

RACF

zSecure V2.3.0 Compliance Controls for RACF

RACF STIG controls	CARLa members	STIG rules	Description
Controls customization	CKAG@*	CKAG@ CKAG@DEF CKAG@PLS CKAG@TMP CKAG@6 CKAG@6PL	STIG Compliance members and licenses Deftypes STIG Compliance Audit RACF STIGplus Compliance members AU.R STIG Temporary Implementations STANDARD and IMBEDS RACF STIG 6.31 STANDARD and IMBEDS RACF STIG PLUS 6.x
Access Control Program (ACP)	CKAGC*	CKAGC010 CKAGC020 CKAGC030 CKAGC040 CKAGC050 CKAGC060 CKAGC070 CKAGC080 CKAGC110 CKAGC120 CKAGC130 CKAGC135 CKAGC150 CKAGC170 CKAGC180 CKAGC220 CKAGC230 CKAGC250 CKAGC260 CKAGC270 CKAGC282 CKAGC293 CKAGC340 CKAGC350	ACP00010 PARMLIB protected ACP00020 Update on SYS1.LINKLIB ACP00030 Update on SYS1.SVCLIB ACP00040 Update on SYS1.IMAGELIB ACP00050 Update on SYS1.LPALIB ACP00060 Update+alter on APF list ACP00070 Update+alter on LPA list ACP00080 Update+alter on Nucleus ACP00110 Update+alter on Linklist ACP00120 RACF db protected ACP00130 Master Catalog protected ACP00135 User Catalogs protected ACP00150 JES data sets protected ACP00170 UADS protected ACP00180 SMF data sets protected ACP00220 GTF Trace security ACP00230 PAGE data sets protected ACP00250 PROCLIBs protected ACP00260 IEAABD profile protection ACP00270 dynamic lists ACP00282 MVS system commands ACP00293 MCS console ACP00340 z/OS baseline reports ACP00350 IEASYMUP protection
CICS	CKAGCI*	CKAGCI10	ZCIC0010 CICS system data sets

RACF

		CKAGCI20	ZCIC0020 Sensitive CICS Trans
		CKAGCI30	ZCIC0030 Proper SIT parameters
		CKAGCI40	ZCIC0040 Unique CICS Region user
		CKAGCI41	ZCIC0041 CICS default user
		CKAGCI42	ZCIC0042 CICS Timeout
	CKAGCR*	CKAGCR21	ZCICR021 CICS Trans class active
		CKAGCR41	ZCICR041 CICS PROPCNTL active
FTP	CKAGF*	CKAGF010	IFTP0010 FTP server daemon
		CKAGF020	IFTP0020 FTP parameter rules
		CKAGF030	IFTP0030 FTP.DATA config rules
		CKAGF040	IFTP0040 FTP User exits
		CKAGF050	IFTP0050 FTP warning banner
		CKAGF060	IFTP0060 FTP SMF record rules
		CKAGF070	IFTP0070 FTP UNIX directories
		CKAGF080	IFTP0080 FTP data sets
		CKAGF090	IFTP0090 TFTP Server protection
		CKAGF100	IFTP0100 FTP/Telnet AORL
		CKAGF110	IFTP0110 FTP control cards
Front End Processor (FEP)	CKAGFE*	CKAGFE11	ZFEP0011 FEP components
		CKAGFE12	ZFEP0012 FEP access
		CKAGFE13	ZFEP0013 FEP load & dump
IBM Health Checker for z/OS	CKAGHC*	CKAGHC01	ZHCKR001 Health check Datasets
		CKAGHC32	ZHCKR032 Health check STCs
z/OS Integrated Cryptographic Service Facility (ICSF)	CKAGIC*	CKAGIC01	ZICSR001 ICSF data sets
		CKAGIC32	ZICSR032 ICSF started task(s)
z/OS UNIX Telnet Server	CKAGIU*	CKAGIU20	IUTN0020 otelnetd startup command
JES	CKAGJE*	CKAGJE41	ZJES0041 JESSPOOL class active
		CKAGJE60	ZJES0060 Surrogate users
z/OS Data Analysis (AAMV)	CKAGM*	CKAGM010	AAMV0010 Change Management Process
		CKAGM014	AAMV0014 Upgrade OS plan
		CKAGM018	AAMV0018 Software Patches
		CKAGM030	AAMV0030 LNKAUTH=APFTAB
		CKAGM040	AAMV0040 APF libraries exist
		CKAGM050	AAMV0050 APF libraries unique

RACF

		CKAGM160	AAMV0160 PPT programs exist
		CKAGM380	AAMV0380 SMF record (sub)types
		CKAGM400	AAMV0400 Collect and retain SMF
		CKAGM420	AAMV0420 ACP database backup
		CKAGM430	AAMV0430 System DASD backups
		CKAGM440	AAMV0440 PASSWORD data set
		CKAGM450	AAMV0450 System programs
z/OS Communications Server	CKAGMT*	CKAGMT32	ZSMTR032 IBM CSSMTP Started task
SMTP application (CSSMTP)			
RACF-specific	CKAGR*	CKAGR244	RACF0244 FACILITY class active
		CKAGR246	RACF0246 OPERCMDS class active
		CKAGR248	RACF0248 CONSOLE class active
		CKAGR250	RACF0250 SETROPTS NOADSP
		CKAGR260	RACF0260 AUDIT active classes
		CKAGR270	RACF0270 TEMPDSN active
		CKAGR280	RACF0280 SETROPTS CMDVIOL
		CKAGR290	RACF0290 SETROPTS EGN
		CKAGR300	RACF0300 ERASE(ALL)
		CKAGR310	RACF0310 GENCMD active classes
		CKAGR320	RACF0320 GENERIC active classes
		CKAGR330	RACF0330 SETROPTS TERMINAL(READ)
		CKAGR350	RACF0350 SETROPTS GPRLIST
		CKAGR360	RACF0360 SETROPTS INACTIVE(35)
		CKAGR370	RACF0370 SETROPTS INITSTATS
		CKAGR380	RACF0380 SETROPTS BATCHALLRACF
		CKAGR400	RACF0400 SETROPTS XBMALLRACF
		CKAGR420	RACF0420 SETROPTS OPERAUDIT
		CKAGR430	RACF0430 SETROPTS PASSW HIST(10)
		CKAGR440	RACF0440 SETROPTS PASSW INT(60)
		CKAGR445	RACF0445 SETROPTS PASSW MINCHA>0
		CKAGR450	RACF0450 SETROPTS PASSW REVOK(1 2)
		CKAGR460	RACF0460 RACF PWDRULEs
		CKAGR467	RACF0467 Password algorithm
		CKAGR470	RACF0470 SETROPTS PASSW WARN>=10
		CKAGR480	RACF0480 SETROPTS PROTECTALL FAIL

RACF

		CKAGR490	RACF0490 SETROPTS REALDSN
		CKAGR500	RACF0500 SETROPTS RETPD 99999
		CKAGR520	RACF0520 SETROPTS SAUDIT
		CKAGR540	RACF0540 SETROPTS LOGOPTIONS
		CKAGR560	RACF0560 SETROPTS WHEN(PROGRAM)
		CKAGR570	RACF0570 RACF user default fields
		CKAGR590	RACF0590 Batch users have SURROGAT
		CKAGR595	RACF0595 Batch users PROTECT/Activ
		CKAGR620	RACF0620 STC unique users
		CKAGR660	RACF0660 STC TRUST/PRIV
		CKAGR680	RACF0680 DASD maintenance users
		CKAGR690	RACF0690 Emergency users
		CKAGR710	RACF0710 RACF SPECIAL assignment
		CKAGR720	RACF0720 OPERATIONS assignment
		CKAGR730	RACF0730 AUDITOR assignment
		CKAGR760	RACF0760 DASDVOL profiles
Syslog daemon	CKAGSD*	CKAGSD10	ISLG0010 Syslogd init time
		CKAGSD20	ISLG0020 Syslogd protected config
IBM System Display and Search Facility (SDSF) for RACF	CKAGSF*	CKAGSF38	ZISFR038 SDSF class active
IBM DFSMS	CKAGSM*	CKAGSM08	ZSMSR008 DFSMS classes active
		CKAGSM22	ZSMS0022 DFSMS control datasets
		CKAGSM32	ZSMS0032 SMS control ds found
TCP/IP	CKAGTC*	CKAGTC20	ITCP0020 TCPIP config statements
		CKAGTC30	ITCP0030 TCPIP config statements
		CKAGTC60	ITCP0060 TCP/IP started task
		CKAGTC70	ITCP0070 TCPIP datasets accessctrl
Telnet	CKAGTN*	CKAGTN10	ITNT0010 TN3270 settings
		CKAGTN50	ITNT0050 TN3270 SSL encryption
		CKAGTN60	ITNT0060 TN3270 SMF recording
TSO Telnet	CKAGTS*	CKAGTS20	ZTSO0020 UADS users
VTAM	CKAGVT*	CKAGVT18	ZVTM0018 VTAM system datasets
MQ	CKAGWM*	CKAGWM20	ZWMQ0020 MQ standard timeout
		CKAGWM30	ZWMQ0030 MQ started tasks

RACF

		CKAGWM40	ZWMQ0040 MQ data sets protection
		CKAGWM49	ZWMQ0049 MQ RACF classes active
		CKAGWM51	ZWMQ0051 MQ security switches on
		CKAGWM52	ZWMQ0052 MQCONN security
		CKAGWM53	ZWMQ0053 MQ dead letter protection
		CKAGWM54	ZWMQ0054 MQ QUEUE protection
		CKAGWM55	ZWMQ0055 MQPROC security
		CKAGWM56	ZWMQ0056 MQNLIST,GMQNLIST security
		CKAGWM58	ZWMQ0058 MQ context protection
		CKAGWM59	ZWMQ0059 MQCMDS security
		CKAGWM60	ZWMQ0060 MQ reslevel protection
z/OS UNIX	CKAGZU*	CKAGZU11	ZUSS0011 OMVS statement
		CKAGZU13	ZUSS0013 UNIX MOUNT parms
		CKAGZU22	ZUSS0022 SURROGAT resources
		CKAGZU32	ZUSS0032 UNIX components dsn
		CKAGZU41	ZUSS0041 UNIX system groups
		CKAGZU42	ZUSS0042 UNIX group unique
		CKAGZU43	ZUSS0043 UNIX kernel user
		CKAGZU44	ZUSS0044 UNIX user for BPXROOT
		CKAGZU45	ZUSS0045 UNIX user for RMFGAT
		CKAGZU46	ZUSS0046 UID(0) assignment
		CKAGZU47	ZUSS0047 UNIX user attributes
		CKAGZU48	ZUSS0048 OMVS default user
		CKAGZU60	ZUSSR060 UNIX classes active
		CKAGZU70	ZUSSR070 UNIX classes RACLISTed

RACF STIG Plus control STIG Plus

CARLa members
CKAGPL* CKAGPL01

STIG rules Description
ZCA1R003 RMM data sets security

RACF PCI-DSS controls PCI-DSS

CARLa members
CKAP@* CKAP@DEF
CKAP@32
CKAPC@
CKAPC* CKAPC121
CKAPC223

Rules Description
Deftypes and simulate statements PCI-DSS
STANDARD and IMBEDS RACF PCI-DSS V3.2
Main PCI-DSS V3.2 member
1.2.1 Restrict network traffic
2.2.3 Insecure services

RACF

CKAPC711	7.1.1 ID<>OWNER ALTER profiles
CKAPC722	7.2.2 PCI access control
CKAPC723	7.2.3 Default deny all
CKAPC811	8.1.1 Unique user id
CKAPC814	8.1.4 SETROPTS INACTIVE(90)
CKAPC816	8.1.6 SETROPTS PASSW REVOKE<=6
CKAPC821	8.2.1 Encrypt passwords
CKAPC823	8.2.3 SETROPTS PASSW LEN>=7
CKAPC824	8.2.4 SETROPTS PASSW INT<=90
CKAPC825	8.2.5 SETROPTS PASSW HIST>=4
CKAPCA22	10.2.2 Log root/admin actions
CKAPCA25	10.2.5 Log ident/authentication

RACF GSD controls GSD

CARLa members

CKAO@*	CKAO@
	CKAO@TMP
	CKAO@20C
CKAO*	CKAO111
	CKAO112
	CKAO113
	CKAO114
	CKAO115
	CKAO116
	CKAO117
	CKAO141
	CKAO1410
	CKAO1411
	CKAO1412
	CKAO1413
	CKAO1414
	CKAO1415
	CKAO1416
	CKAO1417
	CKAO1419
	CKAO142

Rules Description

	Main GSD member
	AU.R GSD Temporary Implementations
	STANDARD and IMBEDs for GSD version 2.0C
F.1.1.1	SETROPTS PASSW INT(90)
F.1.1.2	SETROPTS PASSW HIST(8)
F.1.1.3	SETROPTS PASSW REVOK(4)
F.1.1.4	SETROPTS PASSW NORULES
F.1.1.5	SETROPTS PASSW MINCHA(1)
F.1.1.6	SETROPTS PASSW INACT(180)
F.1.1.7	RVARY PASSW changed
F.1.4.1	SETROPTS BATCHALLRACF
F.1.4.10	TAPEVOL class active
F.1.4.11	UNIXPRIV class active
F.1.4.12	OPERCMDs class RACLISTEd
F.1.4.13	UNIXPRIV class RACLISTEd
F.1.4.14	DATASET class GENERIC
F.1.4.15	SETROPTS PROTECTALL FAIL
F.1.4.16	RVARY SWITCH PASSW changd
F.1.4.17	SETROPTS INITSTATS
F.1.4.19	SETROPTS CMDVIOL
F.1.4.2	DATASET class active

RACF

CKAO1420	F.1.4.20 SETROPTS SAUDIT
CKAO1421	F.1.4.21 SETROPTS OPERAUDIT
CKAO1422	F.1.4.22 DATASET class AUDIT
CKAO1423	F.1.4.23 GROUP entity AUDIT
CKAO1424	F.1.4.24 USER entity AUDIT
CKAO1425	F.1.4.25 OPERCMDS class AUDIT
CKAO1426	F.1.4.26 TSOAUTH class AUDIT
CKAO1427	F.1.4.27 SDSF class AUDIT
CKAO1428	F.1.4.28 FACILITY class AUDIT
CKAO1429	F.1.4.29 UNIXPRIV class AUDIT
CKAO143	F.1.4.3 GROUP entity active
CKAO1431	F.1.4.31 PROCESS class AUDIT
CKAO1439	F.1.4.39 MCS consoles LOGON
CKAO144	F.1.4.4 USER entity active
CKAO1441	F.1.4.41 DFHSM privileges
CKAO145	F.1.4.5 TEMPDSN class active
CKAO146	F.1.4.6 OPERCMDS class active
CKAO147	F.1.4.7 TSOAUTH class active
CKAO148	F.1.4.8 SDSF class active
CKAO149	F.1.4.9 FACILITY class active
CKAO1731	F.1.7.31 UNIX user unique HOME
CKAO1735	F.1.7.35 UID(0) home dir
CKAO1832	F.1.8.32 STGADMIN ENDUSER
CKAO1835	F.1.8.35 STGADMIN DELGDG
CKAO1848	F.1.8.48 TSOAUTH ACCT
CKAO1861	F.1.8.61 OPERCMDS SETPROG
CKAO1862	F.1.8.62 OPERCMDS SET.PROG
CKAO1863	F.1.8.63 OPERCMDS MVS.UNKNOWN
CKAO1866	F.1.8.66 OPERCMDS TCPIP.OBEYFILE
CKAO1867	F.1.8.67 FACILITY BPX.DAEMON
CKAO1868	F.1.8.68 FACILITY BPX.DEFAULT.USER
CKAO1869	F.1.8.69 FACILITY BPX.FILEATTR.APF
CKAO1870	F.1.8.70 FACILITY BPX.FILEATTR.PRO
CKAO1873	F.1.8.73 FACILITY BPX.SMF
CKAO1874	F.1.8.74 FACILITY BPX.STOR.SWAP

RACF

CKAO1875	F.1.8.75 FACILITY BPX.SUPERUSER
CKAO1876	F.1.8.76 FACILITY BPX.WLMSEVER
CKAO1895	F.1.8.95 RRSF profiles
CKAO1896	F.1.8.96 VTAMAAPL <RRSF acbname>