be configured to write SMF records for all eligible events.
ACF2-SH-000030	C2RHSH40	IBM z/OS SSH daemon must be configured with the Department of Defense (DoD) logon banner.
ACF2-SH-000040	C2RHSH50	IBM z/OS SSH daemon must be configured to only use the SSHv2 protocol.
ACF2-SH-000050	C2RHSH20	IBM z/OS SSH daemon must be configured to use a FIPS 140-2 compliant cryptographic algorithm.
ACF2-SL-000010	C2AHSL10	IBM z/OS permission bits and user audit bits for HFS objects that are part of the Syslog daemon component must be configured properly.
ACF2-SL-000020	C2RHSL20	IBM z/OS Syslog daemon must be started at z/OS initialization.
ACF2-SL-000030	C2AHSL30	IBM z/OS Syslog daemon must be properly defined and secured.
ACF2-SM-000010	C2AHSM10	IBM z/OS DFSMS resource class(es) must be defined to the GSO CLASMAP record in accordance with security requirements.
ACF2-SM-000020	C2AHSM20	IBM z/OS DFSMS Program Resources must be properly defined and protected.
ACF2-SM-000030	C2AHSM30	IBM z/OS DFSMS control data sets must be protected in accordance with security requirements.
ACF2-SM-000040	C2AHSM40	IBM z/OS DFMSM resource class(es)must be defined to the GSO SAFDEF record in accordance with security requirements.
ACF2-SM-000050	C2AHSM50	IBM z/OS DFSMS resources must be protected in accordance with the proper security requirements.
ACF2-SM-000060	C2RHSM50	IBM z/OS using DFSMS must properly specify SYS(x).PARMLIB(IGDSMSxx), SMS parameter settings.
ACF2-SM-000070	C2RHSM60	IBM z/OS DFSMS control data sets must reside on separate volumes.
ACF2-TC-000010	C2RHT010	IBM z/OS PROFILE.TCPIP configuration statements for the TCP/IP stack must be coded properly.
ACF2-TC-000020	Not supported	IBM z//OS must be configured to restrict all TCP/IP ports to ports, protocols, and/or services as defined in the PPSM CAL and vulnerability assessments.
ACF2-TC-000030	C2AHT030	IBM z/OS TCP/IP resources must be properly protected.
ACF2-TC-000040	C2RHT030	IBM z/OS permission bits and user audit bits for HFS objects that are part of the Base TCP/IP component must be configured properly.
ACF2-TC-000050	C2AHT050	IBM z/OS data sets for the Base TCP/IP component must be properly protected.
ACF2-TC-000060	C2RHT080	IBM z/OS Configuration files for the TCP/IP stack must be properly specified.
ACF2-TC-000070	C2AHT070	IBM z/OS Started tasks for the Base TCP/IP component must be defined in accordance with security requirements.

Table 8. IBM z/OS ACF2 STIG (continued)

STIG ID	CARLa member	Rule Title
ACF2-TC-000090	C2RHT100	IBM z/OS TCPIP.DATA configuration statement must contain the DOMAINORIGIN or DOMAIN specified for each TCP/IP defined.
ACF2-TC-000100	Not supported	IBM z/OS TCP/IP AT-TLS policy must be properly configured in Policy Agent.
ACF2-TN-000010	C2RHTN60	IBM z/OS PROFILE.TCPIP configuration INACTIVITY statement must be configured to 900 seconds.
ACF2-TN-000020	C2RHO030	IBM z/OS SMF recording options for the TN3270 Telnet Server must be properly specified.
ACF2-TN-000030	C2RHTN20	IBM z/OS SSL encryption options for the TN3270 Telnet Server must be specified properly for each statement that defines a SECUREPORT or within the TELNETGLOBALS.
ACF2-TN-000040	C2RHTN40	IBM z/OS TN3270 Telnet Server configuration statement MSG10 text must have the Standard Mandatory DoD Notice and Consent Banner.
ACF2-TN-000060	C2RHTN50	IBM z/OS VTAM session setup controls for the TN3270 Telnet Server must be properly specified.
ACF2-TS-000010	C2AHTS10	IBM z/OS TSOAUTH resources must be restricted to authorized users.
ACF2-US-000010	C2AHU010	IBM z/OS UNIX SUPERUSER resource must be protected in accordance with guidelines.
ACF2-US-000020	C2RHU050	IBM z/OS UNIX security parameters in etc/profile must be properly specified.
ACF2-US-000030	C2RHU060	IBM z/OS UNIX security parameters in /etc/rc must be properly specified.
ACF2-US-000040	C2AHU040	IBM z/OS UNIX resources must be protected in accordance with security requirements.
ACF2-US-000050	C2RHU030	IBM z/OS UNIX MVS HFS directory(s) with other write permission bit set must be properly defined.
ACF2-US-000060	C2AHU060	IBM z/OS BPX resource(s) must be protected in accordance with security requirements.
ACF2-US-000070	C2RHU110	IBM z/OS UNIX SYSTEM FILE SECURITY SETTINGS must be properly protected or specified.
ACF2-US-000080	C2AHU080	IBM z/OS UNIX MVS data sets with z/OS UNIX components must be properly protected.
ACF2-US-000090	C2AHU090	IBM z/OS UNIX MVS data sets or HFS objects must be properly protected.
ACF2-US-000100	C2RHU100	IBM z/OS UNIX HFS permission bits and audit bits for each directory must be properly protected.
ACF2-US-000110	C2AHU110	IBM z/OS UNIX MVS data sets used as step libraries in /etc/steplib must be properly protected.
ACF2-US-000140	C2RHU140	IBM z/OS UNIX OMVS parameters in PARMLIB must be properly specified.

Table 8. IBM z/OS ACF2 STIG (continued)		
STIG ID	**CARLa member**	**Rule Title**
ACF2-US-000150	C2RHU170	IBM z/OS UNIX HFS MapName files security parameters must be properly specified.
ACF2-US-000160	C2RHU150	IBM z/OS UNIX BPXPRMxx security parameters in PARMLIB must be properly specified.
ACF2-US-000170	C2RHF090	IBM z/OS User exits for the FTP Server must not be used without proper approval and documentation.
ACF2-US-000180	C2RHU180	IBM z/OS UNIX security parameters for restricted network service(s) in /etc/inetd.conf must be properly specified.
ACF2-US-000190	C2AHU190	IBM z/OS user account for the z/OS UNIX SUPERSUSER user ID must be properly defined.
ACF2-US-000200	C2AHU200	IBM z/OS UNIX user accounts must be properly defined.
ACF2-US-000210	C2AHU210	IBM z/OS UNIX groups must be defined with a unique GID.
ACF2-US-000220	C2AHU220	IBM z/OS Attributes of z/OS UNIX user accounts must have a unique GID in the range of 1-99.
ACF2-US-000230	C2AHU230	IBM z/OS Attributes of UNIX user accounts used for account modeling must be defined in accordance with security requirements.
ACF2-UT-000010	C2RHUT10	IBM z/OS startup user account for the z/OS UNIX Telnet Server must be defined properly.
ACF2-UT-000020	C2RHUT20	IBM z/OS HFS objects for the z/OS UNIX Telnet Server must be properly protected.
ACF2-UT-000030	C2RHUT30	IBM z/OS UNIX Telnet Server etc/banner file must have the Standard Mandatory DoD Notice and Consent Banner.
ACF2-UT-000040	C2RHUT50	IBM z/OS UNIX Telnet Server warning banner must be properly specified.
ACF2-UT-000050	C2RHUT50	IBM z/OS UNIX Telnet Server Startup parameters must be properly specified to display the banner.
ACF2-VT-000010	C2AHVT10	IBM z/OS System data sets used to support the VTAM network must be properly secured.
ACF2-VT-000020	C2RHVT20	IBM z/OS VTAM USSTAB definitions must not be used for unsecured terminals.
ACF2-ZO-000010	C2AHZO10	z/OSMF resource class(es) must be defined to the ACF2 GSO CLASMAP record in accordance with security requirements.
ACF2-ZO-000020	Not supported	z/OSMF resources must be protected in accordance with security requirements.

IBM z/OS ACF2 Products STIG

Table 9. IBM z/OS ACF2 Products STIG		
STIG ID	**CARLa member**	**Rule Title**
ZADTA000	C2AHAU00	CA Auditor installation data sets are not properly protected.

Table 9. IBM z/OS ACF2 Products STIG (continued)

STIG ID	CARLa member	Rule Title
ZADTA002	C2AHAU02	CA Auditor User data sets are not properly protected.
ZADTA020	C2AHAU20	CA Auditor resources are not properly defined and protected.
ZAIDA000	C2AHAA00	Compuware Abend-AID installation data sets will be properly protected.
ZAIDA001	C2AHAA01	Compuware Abend-AID STC data sets must be properly protected.
ZAIDA002	C2AHAA02	Compuware Abend-AID user data sets must be properly protected.
ZAIDA020	C2AHAA20	Compuware Abend-AID resources must be properly defined and protected.
ZAIDA030	C2AHAA30	Compuware Abend-AID Started Task name will be properly identified and/or defined to the system ACP.
ZAID0040	C2RHAA40	Compuware Abend-AID external security options must be specified properly
ZCA10041	C2RHTM41	CA 1 Tape Management system password will be changed from the default.
ZCA10060	C2RHTM60	CA 1 Tape Management user exits, when in use, must be reviewed and/or approved.
ZCA1A000	C2AHTM00	CA 1 Tape Management installation data sets must be properly protected.
ZCA1A001	C2AHTM01	CA-1 Tape Management STC data sets must be properly protected.
ZCA1A003	C2AHTM03	CA 1 Tape Management TMC, AUDIT and optional RDS and VPD data sets will be properly protected.
ZCA1A020	C2AHTM20	CA 1 Tape Management command resources must be properly defined and protected.
ZCA1A021	C2AHTM21	CA 1 Tape Management function and password resources must be properly defined and protected.
ZCA1A030	C2AHTM30	CA 1 Tape Management Started Task name will be properly identified and/or defined to the system ACP.
ZCA1A040	C2AHTM40	CA 1 Tape Management external security options must be specified properly.
ZCCSA000	C2AHCS00	CA Common Services installation data sets will be properly protected.
ZCCSA030	C2AHCS30	CA Common Services Started Task name will be properly identified and/or defined to the system ACP.
ZCIC0010	C2AHCI10	CICS system data sets are not properly protected.
ZCIC0020	Not supported	Sensitive CICS transactions are not protected in accordance with security requirements.
ZCIC0030	C2RHCI30	CICS System Initialization Table (SIT) parameter values must be specified in accordance with proper security requirements.
ZCIC0040	C2AHCI40	CICS region logonid(s) must be defined and/or controlled in accordance with the security requirements.

Table 9. IBM z/OS ACF2 Products STIG (continued)		
STIG ID	**CARLa member**	**Rule Title**
ZCIC0041	C2AHCI41	CICS default logonid(s) must be defined and/or controlled in accordance with the security requirements.
ZCIC0042	C2AHCI42	CICS logonid(s) must be configured with proper timeout and sign on limits.
ZCICA011	C2AHCI11	ACF2/CICS parameter data sets are not protected in accordance with the proper security requirements.
ZCICA021	C2AHCC21	IBM CICS Transaction Server SPI command resources must be properly defined and protected.
ZCICA022	Not supported	CICS startup JCL statement is not specified in accordance with the proper security requirements.
ZCICA023	Not supported	Key ACF2/CICS parameters must be properly coded.
ZCICA024	Not supported	Sensitive CICS transactions are not protected in accordance with the proper security requirements.
ZCICA025	Not supported	Sensitive CICS transactions are not protected in accordance with the proper security requirements.
ZCLS0040	C2RHSS40	CL/SuperSession profile options are set improperly.
ZCLS0041	C2RHSS41	CL/SuperSession is not properly configured to generate SMF records for audit trail and accounting reports.
ZCLSA000	C2AHSS00	CL/SuperSession Install data sets must be properly protected.
ZCLSA001	C2AHSS01	CL/SuperSession STC data sets must be properly protected.
ZCLSA030	C2AHSS30	CL/SuperSession Started Task name is not properly identified / defined to the system ACP.
ZCLSA042	C2AHSS42	CL/SuperSession KLVINNAM member must be configured in accordance to security requirements.
ZCLSA043	C2AHSS43	CL/SuperSession APPCLASS member is not configured in accordance with the proper security requirements.
ZCSLA000	C2AHCT00	Catalog Solution Install data sets are not properly protected.
ZCSLA020	C2AHCT20	Catalog Solutions resources must be properly defined and protected.
ZCTD0040	C2RHCD40	BMC CONTROL-D configuration/parameter values are not specified properly.
ZCTD0060	C2RHCD60	BMC CONTROL-D security exits are not installed or configured properly.
ZCTDA000	C2AHCD00	BMC CONTROL-D installation data sets will be properly protected.
ZCTDA001	C2AHCD01	BMC CONTROL-D STC data sets must be properly protected.
ZCTDA002	C2AHCD02	BMC CONTROL-D user data sets must be properly protected.
ZCTDA020	C2AHCD20	BMC CONTROL-D resources will be properly defined and protected.
ZCTDA030	C2AHCD30	BMC CONTROL-D Started Task name is not properly identified / defined to the system ACP.

Table 9. IBM z/OS ACF2 Products STIG (continued)

STIG ID	CARLa member	Rule Title
ZCTM0060	C2RHCM60	BMC CONTROL-M security exits are not installed or configured properly.
ZCTMA000	C2AHCM00	BMC CONTROL-M installation data sets will be properly protected.
ZCTMA001	C2AHCM01	BMC CONTROL-M STC data sets will be properly protected.
ZCTMA002	C2AHCM02	BMC CONTROL-M User data sets will be properly protected.
ZCTMA003	C2AHCM03	BMC CONTROL-M User/Application JCL data sets must be properly protected.
ZCTMA020	C2AHCM20	BMC C0NTROL-M resources must be properly defined and protected.
ZCTMA030	C2AHCM30	BMC CONTROL-M Started Task name is not properly identified / defined to the system ACP.
ZCTMA040	C2AHCM40	BMC CONTROL-M configuration/parameter values must be specified properly.
ZCTO0040	C2RHCO40	BMC CONTROL-O configuration/parameter values are not specified properly.
ZCTO0041	C2RHCO41	BMC CONTROL-O configuration/parameter values are not specified properly.
ZCTO0060	C2RHCO60	BMC CONTROL-O security exits are not installed or configured properly.
ZCTOA000	C2AHCO00	BMC CONTROL-O installation data sets will be properly protected.
ZCTOA001	C2AHCO01	BMC CONTROL-O STC data sets must be properly protected.
ZCTOA020	C2AHCO20	BMC CONTROL-O resources must be properly defined and protected.
ZCTOA030	C2AHCO30	BMC CONTROL-O Started Task name is not properly identified / defined to the system ACP.
ZCTRA000	C2AHCR00	BMC CONTROL-M/Restart installation data sets will be properly protected.
ZCTRA002	C2AHCR02	BMC CONTROL-M/Restart Archived Sysout data sets must be properly protected.
ZFDR0040	C2RHFD40	FDR (Fast Dump Restore) security options are improperly specified.
ZFDRA000	C2AHFD00	Fast Dump Restore (FDR) install data sets are not properly protected.
ZFEP0011	C2RHFE11	All hardware components of the FEPs are not placed in secure locations where they cannot be stolen, damaged, or disturbed
ZFEP0013	C2RHFE13	A documented procedure is not available instructing how to load and dump the FEP NCP (Network Control Program).
ZFEP0014	C2RHFE14	An active log is not available to keep track of all hardware upgrades and software changes made to the FEP (Front End Processor).
ZFEP0015	C2AHFE15	NCP (Net Work Control Program) Data set access authorization does not restricts UPDATE and/or ALLOCATE access to appropriate personnel.

Table 9. IBM z/OS ACF2 Products STIG (continued)		
STIG ID	**CARLa member**	**Rule Title**
ZFEP0016	C2RHFE16	A password control is not in place to restrict access to the service subsystem via the operator consoles (local and/or remote) and a key-lock switch is not used to protect the modem supporting the remote console of the service subsystem.
ZHCDA000	C2AHHD00	IBM Hardware Configuration Definition (HCD) install data sets are not properly protected.
ZHCDA002	C2AHHD02	IBM Hardware Configuration Definition (HCD) User data sets are not properly protected.
ZHCDA020	C2AHHD20	IBM Hardware Configuration Definition (HCD) resources are not properly defined and protected.
ZHCKA001	C2AHHC01	IBM Health Checker STC data sets will be properly protected.
ZHCKA030	C2AHHC30	IBM Health Checker Started Task name will be properly identified and/or defined to the system ACP.
ZIOA0060	C2RHOA60	BMC IOA security exits are not installed or configured properly.
ZIOAA000	C2AHOA00	BMC IOA installation data sets will be properly protected.
ZIOAA001	C2AHOA01	BMC IOA STC data sets must be properly protected.
ZIOAA002	C2AHOA02	BMC IOA User data sets will be properly protected.
ZIOAA020	C2AHOA20	BMC IOA resources will be properly defined and protected.
ZIOAA030	C2AHOA30	BMC IOA Started Task name must be properly identified and defined to the system ACP.
ZIOAA040	C2AHOA40	BMC IOA configuration/parameter values are not specified properly.
ZISF0040	C2RHSF40	IBM System Display and Search Facility (SDSF) Configuration parameters must be correctly specified.
ZISFA000	C2AHSF00	IBM System Display and Search Facility (SDSF) installation data sets will be properly protected.
ZISFA002	C2AHSF02	IBM System Display and Search Facility (SDSF) HASPINDX data set identified in the INDEX parameter must be properly protected.
ZISFA020	C2AHSF20	IBM System Display and Search Facility (SDSF) resources must be properly defined and protected.
ZISFA021	C2AHSF21	IBM System Display and Search Facility (SDSF) resources will be properly defined and protected.
ZISFA030	C2AHSF30	IBM System Display and Search Facility (SDSF) Started Task name will be properly identified and/or defined to the system ACP.
ZISFA038	C2AHSF38	IBM System Display and Search Facility (SDSF) Resource Class will be defined or active in the ACP.
ZMICA000	C2AHMC00	CA MICS Resource Management installation data sets must be properly protected.
ZMICA002	C2AHMC02	CA MICS Resource Management User data sets must be properly protected.

Table 9. IBM z/OS ACF2 Products STIG (continued)

STIG ID	CARLa member	Rule Title
ZMIM0040	C2RHMI40	CA MIM Resource Sharing external security options must be specified properly.
ZMIMA000	C2AHMI00	CA MIM Resource Sharing installation data sets will be properly protected.
ZMIMA001	C2AHMI01	CA MIM Resource Sharing STC data sets will be properly protected.
ZMIMA020	C2AHMI20	CA MIM Resource Sharing resources will be properly defined and protected.
ZMIMA030	C2AHMI30	CA MIM Resource Sharing Started Task name will be properly identified and/or defined to the system ACP.
ZMVZA000	C2AHMV00	BMC MAINVIEW for z/OS installation data sets are not properly protected.
ZMVZA001	C2AHMV01	BMC MAINVIEW for z/OS STC data sets are not properly protected.
ZMVZA020	C2AHMV20	BMC MAINVIEW resources must be properly defined and protected.
ZMVZA030	C2AHMV30	BMC Mainview for z/OS Started Task name must be properly identified and/or defined to the system ACP.
ZMVZA038	Not supported	BMC Mainview for z/OS Resource Class will be defined or active in the ACP.
ZMVZA040	C2AHMV40	BMC MAINVIEW for z/OS configuration/parameter values are not specified properly.
ZNCPA000	C2AHNC00	Quest NC-Pass installation data sets will be properly protected.
ZNCPA001	C2AHNC01	Quest NC-Pass STC data sets will be properly protected.
ZNCPA020	C2AHNC20	Quest NC-Pass will be used by Highly-Sensitive users.
ZNCPA030	C2AHNC30	Quest NC-Pass Started Task name will be properly identified and/or defined to the system ACP.
ZNET0040	C2RHNV40	NetView configuration/parameter values must be specified properly.
ZNETA000	C2AHNV00	NetView install data sets are not properly protected.
ZNETA001	C2AHNV01	NetView STC data sets are not properly protected.
ZNETA020	C2AHNV20	NetView resources must be properly defined and protected.
ZNETA030	C2AHNV30	NetView Started Task name must be properly identified / defined to the system ACP.
ZROSA000	C2AHRS00	ROSCOE Install data sets are not properly protected.
ZROSA001	C2AHRS01	ROSCOE STC data sets are not properly protected.
ZROSA020	C2AHRS20	ROSCOE resources must be properly defined and protected.
ZROSA030	C2AHRS30	ROSCOE Started Task name is not properly identified / defined to the system ACP.
ZROSA038	C2AHRS38	The ROSCOE's Resource Class is not defined or active in the ACP.
ZROSA040	C2AHRS40	ROSCOE configuration/parameter values are not specified properly.

Table 9. IBM z/OS ACF2 Products STIG (continued)		
STIG ID	**CARLa member**	**Rule Title**
ZSMTA001	C2AHMT01	IBM Communications Server Simple Mail Transfer Protocol (CSSMTP) STC data sets must be properly protected.
ZSMTA030	C2AHMT30	IBM CSSMTP Started Task name is not properly identified and/or defined to the system ACP.
ZSRRA000	C2AHSR00	SRRAUDIT installation data sets must be properly protected.
ZSRRA002	C2AHSR02	SRRAUDIT User data sets are not properly protected.
ZTADA000	C2AHAD00	Tivoli Asset Discovery for z/OS (TADz) Install data sets are not properly protected.
ZTADA001	C2AHAD01	Tivoli Asset Discovery for z/OS (TADz) STC and/or batch data sets are not properly protected.
ZTADA030	C2AHAD30	Tivoli Asset Discovery for z/OS (TADz) Started Task name(s) must be properly identified / defined to the system ACP.
ZTDM0040	C2RHDM40	Transparent Data Migration Facility (TDMF) configuration/ parameter/option values are not specified properly.
ZTDMA000	C2AHDM00	Transparent Data Migration Facility (TDMF) installation data sets will be not properly protected.
ZVTAA000	C2AHVA00	CA VTAPE installation data sets are not properly protected.
ZVTAA001	C2AHVA01	CA VTAPE STC data sets will be properly protected.
ZVTAA030	C2AHVA30	CA VTAPE Started Task name is not properly identified/defined to the system ACP.
ZWAS0010	C2AHWS10	MVS data sets for the WebSphere Application Server must be protected in accordance with the proper security requirements.
ZWAS0020	C2RHWS20	HFS objects for the WebSphere Application Server must be protected in accordance with the proper security requirements.
ZWAS0030	C2AHWS30	The CBIND Resource(s) for the WebSphere Application Server is(are) not protected in accordance with security requirements.
ZWAS0040	C2RHWS40	Vendor-supplied user accounts for the WebSphere Application Server must be defined to the ACP.
ZWAS0050	C2RHWS50	The WebSphere Application Server plug-in is not specified in accordance with the proper security requirements.
ZWMQ0011	C2RHWM11	IBM MQ for z/OS channel security must be implemented in accordance with security requirements.
ZWMQ0012	C2RHWM12	IBM MQ for z/OS channel security must be implemented in accordance with security requirements.
ZWMQ0014	C2RHWM14	Production IBM MQ for z/OS remote subsystems must utilize Certified Name Filters (CNF).
ZWMQ0020	C2RHWM20	User timeout parameter values for IBM MQ for z/OS queue managers must be specified in accordance with security requirements.
ZWMQ0030	C2AHWM30	IBM MQ for z/OS started tasks must be defined in accordance with the proper security requirements.

Table 9. IBM z/OS ACF2 Products STIG (continued)		
STIG ID	**CARLa member**	**Rule Title**
ZWMQ0040	C2AHWM40	IBM MQ for z/OS all WRITE and ALLOCATE access to MQSeries/ WebSphere MQ product and system data sets must be properly restricted.
ZWMQ0049	C2AHWM49	IBM MQ for z/OS resource classes must be properly activated.
ZWMQ0051	C2RHWM51	IBM MQ for z/OS switch profiles must be properly defined to the appropriate class.
ZWMQ0052	C2AHWM52	IBM MQ for z/OS connection class resources must be protected in accordance with security.
ZWMQ0053	C2RHWM53	IBM MQ for z/OS dead-letter and alias dead-letter queues must be properly defined.
ZWMQ0054	C2AHWM54	IBM MQ for z/OS queue resource defined to the MQQUEUE or MXQUEUE resource class must be protected in accordance with security requirements.
ZWMQ0055	C2AHWM55	IBM MQ for z/OS process resources must be protected in accordance with security requirements.
ZWMQ0056	C2AHWM56	IBM MQ for z/OS namelist resources must be protected in accordance with security requirements.
ZWMQ0057	C2AHWM57	IBM MQ for z/OS alternate user resources defined to the appropriate resource class must be protected in accordance with security requirements.
ZWMQ0058	C2AHWM58	IBM MQ for z/OS context resources defined to the appropriate resource class must be protected in accordance with security requirements.
ZWMQ0059	C2AHWM59	IBM MQ for z/OS command resources defined to MQCMDS resource class are protected in accordance with security requirements.
ZWMQ0060	C2AHWM60	IBM MQ for z/OS RESLEVEL resources in the appropriate ADMIN resource class must be protected in accordance with security requirements.

IBM zSecure for ACF2 STIG

Table 10. IBM zSecure for ACF2 STIG		
STIG ID	**CARLa member**	**Rule Title**
ZSEC-00-000040	C2AHZ040	Access to IBM zSecure installation data sets must be properly restricted and logged
ZSEC-00-000060	C2AHZ060	Access to IBM zSecure STC data sets must be properly restricted and logged
ZSEC-00-000080	C2AHZ080	Access to IBM zSecure user data sets must be properly restricted and logged
ZSEC-00-000100	C2AHZ100	Started tasks for IBM zSecure products must be properly defined
ZSEC-00-000120	C2AHZ120	Access to IBM zSecure program resources must be limited to authorized users

Table 10. IBM zSecure for ACF2 STIG (continued)		
STIG ID	**CARLa member**	**Rule Title**
ZSEC-00-000160	C2AHZ160	The use of zSecure programs CKFCOLL and CKGRACF, and the APF-authorized version of program CKRCARLA, must be restricted to security administrators, security batch jobs performing External Security Manager (ESM) maintenance, auditors, and systems programmers, and audited
ZSEC-00-000200	C2RHZ200	IBM zSecure must implement organization-defined automated responses if baseline zSecure configurations are changed in an unauthorized manner
ZSEC-00-000220	C2RHZ220	IBM zSecure must remove all upgraded/replaced zSecure software components that are no longer required for operation after updated versions have been installed
ZSEC-00-000240	C2RHZ240	IBM zSecure system administrators must install security-software updates within the time period directed by an authoritative source (e.g., IAVMs, CTOs, DTMs, and STIGs)

PCI-DSS for ACF2

The following table lists the Payment Card Industry Data Security Standard (PCI-DSS) standards that zSecure Audit supports. zSecure Audit does not support any other PCI-DSS requirements.

Table 11. PCI-DSS for ACF2		
PCI-DSS ID	**CARLa member**	**Rule Title**
PCI-DSS-1.2.5	C2RHP125	All services, protocols, and ports allowed are identified, approved, and have a defined business need.
PCI-DSS-1.2.6	C2RHP126	Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.
PCI-DSS-2.2.2	C2AHP222	Vendor default accounts must be disabled or removed.
PCI-DSS-3.5.1	C2RHP351	PCI-PAN-clr classified data sets must be encrypted.
PCI-DSS-8.2.1	C2AHP821	All users are assigned a unique ID before access to system components or cardholder data is allowed.
PCI-DSS-8.2.8	C2AHP828	If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session.
PCI-DSS-8.3.1	C2AHP831	All user access to system components for users and administrators is authenticated via at least one authentication factor.
PCI-DSS-8.3.2	C2AHP832	Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.
PCI-DSS-8.3.4	C2AHP834	Invalid authentication attempts are limited by locking out the user ID after not more than 10 attempts.
PCI-DSS-8.3.5	C2AHP835	Passwords and password phrases must be changed immediately after first use.
PCI-DSS-8.3.7	C2AHP837	Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.

Table 11. PCI-DSS for ACF2 (continued)

PCI-DSS ID	CARLa member	Rule Title
PCI-DSS-8.3.9	C2AHP839	User passwords and password phrases must be changed at least every 90 days.
PCI-DSS-8.4.6	C2AHP846	Users passwords and passphrases must require a minimum of seven characters and contain both numeric and alphabetic characters.
PCI-DSS-10.2.1.2	C2AHPA2C	Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts.

Chapter 4. zSecure compliance standards for Top Secret

CIS IBM Db2 for z/OS Benchmark (Top Secret)

This standard is available only if your organization has a license for Z Security and Compliance Center.

zSecure has added the CIS-DB2 prefix to the control number to help distinguish between CIS IBM z/OS RACF Benchmark control numbers and CIS IBM Db2 for z/OS Benchmark control numbers.

Table 12. CIS IBM Db2 for z/OS Benchmark (Top Secret)

CIS Db2 Control ID	CARLa member	Rule Title
CIS-DB2-1.1.1	Not supported	Ensure that Db2 system data sets are protected
CIS-DB2-1.1.2	C2RHD112	Ensure that Db2 USS file system is protected
CIS-DB2-1.1.3	C2RHD113	Secure installation process
CIS-DB2-1.2.1	C2RHD121	Ensure that RACF changes are accepted immediately
CIS-DB2-1.2.2	C2RHD122	Ensure that authorization is enabled
CIS-DB2-1.2.3	Not supported	Ensure that the default authorization IDs are changed from the installation defined
CIS-DB2-1.2.4	C2RHD124	Ensure that generic error codes are returned for remote security errors
CIS-DB2-1.2.5	C2RHD125	Separate security administration from system administration
CIS-DB2-2.1.1	Not supported	Ensure subsystem access is protected
CIS-DB2-2.1.2	C2RHD212	Ensure secure authentication is enabled for remote access
CIS-DB2-2.1.3	Not supported	Secure access by using Multi-Factor Authentication (MFA)
CIS-DB2-2.1.4	C2RHD214	Secure all remote connections by using SSL
CIS-DB2-2.1.5	Not supported	Secure remote connections by using TCP/IP Network Access control with the RACF SERVAUTH class
CIS-DB2-2.1.6	Not supported	Secure connections by using trusted contexts
CIS-DB2-2.1.7	Not supported	Secure object ownership by using Db2 roles
CIS-DB2-2.1.8	Not supported	Secure application access by using package controls
CIS-DB2-2.1.9	Not supported	Ensure that grant authorization IDs are defined in RACF
CIS-DB2-2.2.1	Not supported	Ensure that access to the catalog tables in the communications database (CDB) is restricted
CIS-DB2-2.2.2	Not supported	Ensure that access to SYSIBM.SYSAUDITPOLICIES is restricted
CIS-DB2-2.2.3	Not supported	Ensure that access to SYSIBM.SYSAUDITPOLICIES is restricted
CIS-DB2-2.2.4	Not supported	Ensure that access to SYSIBM.SYSCOLUMNS is restricted
CIS-DB2-2.2.5	Not supported	Ensure that access to trusted context tables is restricted
CIS-DB2-2.2.6	Not supported	Ensure that access to SYSIBM.SYSCONTROLS is restricted

Table 12. CIS IBM Db2 for z/OS Benchmark (Top Secret) (continued)		
CIS Db2 Control ID	**CARLa member**	**Rule Title**
CIS-DB2-2.2.7	Not supported	Ensure that access to SYSIBM.SYSDATABASE is restricted
CIS-DB2-2.2.8	Not supported	Ensure that access to SYSIBM.SYSDBAUTH is restricted
CIS-DB2-2.2.9	Not supported	Ensure that access to dynamic query-related tables is restricted
CIS-DB2-2.2.10	Not supported	Ensure that access to SYSIBM.SYSINDEXES is restricted (Manual)
CIS-DB2-2.2.11	Not supported	Ensure that access to SYSIBM.SYSOBJROLEDEP is restricted
CIS-DB2-2.2.12	Not supported	Ensure that access to package-related tables is restricted
CIS-DB2-2.2.13	Not supported	Ensure that access to SYSIBM.SYSPACKAUTH is restricted
CIS-DB2-2.2.14	Not supported	Ensure that access to SYSIBM.SYSPARMS is restricted
CIS-DB2-2.2.15	Not supported	Ensure that access to SYSIBM.SYSPLAN is restricted
CIS-DB2-2.2.16	Not supported	Ensure that access to SYSIBM.SYSPLANAUTH is restricted
CIS-DB2-2.2.17	Not supported	Ensure that access to SYSIBM.SYSQUERY is restricted
CIS-DB2-2.2.18	Not supported	Ensure that access to SYSIBM.SYSRESAUTH is restricted
CIS-DB2-2.2.19	Not supported	Ensure that access to SYSIBM.SYSROLES is restricted
CIS-DB2-2.2.20	Not supported	Ensure that access to SYSIBM.SYSROUTINEAUTH is restricted
CIS-DB2-2.2.21	Not supported	Ensure that access to SYSIBM.SYSROUTINES is restricted
CIS-DB2-2.2.22	Not supported	Ensure that access to SYSIBM.SYSROUTINESTEXT is restricted
CIS-DB2-2.2.23	Not supported	Ensure that access to SYSIBM.SYSSCHEMAAUTH is restricted
CIS-DB2-2.2.24	Not supported	Ensure that access to SYSIBM.SYSSEQUENCEAUTH is restricted
CIS-DB2-2.2.25	Not supported	Ensure that access to SYSIBM.SYSSEQUENCES is restricted
CIS-DB2-2.2.26	Not supported	Ensure that access to SYSIBM.SYSSTMT is restricted
CIS-DB2-2.2.27	Not supported	Ensure that access to SYSIBM.SYSSTOGROUP is restricted
CIS-DB2-2.2.28	Not supported	Ensure that access to SYSIBM.SYSTABAUTH is restricted
CIS-DB2-2.2.29	Not supported	Ensure that access to SYSIBM.SYSTABLES is restricted
CIS-DB2-2.2.30	Not supported	Ensure that access to SYSIBM.SYSTABLESPACE is restricted
CIS-DB2-2.2.31	Not supported	Ensure that access to SYSIBM.SYSTRIGGERS is restricted
CIS-DB2-2.2.32	Not supported	Ensure that access to SYSIBM.SYSUSERAUTH is restricted
CIS-DB2-2.2.33	Not supported	Ensure that access to variable-related tables is restricted
CIS-DB2-2.2.34	Not supported	Ensure that access to SYSIBM.SYSVARIABLEAUTH is restricted
CIS-DB2-2.2.35	Not supported	Ensure that access to SYSIBM.SYSVIEWS is restricted
CIS-DB2-2.3.1	Not supported	Ensure that access to the program authorization table is restricted
CIS-DB2-2.3.2	Not supported	Ensure that access to the REST services definition table is restricted
CIS-DB2-2.3.3	Not supported	Ensure that access to the query accelerator tables is restricted
CIS-DB2-2.3.4	Not supported	Ensure that access to profile tables is restricted
CIS-DB2-2.3.5	Not supported	Ensure that access to SQL Data Insights tables is restricted

Table 12. CIS IBM Db2 for z/OS Benchmark (Top Secret) (continued)		
CIS Db2 Control ID	**CARLa member**	**Rule Title**
CIS-DB2-2.4.1	Not supported	Secure SYSADM authority access
CIS-DB2-2.4.2	Not supported	Secure SYSCTRL authority access
CIS-DB2-2.4.3	Not supported	Secure SYSOPR authority access
CIS-DB2-2.4.4	Not supported	Secure system DBADM authority access
CIS-DB2-2.4.5	Not supported	Secure DATAACCESS authority access
CIS-DB2-2.4.6	Not supported	Secure ACCESSCTRL authority access
CIS-DB2-2.4.7	Not supported	Secure PACKADM authority access
CIS-DB2-2.4.8	Not supported	Secure SQLADM authority access
CIS-DB2-2.4.9	Not supported	Secure database DBADM authority access
CIS-DB2-2.4.10	Not supported	Secure database DBCTRL authority access
CIS-DB2-2.4.11	Not supported	Secure database DBMAINT authority access
CIS-DB2-2.5.1	C2RHD251	Ensure that data is encrypted at rest and in-flight
CIS-DB2-2.5.2	Not supported	Secure sensitive data in memory
CIS-DB2-2.6.1	C2RHD261	Secure row access using row permit
CIS-DB2-2.6.2	C2RHD262	Secure column values using column mask
CIS-DB2-3.1.1	CKCHD311	Ensure that audit tracing is enabled during Db2 start up
CIS-DB2-3.1.2	CKCHD312	Ensure that critical audit traces are always enabled
CIS-DB2-3.1.3	C2RHD313	Ensure that authorization failures are audited
CIS-DB2-3.1.4	CKCHD314	Enable audit policies to audit installation system administrator and system operator access
CIS-DB2-3.1.5	CKCHD315	Enable auditing of system administrator access
CIS-DB2-3.1.6	CKCHD316	Enable auditing of database administrator access

IBM z/OS TSS STIG

Table 13. IBM z/OS TSS STIG		
STIG ID	**CARLa member**	**Rule Title**
TSS0-CE-000010	Not supported	All IBM z/OS digital certificates in use must have a valid path to a trusted Certification Authority (CA).
TSS0-CE-000020	Not supported	Expired IBM z/OS digital certificates must not be used.
TSS0-CE-000030	Not supported	IBM z/OS must have Certificate Name Filtering implemented with appropriate authorization and documentation.
TSS0-ES-000010	Not supported	CA-TSS Security control ACIDs must be limited to the administrative authorities authorized and that require these privileges to perform their job duties.
TSS0-ES-000020	Not supported	The number of CA-TSS ACIDs possessing the tape Bypass Label Processing (BLP) privilege must be limited.

Table 13. IBM z/OS TSS STIG (continued)

STIG ID	CARLa member	Rule Title
TSS0-ES-000030	Not supported	CA-TSS MODE Control Option must be set to FAIL.
TSS0-ES-000040	Not supported	The CA-TSS NPWRTHRESH Control Option must be properly set.
TSS0-ES-000050	Not supported	The CA-TSS NPPTHRESH Control Option must be properly set.
TSS0-ES-000060	Not supported	The CA-TSS PTHRESH Control Option must be set to 2.
TSS0-ES-000080	Not supported	IBM z/OS must limit access for SMF collection files (that is, SYS1.MANx) to appropriate users and/or batch jobs that perform SMF dump processing.
TSS0-ES-000090	Not supported	IBM z/OS SYS1.PARMLIB must be properly protected.
TSS0-ES-000100	C2RHSH60	IBM z/OS for PKI-based authentication must use the ICSF or ESM for key management.
TSS0-ES-000120	Not supported	The CA-TSS NEWPHRASE and PPSCHAR Control Options must be properly set.
TSS0-ES-000130	Not supported	The CA-TSS NEWPW control options must be properly set.
TSS0-ES-000140	Not supported	IBM z/OS must use NIST FIPS-validated cryptography to protect passwords in the security database.
TSS0-ES-000150	Not supported	The CA-TSS PWEXP Control Option must be set to 60.
TSS0-ES-000160	Not supported	The CA-TSS PPEXP Control Option must be properly set.
TSS0-ES-000170	Not supported	The CA-TSS PWHIST Control Option must be set to 10 or greater.
TSS0-ES-000180	Not supported	The CA-TSS PPHIST Control Option must be properly set.
TSS0-ES-000200	Not supported	CA-TSS access to SYS1.LINKLIB must be properly protected.
TSS0-ES-000210	Not supported	CA-TSS must limit Write or greater access to SYS1.SVCLIB to system programmers only.
TSS0-ES-000220	Not supported	CA-TSS must limit Write or greater access to SYS1.IMAGELIB to system programmers only.
TSS0-ES-000230	Not supported	CA-TSS must limit Write or greater access to SYS1.LPALIB to system programmers only.
TSS0-ES-000240	Not supported	CA-TSS must limit WRITE or greater access to all APF-authorized libraries to system programmers only.
TSS0-ES-000250	Not supported	IBM z/OS libraries included in the system REXXLIB concatenation must be properly protected.
TSS0-ES-000260	Not supported	CA-TSS must limit Write or greater access to all LPA libraries to system programmers only.
TSS0-ES-000270	Not supported	CA-TSS must limit Write or greater access to SYS1.NUCLEUS to system programmers only.
TSS0-ES-000280	Not supported	CA-TSS must limit Write or greater access to libraries that contain PPT modules to system programmers only.
TSS0-ES-000290	Not supported	CA-TSS must limit WRITE or greater access to LINKLIST libraries to system programmers only.
TSS0-ES-000300	Not supported	CA-TSS security data sets and/or databases must be properly protected.

Table 13. IBM z/OS TSS STIG (continued)

STIG ID	CARLa member	Rule Title
TSS0-ES-000310	Not supported	CA-TSS must limit access to the System Master Catalog to appropriate authorized users.
TSS0-ES-000320	Not supported	CA-TSS allocate access to system user catalogs must be limited to system programmers only.
TSS0-ES-000330	Not supported	CA-TSS must limit WRITE or greater access to all system-level product installation libraries to system programmers only.
TSS0-ES-000340	Not supported	CA-TSS must limit WRITE or greater access to the JES2 System data sets (for example, Spool, Checkpoint, and Initialization parameters) to system programmers only.
TSS0-ES-000350	Not supported	CA-TSS must limit Write or greater access to SYS1.UADS to system programmers only, and Read and Update access must be limited to system programmer personnel and/or security personnel.
TSS0-ES-000360	Not supported	CA-TSS must limit access to data sets used to back up and/or dump SMF collection files to appropriate users and/or batch jobs that perform SMF dump processing.
TSS0-ES-000370	Not supported	CA-TSS must limit access to SYSTEM DUMP data sets to system programmers only.
TSS0-ES-000380	Not supported	CA-TSS WRITE or Greater access to System backup files must be limited to system programmers and/or batch jobs that perform DASD backups.
TSS0-ES-000390	Not supported	CA-TSS must limit access to SYS(x).TRACE to system programmers only.
TSS0-ES-000400	Not supported	CA-TSS must limit access to System page data sets (that is, PLPA, COMMON, and LOCALx) to system programmers only.
TSS0-ES-000410	Not supported	CA-TSS must limit WRITE or greater access to libraries containing EXIT modules to system programmers only.
TSS0-ES-000420	Not supported	CA-TSS must limit all system PROCLIB data sets to system programmers only and appropriate authorized users.
TSS0-ES-000430	Not supported	CA-TSS must protect memory and privileged program dumps in accordance with proper security requirements.
TSS0-ES-000440	Not supported	IBM z/OS must protect dynamic lists in accordance with proper security requirements.
TSS0-ES-000450	Not supported	IBM z/OS system commands must be properly protected.
TSS0-ES-000460	Not supported	IBM z/OS MCS consoles access authorization(s) for CONSOLE resource(s) must be properly protected.
TSS0-ES-000470	Not supported	CA-TSS must properly define users that have access to the CONSOLE resource in the TSOAUTH resource class.
TSS0-ES-000480	Not supported	IBM z/OS Operating system commands (MVS.) of the OPERCMDS resource class must be properly owned.
TSS0-ES-000490	Not supported	CA-TSS AUTH Control Option values specified must be set to (OVERRIDE,ALLOVER) or (MERGE,ALLOVER).
TSS0-ES-000500	Not supported	Access to the CA-TSS MODE resource class must be appropriate.

Table 13. IBM z/OS TSS STIG (continued)

STIG ID	CARLa member	Rule Title
TSS0-ES-000505	Not supported	Data set masking characters must be properly defined to the CA-TSS security database.
TSS0-ES-000510	Not supported	CA-TSS Emergency ACIDs must be properly limited and must audit all resource access.
TSS0-ES-000520	Not supported	CA-TSS ACIDs must not have access to FAC(*ALL*).
TSS0-ES-000530	Not supported	The CA-TSS ALL record must have appropriate access to Facility Matrix Tables.
TSS0-ES-000550	Not supported	Data set masking characters allowing access to all data sets must be properly restricted in the CA-TSS security database.
TSS0-ES-000560	Not supported	IBM z/OS DASD Volume access greater than CREATE found in the CA-TSS database must be limited to authorized information technology personnel requiring access to perform their job duties.
TSS0-ES-000570	Not supported	IBM z/OS Sensitive Utility Controls must be properly defined and protected.
TSS0-ES-000580	Not supported	IBM z/OS Started tasks must be properly defined to CA-TSS.
TSS0-ES-000590	Not supported	The CA-TSS CANCEL Control Option must not be specified.
TSS0-ES-000600	Not supported	The CA-TSS HPBPW Control Option must be set to three days maximum.
TSS0-ES-000610	Not supported	The CA-TSS INSTDATA Control Option must be set to 0.
TSS0-ES-000620	Not supported	The CA-TSS OPTIONS Control Option must include option 4 at a minimum.
TSS0-ES-000630	Not supported	CA-TSS TEMPDS Control Option must be set to YES.
TSS0-ES-000640	Not supported	The number of CA-TSS control ACIDs must be justified and properly assigned.
TSS0-ES-000650	Not supported	The number of CA-TSS ACIDs with MISC9 authority must be justified.
TSS0-ES-000660	Not supported	The CA-TSS LUUPDONCE Control Option value specified must be set to NO.
TSS0-ES-000670	Not supported	The CA-TSS Automatic Data Set Protection (ADSP) Control Option must be set to NO.
TSS0-ES-000680	Not supported	CA-TSS RECOVER Control Option must be set to ON.
TSS0-ES-000690	C2RHE680	IBM z/OS must properly configure CONSOLxx members.
TSS0-ES-000700	Not supported	IBM z/OS must properly protect MCS console user ID(s).
TSS0-ES-000710	Not supported	The CA-TSS CPFRCVUND Control Option value specified must be set to NO.
TSS0-ES-000720	Not supported	The CA-TSS CPFTARGET Control Option value specified must be set to LOCAL.
TSS0-ES-000730	Not supported	CA-TSS User ACIDs and Control ACIDs must have the NAME field completed.

Table 13. IBM z/OS TSS STIG (continued)

STIG ID	CARLa member	Rule Title
TSS0-ES-000740	Not supported	The CA-TSS PASSWORD(NOPW) option must not be specified for any ACID type.
TSS0-ES-000750	Not supported	Interactive ACIDs defined to CA-TSS must have the required fields completed.
TSS0-ES-000760	Not supported	Started tasks must be properly defined to CA-TSS.
TSS0-ES-000770	Not supported	CA-TSS Batch ACID(s) submitted through RJE and NJE must be sourced.
TSS0-ES-000780	Not supported	IBM z/OS DASD management ACIDs must be properly defined to CA-TSS.
TSS0-ES-000790	Not supported	CA-TSS user accounts must uniquely identify system users.
TSS0-ES-000800	Not supported	CA-TSS security administrator must develop a process to suspend user IDs found inactive for more than 35 days.
TSS0-ES-000810	Not supported	The CA-TSS INACTIVE Control Option must be properly set.
TSS0-ES-000820	Not supported	The CA-TSS AUTOERASE Control Option must be set to ALL for all systems.
TSS0-ES-000830	Not supported	CA-TSS DOWN Control Option values must be properly specified.
TSS0-ES-000840	Not supported	The CA-TSS Facility Control Option must specify the sub option of MODE=FAIL.
TSS0-ES-000850	Not supported	CA-TSS ACID creation must use the EXP option.
TSS0-ES-000860	Not supported	The CA-TSS SUBACID Control Option must be set to U,8.
TSS0-ES-000870	Not supported	CA-TSS must use propagation control to eliminate ACID inheritance.
TSS0-ES-000880	Not supported	IBM z/OS scheduled production batch ACIDs must specify the CA-TSS BATCH Facility, and the Batch Job Scheduler must be authorized to the Scheduled production CA-TSS batch ACID.
TSS0-ES-000890	Not supported	CA-TSS ADMINBY Control Option must be set to ADMINBY.
TSS0-ES-000900	Not supported	CA-TSS LOG Control Option must be set to (SMF,INIT, SEC9, MSG).
TSS0-ES-000910	Not supported	CA-TSS MSCA ACID password changes must be documented in the change log.
TSS0-ES-000920	Not supported	The IBM z/OS IEASYMUP resource must be protected in accordance with proper security requirements.
TSS0-ES-000930	Not supported	CA-TSS Default ACID must be properly defined.
TSS0-ES-000940	Not supported	The CA-TSS BYPASS attribute must be limited to trusted STCs only.
TSS0-ES-000950	Not supported	CA-TSS MSCA ACID must perform security administration only.
TSS0-ES-000960	Not supported	CA-TSS ACIDs granted the CONSOLE attribute must be justified.
TSS0-ES-000970	Not supported	CA-TSS ACIDs defined as security administrators must have the NOATS attribute.
TSS0-ES-000980	Not supported	The CA-TSS PTHRESH Control Option must be properly set.

Table 13. IBM z/OS TSS STIG (continued)

STIG ID	CARLa member	Rule Title
TSS0-ES-000990	Not supported	CA-TSS VTHRESH Control Option values specified must be set to (10,NOT,CAN).
TSS0-FT-000010	C2RHF040	IBM z/OS FTP.DATA configuration statements must have a proper banner statement with the Standard Mandatory Department of Defense (DoD) Notice and Consent Banner.
TSS0-FT-000020	C2RHF010	IBM z/OS SMF recording options for the FTP server must be configured to write SMF records for all eligible events.
TSS0-FT-000030	C2RHF020	CA-TSS permission bits and user audit bits for HFS objects that are part of the FTP server component must be properly configured.
TSS0-FT-000040	Not supported	IBM z/OS data sets for the FTP server must be properly protected.
TSS0-FT-000050	Not supported	IBM z/OS FTP Control cards must be properly stored in a secure PDS file.
TSS0-FT-000060	C2RHF090	IBM z/OS user exits for the FTP server must not be used without proper approval and documentation.
TSS0-FT-000070	Not supported	The IBM z/OS FTP server daemon must be defined with proper security parameters.
TSS0-FT-000080	Not supported	IBM z/OS FTP.DATA configuration for the FTP server must have the INACTIVE statement properly set.
TSS0-FT-000090	C2RHF120	IBM z/OS startup parameters for the FTP server must have the INACTIVE statement properly set.
TSS0-FT-000100	C2RHF050	IBM z/OS FTP.DATA configuration statements for the FTP server must specify the Standard Mandatory DoD Notice and Consent Banner statement.
TSS0-FT-000120	Not supported	The IBM z/OS TFTP server program must be properly protected.
TSS0-FT-000130	C2RHF070	IBM z/OS FTP.DATA configuration statements for the FTP Server must be specified in accordance with requirements
TSS0-IC-000010	C2RHIC10	IBM Integrated Crypto Service Facility (ICSF) Configuration parameters must be correctly specified.
TSS0-IC-000020	Not supported	IBM Integrated Crypto Service Facility (ICSF) install data sets are not properly protected.
TSS0-IC-000030	Not supported	IBM Integrated Crypto Service Facility (ICSF) STC data sets must be properly protected.
TSS0-IC-000040	Not supported	IBM Integrated Crypto Service Facility (ICSF) Started Task name is not properly identified / defined to the system ACP.
TSS0-IC-000050	Not supported	IBM Integrated Crypto Service Facility (ICSF) Started task(s) must be properly defined to the Started Task Table ACID for Top Secret.
TSS0-IC-000060	Not supported	ICSF resource class(es) must be properly owned in accordance with security requirements.
TSS0-IC-000070	Not supported	ICSF resources must be protected in accordance with security requirements.
TSS0-JS-000010	Not supported	IBM z/OS JES2.** resource must be properly protected in the CA-TSS database.

Table 13. IBM z/OS TSS STIG (continued)

STIG ID	CARLa member	Rule Title
TSS0-JS-000020	Not supported	IBM z/OS RJE workstations and NJE nodes must be controlled in accordance with STIG requirements.
TSS0-JS-000030	Not supported	IBM z/OS JES2 input sources must be controlled in accordance with the proper security requirements.
TSS0-JS-000040	Not supported	IBM z/OS JES2 input sources must be properly controlled.
TSS0-JS-000050	Not supported	IBM z/OS JES2 output devices must be controlled in accordance with the proper security requirements.
TSS0-JS-000060	Not supported	IBM z/OS JES2 output devices must be properly controlled for classified systems.
TSS0-JS-000070	Not supported	IBM z/OS JESSPOOL resources must be protected in accordance with security requirements.
TSS0-JS-000080	Not supported	IBM z/OS JESNEWS resources must be protected in accordance with security requirements.
TSS0-JS-000090	Not supported	IBM z/OS JESTRACE and/or SYSLOG resources must be protected in accordance with security requirements.
TSS0-JS-000100	Not supported	IBM z/OS JES2 spool resources must be controlled in accordance with security requirements.
TSS0-JS-000110	Not supported	IBM z/OS JES2 system commands must be protected in accordance with security requirements.
TSS0-JS-000120	Not supported	IBM z/OS Surrogate users must be controlled in accordance with proper security requirements.
TSS0-OS-000010	C2RHO310	Duplicated IBM z/OS sensitive utilities and/or programs must not exist in APF libraries.
TSS0-OS-000020	C2RHO110	IBM z/OS required SMF data record types must be collected.
TSS0-OS-000030	C2RHO410	IBM z/OS Session manager must properly configure wait time limits.
TSS0-OS-000040	Not supported	The IBM z/OS BPX.SMF resource must be properly configured.
TSS0-OS-000050	C2RHO130	IBM z/OS must specify SMF data options to ensure appropriate activation.
TSS0-OS-000060	C2RHO160	IBM z/OS BUFUSEWARN in the SMFPRMxx must be properly set.
TSS0-OS-000070	C2RHO220	IBM z/OS PASSWORD data set and OS passwords must not be used.
TSS0-OS-000080	Not supported	The CA-TSS database must be on a separate physical volume from its backup and recovery data sets.
TSS0-OS-000090	Not supported	The CA-TSS database must be backed up on a scheduled basis.
TSS0-OS-000100	C2RHO240	IBM z/OS Policy Agent must be configured to deny-all, allow-by-exception firewall policy for allowing connections to other systems.
TSS0-OS-000110	C2RHO280	IBM z/OS must not have Inaccessible APF libraries defined.
TSS0-OS-000120	C2RHO290	IBM z/OS inapplicable PPT entries must be invalidated.

Table 13. IBM z/OS TSS STIG (continued)

STIG ID	CARLa member	Rule Title
TSS0-OS-000130	C2RHO300	IBM z/OS LNKAUTH=APFTAB must be specified in the IEASYSxx member(s) in the currently active parmlib data set(s).
TSS0-OS-000140	C2RHO350	IBM z/OS sensitive and critical system data sets must not exist on shared DASD.
TSS0-OS-000150	C2RHO370	IBM z/OS Policy Agent must contain a policy that manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of Denial of Service (DoS) attacks.
TSS0-OS-000170	C2RHO060	The IBM z/OS System Administrator must develop a process to notify appropriate personnel when accounts are created.
TSS0-OS-000180	C2RHO070	The IBM z/OS System Administrator must develop a process to notify appropriate personnel when accounts are modified.
TSS0-OS-000190	C2RHO080	The IBM z/OS System Administrator must develop a process to notify appropriate personnel when accounts are deleted.
TSS0-OS-000200	C2RHO090	The IBM z/OS System Administrator must develop a process to notify appropriate personnel when accounts are removed.
TSS0-OS-000210	C2RHO250	Unsupported IBM z/OS system software must not be installed and/or active on the system.
TSS0-OS-000220	C2RHO270	IBM z/OS must not allow nonexistent or inaccessible Link Pack Area (LPA) libraries.
TSS0-OS-000225	C2RHO260	IBM z/OS must not allow nonexistent or inaccessible LINKLIST libraries.
TSS0-OS-000230	Not supported	CA-TSS must be installed and properly configured.
TSS0-OS-000240	C2RHO140	IBM z/OS SMF collection files (system MANx data sets or LOGSTREAM DASD) must have storage capacity to store at least one week audit data.
TSS0-OS-000250	C2RHO150	IBM z/OS System Administrators must develop an automated process to collect and retain SMF data.
TSS0-OS-000270	C2RHO180	The IBM z/OS SNTP daemon (SNTPD) must be active.
TSS0-OS-000280	C2RHO190	IBM z/OS SNTP daemon (SNTPD) permission bits must be properly configured.
TSS0-OS-000290	C2RHO200	IBM z/OS PARMLIB CLOCKxx must have the Accuracy PARM coded properly.
TSS0-OS-000300	C2RHO360	The IBM z/OS Policy Agent must contain a policy that protects against or limits the effects of Denial of Service (DoS) attacks by ensuring IBM z/OS is implementing rate-limiting measures on impacted network interfaces.
TSS0-OS-000320	C2RHO320	The IBM z/OS systems requiring data-at-rest protection must properly employ IBM DS8880 or equivalent hardware solutions for full disk encryption.
TSS0-OS-000330	Not supported	IBM z/OS must employ a session manager to manage retaining a users session lock until that user reestablishes access using established identification and authentication procedures.

Table 13. IBM z/OS TSS STIG (continued)

STIG ID	CARLa member	Rule Title
TSS0-OS-000350	C2RHO010	IBM z/OS must configure system wait times to protect resource availability based on site priorities.
TSS0-OS-000360	C2RHO400	IBM z/OS must employ a session manager to conceal, via the session lock, information previously visible on the display with a publicly viewable image.
TSS0-OS-000380	C2RHO430	IBM z/OS must employ a session manager to manage retaining a users session lock until that user reestablishes access using established identification and authentication procedures.
TSS0-OS-000390	C2RHO440	IBM z/OS system administrator must develop a procedure to remove or disable temporary user accounts after 72 hours.
TSS0-OS-000400	C2RHO450	IBM z/OS system administrator must develop a procedure to remove or disable emergency accounts after the crisis is resolved or 72 hours.
TSS0-OS-000410	Not supported	IBM z/OS system administrator must develop a procedure to notify System Administrators and ISSOs of account enabling actions.
TSS0-OS-000420	C2RHO460	IBM z/OS system administrator must develop a procedure to notify designated personnel if baseline configurations are changed in an unauthorized manner.
TSS0-OS-000440	C2RHO480	IBM z/OS system administrator must develop a procedure to terminate all sessions and network connections related to non-local maintenance when non-local maintenance is completed. Removed starting with z/OS TSS STIG version 9.1.
TSS0-OS-000450	C2RHO490	IBM z/OS system administrator must develop a procedure to remove all software components after updated versions have been installed.
TSS0-OS-000460	C2RHO500	IBM z/OS system administrator must develop a procedure to shut down the information system, restart the information system, and/or notify the system administrator when anomalies in the operation of any security functions are discovered.
TSS0-OS-000470	C2RHO510	IBM z/OS system administrator must develop a procedure to offload SMF files to a different system or media than the system being audited.
TSS0-OS-000480	C2RHO420	IBM z/OS must employ a session manager for users to directly initiate a session lock for all connection types.
TSS0-SH-000020	C2RHSH20	The SSH daemon must be configured to use a FIPS 140-2 compliant cryptographic algorithm.
TSS0-SH-000030	C2RHSH50	IBM z/OS SSH daemon must be configured to only use the SSHv2 protocol.
TSS0-SL-000010	Not supported	IBM z/OS permission bits and user audit bits for HFS objects that are part of the Syslog daemon component must be configured properly.
TSS0-SL-000020	C2RHSL20	The IBM z/OS Syslog daemon must not be started at z/OS initialization.

Table 13. IBM z/OS TSS STIG (continued)

STIG ID	CARLa member	Rule Title
TSS0-SL-000030	Not supported	The IBM z/OS Syslog daemon must be properly defined and secured.
TSS0-SM-000010	Not supported	IBM z/OS DFSMS resources must be protected in accordance with the proper security requirements.
TSS0-SM-000020	Not supported	IBM z/OS DFSMS Program Resources must be properly defined and protected.
TSS0-SM-000030	Not supported	IBM z/OS DFSMS control data sets must be protected in accordance with security requirements.
TSS0-SM-000040	C2RHSM50	IBM z/OS using DFSMS must properly specify SYS(x).PARMLIB(IGDSMSxx), SMS parameter settings.
TSS0-SM-000050	C2RHSM60	IBM z/OS DFSMS control data sets must reside on separate volumes.
TSS0-SS-000010	C2RHO030	IBM z/OS SMF recording options for the SSH daemon must be configured to write SMF records for all eligible events.
TSS0-SS-000040	C2RHSH40	The IBM z/OS SSH daemon must be configured with the Standard Mandatory DoD Notice and Consent Banner.
TSS0-TC-000010	C2RHT010	IBM z/OS PROFILE.TCPIP configuration statements for the TCP/IP stack must be properly coded.
TSS0-TC-000020	C2RHT030	IBM z/OS permission bits and user audit bits for HFS objects that are part of the Base TCP/IP component must be configured properly.
TSS0-TC-000030	Not supported	IBM z/OS TCP/IP resources must be properly protected.
TSS0-TC-000040	Not supported	IBM z/OS data sets for the Base TCP/IP component must be properly protected.
TSS0-TC-000050	C2RHT080	IBM z/OS Configuration files for the TCP/IP stack must be properly specified.
TSS0-TC-000060	Not supported	IBM z/OS started tasks for the Base TCP/IP component must be defined in accordance with security requirements.
TSS0-TC-000070	Not supported	IBM z//OS must be configured to restrict all TCP/IP ports to ports, protocols, and/or services as defined in the PPSM CAL and vulnerability assessments.
TSS0-TC-000080	C2RHT100	The IBM z/OS TCPIP.DATA configuration statement must contain the DOMAINORIGIN or DOMAIN specified for each TCP/IP defined.
TSS0-TC-000100	Not supported	IBM z/OS TCP/IP AT-TLS policy must be properly configured in Policy Agent.
TSS0-TN-000010	C2RHTN40	IBM z/OS TN3270 Telnet server configuration statement MSG10 text must have the Standard Mandatory DoD Notice and Consent Banner.
TSS0-TN-000020	Not supported	IBM z/OS SMF recording options for the TN3270 Telnet server must be properly specified.
TSS0-TN-000030	C2RHTN20	IBM z/OS SSL encryption options for the TN3270 Telnet server must be specified properly for each statement that defines a SECUREPORT or within the TELNETGLOBALS.

Table 13. IBM z/OS TSS STIG (continued)

STIG ID	CARLa member	Rule Title
TSS0-TN-000040	C2RHTN50	IBM z/OS VTAM session setup controls for the TN3270 Telnet server must be properly specified.
TSS0-TN-000050	C2RHTN60	IBM z/OS PROFILE.TCPIP configuration for the TN3270 Telnet server must have the INACTIVE statement properly specified.
TSS0-TN-000060	C2RHTN40	The IBM z/OS warning banner for the TN3270 Telnet server must be properly specified. Removed from z/OS RACF STIG version 8.13.
TSS0-TS-000010	Not supported	IBM Z/OS TSOAUTH resources must be restricted to authorized users.
TSS0-TS-000020	C2RHTS20	CA-TSS logonids must not be defined to SYS1.UADS for non-emergency use.
TSS0-US-000010	C2RHU170	IBM z/OS UNIX HFS MapName file security parameters must be properly specified.
TSS0-US-000020	C2RHO170	IBM z/OS NOBUFFS in SMFPRMxx must be properly set (default is MSG).
TSS0-US-000030	Not supported	IBM z/OS BPX resource(s) must be protected in accordance with security requirements.
TSS0-US-000040	Not supported	IBM z/OS UNIX resources must be protected in accordance with security requirements.
TSS0-US-000050	Not supported	IBM z/OS UNIX SUPERUSER resources must be protected in accordance with guidelines.
TSS0-US-000060	Not supported	IBM z/OS UNIX MVS data sets or HFS objects must be properly protected.
TSS0-US-000070	Not supported	IBM z/OS UNIX MVS data sets with z/OS UNIX components must be properly protected.
TSS0-US-000080	Not supported	IBM z/OS UNIX MVS data sets used as step libraries in /etc/steplib must be properly protected.
TSS0-US-000090	C2RHU100	IBM z/OS UNIX HFS permission bits and audit bits for each directory must be properly protected.
TSS0-US-000100	C2RHU110	IBM z/OS UNIX system file security settings must be properly protected or specified.
TSS0-US-000110	C2RHU030	IBM z/OS UNIX MVS HFS directory(s) with OTHER write permission bit set must be properly defined.
TSS0-US-000120	Not supported	The CA-TSS HFSSEC resource class must be defined with DEFPROT.
TSS0-US-000130	C2RHU140	IBM z/OS UNIX OMVS parameters in PARMLIB must be properly specified.
TSS0-US-000140	C2RHU150	IBM z/OS UNIX BPXPRMxx security parameters in PARMLIB must be properly specified.
TSS0-US-000150	C2RHU050	IBM z/OS UNIX security parameters in etc/profile must be properly specified.
TSS0-US-000160	C2RHU060	IBM z/OS UNIX security parameters in /etc/rc must be properly specified.

Table 13. IBM z/OS TSS STIG (continued)		
STIG ID	**CARLa member**	**Rule Title**
TSS0-US-000170	Not supported	IBM z/OS Default profiles must not be defined in TSS OMVS UNIX security parameters for classified systems.
TSS0-US-000180	C2RHU180	IBM z/OS UNIX security parameters for restricted network service(s) in /etc/inetd.conf must be properly specified.
TSS0-US-000190	Not supported	IBM z/OS attributes of z/OS UNIX user accounts must have a unique GID in the range of 1-99.
TSS0-US-000200	Not supported	The IBM z/OS user account for the UNIX kernel (OMVS) must be properly defined to the security database.
TSS0-US-000210	Not supported	The IBM z/OS user account for the z/OS UNIX SUPERUSER user ID must be properly defined.
TSS0-US-000220	Not supported	The IBM z/OS user account for the UNIX (RMFGAT) must be properly defined.
TSS0-US-000230	Not supported	IBM z/OS UID(0) must be properly assigned.
TSS0-US-000240	Not supported	IBM z/OS UNIX user accounts must be properly defined.
TSS0-US-000250	Not supported	IBM z/OS attributes of UNIX user accounts used for account modeling must be defined in accordance with security requirements.
TSS0-UT-000010	C2RHUT30	The IBM z/OS UNIX Telnet server etc/banner file must have the Standard Mandatory DoD Notice and Consent Banner.
TSS0-UT-000020	Not supported	The IBM z/OS startup user account for the z/OS UNIX Telnet server must be properly defined.
TSS0-UT-000030	C2RHUT20	IBM z/OS HFS objects for the z/OS UNIX Telnet server must be properly protected.
TSS0-UT-000040	C2RHUT40	The IBM z/OS UNIX Telnet server Startup parameters must be properly specified.
TSS0-UT-000050	C2RHUT50	The IBM z/OS UNIX Telnet server warning banner must be properly specified.
TSS0-VT-000010	Not supported	IBM z/OS System data sets used to support the VTAM network must be properly secured.
TSS0-VT-000020	C2RHVT20	IBM z/OS VTAM USSTAB definitions must not be used for unsecured terminals.
TSS0-ZO-000010	Not supported	z/OSMF resource class(es) must be active in accordance with security requirements.
TSS0-ZO-000020	Not supported	z/OSMF resources must be protected in accordance with security requirements.

IBM z/OS TSS Products STIG

Table 14. IBM z/OS TSS Products STIG		
STIG ID	**CARLa member**	**Rule Title**
ZADTT000	Not supported	CA Auditor installation data sets are not properly protected.

Table 14. IBM z/OS TSS Products STIG (continued)		
STIG ID	**CARLa member**	**Rule Title**
ZADTT002	Not supported	CA Auditor User data sets are not properly protected.
ZADTT020	Not supported	CA Auditor resources are not properly defined and protected.
ZAID0040	C2RHAA40	Compuware Abend-AID external security options must be specified properly.
ZAIDT000	Not supported	Compuware Abend-AID installation data sets will be properly protected.
ZAIDT001	Not supported	Compuware Abend-AID STC data sets will be properly protected.
ZAIDT002	Not supported	Compuware Abend-AID user data sets must be properly protected.
ZAIDT020	Not supported	Compuware Abend-AID resources must be properly defined and protected.
ZAIDT030	Not supported	Compuware Abend-AID Started Task name will be properly identified and/or defined to the system ACP.
ZAIDT032	Not supported	Compuware Abend-AID Started task will be properly defined to the Started Task Table for Top Secret.
ZCA10041	C2RHTM41	CA 1 Tape Management system password will be changed from the default.
ZCA10060	C2RHTM60	CA 1 Tape Management user exits, when in use, must be reviewed and/or approved.
ZCA1T000	Not supported	CA 1 Tape Management installation data sets must be properly protected.
ZCA1T001	Not supported	CA-1 Tape Management STC data sets must be properly protected.
ZCA1T003	Not supported	CA 1 Tape Management TMC, AUDIT and optional RDS and VPD data sets will be properly protected.
ZCA1T020	Not supported	CA 1 Tape Management command resources must be properly defined and protected.
ZCA1T021	Not supported	CA 1 Tape Management function and password resources must be properly defined and protected.
ZCA1T030	Not supported	CA 1 Tape Management Started Task name will be properly identified and/or defined to the system ACP.
ZCA1T032	Not supported	CA 1 Tape Management Started task will be properly defined to the Started Task Table ACID for Top Secret.
ZCA1T036	Not supported	CA 1 Tape Management will be properly defined to the Facility Matrix Table.
ZCA1T040	CKTHTM40	CA 1 Tape Management external security options must be specified properly.
ZCCST000	Not supported	CA Common Services installation data sets will be properly protected.
ZCCST032	Not supported	CA Common Services Started task will be properly defined to the Started Task Table ACID for Top Secret.
ZCIC0010	Not supported	CICS system data sets are not properly protected.

Table 14. IBM z/OS TSS Products STIG (continued)		
STIG ID	**CARLa member**	**Rule Title**
ZCIC0020	Not supported	Sensitive CICS transactions are not protected in accordance with security requirements.
ZCIC0030	C2RHCI30	CICS System Initialization Table (SIT) parameter values must be specified in accordance with proper security requirements.
ZCIC0040	Not supported	CICS region logonid(s) must be defined and/or controlled in accordance with the security requirements.
ZCIC0041	Not supported	CICS default logonid(s) must be defined and/or controlled in accordance with the security requirements.
ZCIC0042	Not supported	CICS logonid(s) must be configured with proper timeout and sign on limits.
ZCICT021	Not supported	IBM CICS Transaction Server SPI command resources must be properly defined and protected.
ZCICT041	Not supported	CICS user ids are not defined and/or controlled in accordance with proper security requirements.
ZCICT050	Not supported	Control options for the Top Secret CICS facilities must meet minimum requirements.
ZCLS0040	C2RHSS40	CL/SuperSession profile options are set improperly.
ZCLS0041	C2RHSS41	CL/SuperSession is not properly configured to generate SMF records for audit trail and accounting reports.
ZCLST000	Not supported	CL/SuperSession Install data sets must be properly protected.
ZCLST001	Not supported	CL/SuperSession STC data sets must be properly protected.
ZCLST030	Not supported	CL/SuperSession Started Task name is not properly identified / defined to the system ACP.
ZCLST032	Not supported	CL/SuperSession Started task(s) must be properly defined to the Started Task Table ACID for Top Secret.
ZCLST036	Not supported	CL/SuperSession is not properly defined to the Facility Matrix Table for Top Secret.
ZCLST038	Not supported	CL/SuperSession's Resource Class is not defined or active in the ACP.
ZCLST042	Not supported	CL/SuperSession KLVINNAM member must be configured in accordance to security requirements.
ZCLST043	CKTHSS43	CL/SuperSession APPCLASS member is not configured in accordance with the proper security requirements.
ZCSLT000	Not supported	Catalog Solution Install data sets are not properly protected.
ZCSLT020	Not supported	Catalog Solutions resources must be properly defined and protected.
ZCTD0040	C2RHCD40	BMC CONTROL-D configuration/parameter values are not specified properly.
ZCTD0060	C2RHCD60	BMC CONTROL-D security exits are not installed or configured properly.
ZCTDT000	Not supported	BMC CONTROL-D installation data sets will be properly protected.

Table 14. IBM z/OS TSS Products STIG (continued)		
STIG ID	**CARLa member**	**Rule Title**
ZCTDT001	Not supported	BMC CONTROL-D STC data sets must be properly protected.
ZCTDT002	Not supported	BMC CONTROL-D user data sets must be properly protected.
ZCTDT020	Not supported	BMC CONTROL-D resources must be properly defined and protected.
ZCTDT030	Not supported	BMC CONTROL-D Started Task name is not properly identified / defined to the system ACP.
ZCTDT032	Not supported	BMC CONTROL-D Started task(s) must be properly defined to the Started Task Table ACID for Top Secret.
ZCTDT036	Not supported	BMC CONTROL-D is not properly defined to the Facility Matrix Table for Top Secret.
ZCTM0060	C2RHCM60	BMC CONTROL-M security exits are not installed or configured properly.
ZCTMT000	Not supported	BMC CONTROL-M installation data sets will be properly protected.
ZCTMT001	Not supported	BMC CONTROL-M STC data sets will be properly protected.
ZCTMT002	Not supported	BMC CONTROL-M User data sets will be properly protected.
ZCTMT003	Not supported	BMC CONTROL-M User/Application JCL data sets must be properly protected.
ZCTMT020	Not supported	BMC C0NTROL-M resources must be properly defined and protected.
ZCTMT030	Not supported	BMC CONTROL-M Started Task name is not properly identified / defined to the system ACP.
ZCTMT032	Not supported	BMC CONTROL-M Started task(s) must be properly defined to the Started Task Table ACID for Top Secret.
ZCTMT036	Not supported	BMC CONTROL-M is not properly defined to the Facility Matrix Table for Top Secret.
ZCTMT040	CKTHCM40	BMC CONTROL-M configuration/parameter values must be specified properly.
ZCTO0040	C2RHCO40	BMC CONTROL-O configuration/parameter values are not specified properly.
ZCTO0041	C2RHCO41	BMC CONTROL-O configuration/parameter values are not specified properly.
ZCTO0060	C2RHCO60	BMC CONTROL-O security exits are not installed or configured properly.
ZCTOT000	Not supported	BMC CONTROL-O installation data sets will be properly protected.
ZCTOT001	Not supported	BMC CONTROL-O STC data sets must be properly protected.
ZCTOT020	Not supported	BMC CONTROL-O resources must be properly defined and protected.
ZCTOT030	Not supported	BMC CONTROL-O Started Task name is not properly identified / defined to the system ACP.

Table 14. IBM z/OS TSS Products STIG (continued)		
STIG ID	**CARLa member**	**Rule Title**
ZCTOT032	Not supported	BMC CONTROL-O Started task(s) must be properly defined to the Started Task Table ACID for Top Secret.
ZCTOT036	Not supported	BMC CONTROL-O is not properly defined to the Facility Matrix Table for Top Secret.
ZCTRT000	Not supported	BMC CONTROL-M/Restart installation data sets will be properly protected.
ZCTRT002	Not supported	BMC CONTROL-M/Restart Archived Sysout data sets must be properly protected.
ZFDR0040	C2RHFD40	FDR (Fast Dump Restore) security options are improperly specified.
ZFDRT000	Not supported	Fast Dump Restore (FDR) install data sets are not properly protected.
ZFEP0011	C2RHFE11	All hardware components of the FEPs are not placed in secure locations where they cannot be stolen, damaged, or disturbed
ZFEP0013	C2RHFE13	A documented procedure is not available instructing how to load and dump the FEP NCP (Network Control Program).
ZFEP0014	C2RHFE14	An active log is not available to keep track of all hardware upgrades and software changes made to the FEP (Front End Processor).
ZFEP0015	Not supported	NCP (Net Work Control Program) Data set access authorization does not restricts UPDATE and/or ALLOCATE access to appropriate personnel.
ZFEP0016	C2RHFE16	A password control is not in place to restrict access to the service subsystem via the operator consoles (local and/or remote) and a key-lock switch is not used to protect the modem supporting the remote console of the service subsystem.
ZHCDT000	Not supported	IBM Hardware Configuration Definition (HCD) install data sets are not properly protected.
ZHCDT002	Not supported	IBM Hardware Configuration Definition (HCD) User data sets are not properly protected.
ZHCDT020	Not supported	IBM Hardware Configuration Definition (HCD) resources are not properly defined and protected.
ZHCKT001	Not supported	IBM Health Checker STC data sets will be properly protected.
ZHCKT030	Not supported	IBM Health Checker Started Task name will be properly identified and/or defined to the system ACP.
ZHCKT032	Not supported	IBM Health Checker Started task will be properly defined to the Started Task Table for Top Secret.
ZIOA0060	C2RHOA60	BMC IOA security exits are not installed or configured properly.
ZIOAT000	Not supported	BMC IOA installation data sets will be properly protected.
ZIOAT001	Not supported	BMC IOA STC data sets must be properly protected.
ZIOAT002	Not supported	BMC IOA User data sets will be properly protected.
ZIOAT020	Not supported	BMC IOA resources must be properly defined and protected.

Table 14. IBM z/OS TSS Products STIG (continued)

STIG ID	CARLa member	Rule Title
ZIOAT030	Not supported	BMC IOA Started Task name must be properly identified and defined to the system ACP.
ZIOAT032	Not supported	BMC IOA Started task(s) must be properly defined to the Started Task Table ACID for Top Secret.
ZIOAT036	Not supported	BMC IOA is not properly defined to the Facility Matrix Table for Top Secret.
ZIOAT040	Not supported	BMC IOA configuration/parameter values are not specified properly.
ZISF0040	C2RHSF40	IBM System Display and Search Facility (SDSF) Configuration parameters must be correctly specified.
ZISFT000	Not supported	IBM System Display and Search Facility (SDSF) installation data sets will be properly protected.
ZISFT002	Not supported	IBM System Display and Search Facility (SDSF) HASPINDX data set identified in the INDEX parameter must be properly protected.
ZISFT020	Not supported	IBM System Display and Search Facility (SDSF) resources will be properly defined and protected.
ZISFT021	Not supported	IBM System Display and Search Facility (SDSF) resources will be properly defined and protected.
ZISFT030	Not supported	IBM System Display and Search Facility (SDSF) Started Task name will be properly identified and/or defined to the system ACP.
ZISFT032	Not supported	IBM System Display and Search Facility (SDSF) Started task will be properly defined to the Started Task Table ACID for Top Secret.
ZMICT000	Not supported	CA MICS Resource Management User data sets must be properly protected.
ZMICT002	Not supported	CA MICS Resource Management User data sets must be properly protected.
ZMIM0040	C2RHMI40	CA MIM Resource Sharing external security options must be specified properly.
ZMIMT000	Not supported	CA MIM Resource Sharing installation data sets will be properly protected.
ZMIMT001	Not supported	CA MIM Resource Sharing STC data sets will be properly protected.
ZMIMT020	Not supported	CA MIM Resource Sharing resources will be properly defined and protected.
ZMIMT030	Not supported	CA MIM Resource Sharing Started Task name will be properly identified and/or defined to the system ACP.
ZMIMT032	Not supported	CA MIM Resource Sharing Started task will be properly defined to the Started Task Table for Top Secret.
ZMVZT000	Not supported	BMC MAINVIEW for z/OS installation data sets are not properly protected.
ZMVZT001	Not supported	BMC MAINVIEW for z/OS STC data sets are not properly protected.
ZMVZT020	Not supported	BMC MAINVIEW resources must be properly defined and protected.

Table 14. IBM z/OS TSS Products STIG (continued)		
STIG ID	**CARLa member**	**Rule Title**
ZMVZT030	Not supported	BMC Mainview for z/OS Started Task name is not properly identified and/or defined to the system ACP.
ZMVZT032	Not supported	BMC Mainview for z/OS Started task(s) must be properly defined to the Started Task Table ACID for Top Secret.
ZMVZT036	Not supported	BMC Mainview for z/OS is not properly defined to the Facility Matrix Table for Top Secret.
ZMVZT038	Not supported	BMC Mainview for z/OS Resource Class must be defined or active in the ACP.
ZMVZT040	Not supported	BMC MAINVIEW for z/OS configuration/parameter values are not specified properly.
ZNCPT000	Not supported	Quest NC-Pass installation data sets will be properly protected.
ZNCPT001	Not supported	Quest NC-Pass STC data sets will be properly protected.
ZNCPT020	Not supported	Quest NC-Pass will be used by Highly-Sensitive users.
ZNCPT030	Not supported	Quest NC-Pass Started Task name will be properly identified and/or defined to the system ACP.
ZNCPT032	Not supported	Quest NC-Pass Started task will be properly defined to the Started Task Table ACID for Top Secret.
ZNCPT036	Not supported	Quest NC-Pass will be properly defined to the Facility Matrix Table.
ZNET0040	C2RHNV40	NetView configuration/parameter values must be specified properly.
ZNETT000	Not supported	NetView install data sets are not properly protected.
ZNETT001	Not supported	NetView STC data sets are not properly protected.
ZNETT020	Not supported	NetView resources must be properly defined and protected.
ZNETT030	Not supported	NetView Started Task name(s) is not properly identified / defined to the system ACP.
ZNETT032	Not supported	IBM Z NetView Started task(s) must be properly defined to the Started Task Table ACID for Top Secret.
ZNETT036	Not supported	NetView is not properly defined to the Facility Matrix Table for Top Secret.
ZROST000	Not supported	ROSCOE Install data sets are not properly protected.
ZROST001	Not supported	ROSCOE STC data sets are not properly protected.
ZROST020	Not supported	ROSCOE resources must be properly defined and protected.
ZROST030	Not supported	ROSCOE Started Task name is not properly identified / defined to the system ACP.
ZROST032	Not supported	ROSCOE Started task(s) must be properly defined to the Started Task Table ACID for Top Secret.
ZROST036	Not supported	ROSCOE is not properly defined to the Facility Matrix Table for Top Secret.
ZROST038	Not supported	Resource Class ROSRES is not defined or active in the ACP.

Table 14. IBM z/OS TSS Products STIG (continued)

STIG ID	CARLa member	Rule Title
ZROST040	Not supported	ROSCOE configuration/parameter values are not specified properly.
ZSMTT001	Not supported	IBM Communications Server Simple Mail Transfer Protocol (CSSMTP) STC data sets must be properly protected.
ZSMTT030	Not supported	IBM CSSMTP Started Task name is not properly identified and/or defined to the system ACP.
ZSMTT032	Not supported	IBM CSSMTP Started task(s) must be properly defined to the Started Task Table ACID for Top Secret.
ZSRRT000	Not supported	SRRAUDIT installation data sets must be properly protected.
ZSRRT002	Not supported	SRRAUDIT User data sets are not properly protected.
ZTADT000	Not supported	Tivoli Asset Discovery for z/OS (TADz) Install data sets are not properly protected.
ZTADT001	Not supported	Tivoli Asset Discovery for z/OS (TADz) STC and/or batch data sets are not properly protected.
ZTADT030	Not supported	Tivoli Asset Discovery for z/OS (TADz) Started Task name(s) must be properly identified / defined to the system ACP.
ZTADT032	Not supported	IBM Tivoli Asset Discovery for z/OS (TADz) Started task(s) must be properly defined to the Started Task Table ACID for Top Secret.
ZTDM0040	C2RHDM40	Transparent Data Migration Facility (TDMF) configuration/ parameter/option values are not specified properly.
ZTDMT000	Not supported	Transparent Data Migration Facility (TDMF) installation data sets will be not properly protected.
ZVTAT000	Not supported	CA VTAPE installation data sets are not properly protected.
ZVTAT001	Not supported	CA VTAPE STC data sets will be properly protected.
ZVTAT030	Not supported	CA VTAPE Started Task name is not properly identified/defined to the system ACP.
ZVTAT032	Not supported	CA VTAPE Started task(s) must be properly defined to the Started Task Table ACID for Top Secret.
ZWAS0010	Not supported	MVS data sets for the WebSphere Application Server are not protected in accordance with the proper security requirements.
ZWAS0020	C2RHWS20	HFS objects for the WebSphere Application Server are not protected in accordance with the proper security requirements.
ZWAS0030	Not supported	The CBIND Resource(s) for the WebSphere Application Server is(are) not protected in accordance with security requirements.
ZWAS0040	C2RHWS40	Vendor-supplied user accounts for the WebSphere Application Server must be defined to the ACP.
ZWAS0050	C2RHWS50	The WebSphere Application Server plug-in is not specified in accordance with the proper security requirements.
ZWMQ0011	C2RHWM11	IBM MQ for z/OS channel security must be implemented in accordance with security requirements.
ZWMQ0012	C2RHWM12	IBM MQ for z/OS channel security must be implemented in accordance with security requirements.

Table 14. IBM z/OS TSS Products STIG (continued)		
STIG ID	**CARLa member**	**Rule Title**
ZWMQ0014	C2RHWM14	Production IBM MQ for z/OS remote subsystems must utilize Certified Name Filters (CNF).
ZWMQ0020	C2RHWM20	User timeout parameter values for IBM MQ for z/OS queue managers must be specified in accordance with security requirements.
ZWMQ0030	Not supported	IBM MQ for z/OS started tasks must be defined in accordance with the proper security requirements.
ZWMQ0040	Not supported	IBM MQ for z/OS all WRITE and ALLOCATE access to MQSeries/ WebSphere MQ product and system data sets must be properly restricted.
ZWMQ0049	Not supported	IBM MQ for z/OS resource classes must be active.
ZWMQ0051	C2RHWM51	IBM MQ for z/OS switch profiles must be properly defined to the appropriate ADMIN class.
ZWMQ0052	Not supported	IBM MQ for z/OS connection class resources must be protected properly.
ZWMQ0053	C2RHWM53	IBM MQ for z/OS dead-letter and alias dead-letter queues must be properly defined.
ZWMQ0054	Not supported	IBM MQ for z/OS queue resource defined to the appropriate resource class must be protected in accordance with security requirements.
ZWMQ0055	Not supported	IBM MQ for z/OS process resources must be protected in accordance with security requirements.
ZWMQ0056	Not supported	IBM MQ for z/OS namelist resources must be protected in accordance with security requirements.
ZWMQ0057	Not supported	IBM MQ for z/OS alternate user resources defined to appropriate ADMIN resource class must be protected in accordance with security requirements.
ZWMQ0058	Not supported	IBM MQ for z/OS context resources defined to the appropriate ADMIN resource class must be protected in accordance with security requirements.
ZWMQ0059	Not supported	IBM MQ for z/OS command resources defined to MQCMDS resource class are protected in accordance with security requirements.
ZWMQ0060	Not supported	IBM MQ for z/OS RESLEVEL resources in the appropriate ADMIN resource class must be protected in accordance with security requirements.