

# RACF User Group NY

IBM Security zSecure Suite

Automated Compliance Reporting  
zSecure Audit 3.1.0 (AU.R)

IBM Z Security and Compliance Center (zSCC)



*Marina Zografova*

*zSecure Development*

*mzografova@nl.ibm.com*

# Agenda

- Compliance standards supported in zSecure Audit 3.1
- DISA STIG version 8 (and z/OS Products STIG)
- IBM z/OS V2R5 with RACF Benchmark v1.1.0
- CIS IBM Db2 for z/OS Benchmark v1.0.0



# Agenda

- Compliance standards no longer supported in zSecure Audit 3.1.0 AU.R
- zSecure Audit integration with IBM Z Security and Compliance Center (zSCC)
- Digital Operational Resilience Act (DORA) for zOS (zSCC)
- zSecure Audit and zSCC live demo!



# Compliance standards supported in zSecure Audit 3.1.0 AU.R



## **IBM z/OS STIG v8**

z/OS standards developed by DISA for the DoD to secure DoD computing systems.<sup>1</sup>



## **z/OS Products STIG v6**

z/OS Products standards developed by DISA for the DoD to secure DoD computing systems.<sup>1</sup>



## **zSecure STIG v1.1**

IBM Security zSecure for RACF Security Technical Implementation Guide (STIG). Developed by zSecure and DISA.<sup>1</sup>



## **PCI-DSS**

Payment Card Industry Data Security Standard (PCI-DSS)<sup>3</sup>



## **IBM z/OS V2R5 with RACF v1.1.0**

This CIS Benchmark is the product of a community consensus process and consists of secure configuration guidelines developed for IBM Z System.<sup>2</sup>



## **IBM Db2 for z/OS Benchmark v1.0**

This CIS Benchmark is the product of a community Consensus process and consists of secure configuration guidelines developed for IBM Z System.<sup>2</sup>



Documentation updates technote:[IBM Security zSecure 3.1.0 Compliance Standards \(PDF\)](https://public.cyber.mil/stigs/)

Source 1: <https://public.cyber.mil/stigs/>

Source 2: [https://www.cisecurity.org/benchmark/ibm\\_z](https://www.cisecurity.org/benchmark/ibm_z)

Source 3: <https://www.pcisecuritystandards.org>

# zSecure Audit Release 3.1.0

## Overview of 3.1 compliance updates

IBM APAR	Description
<a href="#">OA66990</a> (base) <a href="#">OA66991</a> (ACF2) <a href="#">OA66992</a> (zSCC)	zSecure version 3.1.0 SSE 2 (October 2024): <ul style="list-style-type: none"> <li>- Further automation for CIS Benchmark for RACF</li> <li>- IBM DB2 for z/OS Benchmark v1.0.0 (NEW standard)</li> <li>- Existing zSecure Audit PCI-DSS controls converter to version 4 (zSecure Audit only)</li> <li>- IBM zSecure STIG for ACF2 1.1</li> </ul>
<a href="#">OA66794</a> (base) <a href="#">OA66795</a> (ACF2) <a href="#">OA66848</a> (zSCC)	STIG quarterly updates zSecure Audit support for: z/OS RACF STIG V9R1, z/OS ACF2 STIG V9R1, and z/OS TSS STIG V9R1
<a href="#">OA66278</a> (base) <a href="#">OA66279</a> (ACF2) <a href="#">OA66280</a> (zSCC)	zSecure version 3.1.0 SSE (March 2024) <ul style="list-style-type: none"> <li>- Further automation for CIS Benchmark for RACF</li> <li>- Separate z/OS Products STIGs introduced in zSCC</li> <li>- IBM zSecure STIG for RACF 1.1</li> </ul>
<a href="#">OA65870</a> (base) <a href="#">OA65871</a> (zSCC)	STIG quarterly updates zSecure Audit support for: z/OS STIG ACF2 8.13, z/OS STIG TSS 8.11, and CIS Benchmark for RACF 1.1.0

# DISA STIG in zSecure Audit 3.1.0

## APAR OA66794, August 2024

Latest version update: August 2024

z/OS STIG:

- ACF2 Versions:  
8.10,8.11,**8.12,8.13,8.14,8.15,9.01**
- RACF Versions:  
8.10,8.11,**8.12,8.13,8.14,9.01**
- TSS Versions:  
8.09,8.10,8.11,8.12,8.13,9.01

z/OS Products STIG:

- Version 6, release differs per product

### z/OS STIG

	ACF2 z/OS	RACF z/OS	TSS z/OS
Total	225	220	237
Ready	208	208	73
Missing	17	12	164
%	92%	95%	31%

### z/OS Products STIG

	ACF2 z/OS Products	RACF z/OS Products	TSS z/OS Products
Total	154	174	179
Ready	148	174	35
Missing	6	0	144
%	96%	100%	20%

# CIS benchmark with RACF (1.1.0)

# IBM z Systems CIS benchmark

CIS benchmark replaces outdated GSD331 support in AU.R.

## IBM Z System

This CIS Benchmark is the product of a community consensus process and consists of secure configuration guidelines developed for IBM Z System

CIS Benchmarks are freely available in PDF format for non-commercial use:

[DOWNLOAD LATEST CIS BENCHMARK →](#)

### Included in this Benchmark

#### FREE DOWNLOAD

#### CIS Benchmark

Safeguard IT systems against cyber threats with these CIS Benchmarks. Click to download a PDF from the list of available versions.

[LEARN MORE ABOUT CIS BENCHMARK →](#)

#### Recent versions available for CIS Benchmark:

- IBM CICS Transaction Server 6.1 (1.0.0)
- IBM Db2 13 for z/OS (1.0.0)
- **IBM z/OS V2R5 with RACF (1.1.0)**
- RHEL8 on IBM Z Linux (1.0.0)



### Discover the CIS Benchmarks

Learn what they are, how to use them, and how to get involved in their development.

[LEARN MORE →](#)

### Discover More Configuration Guides

There are more than 100 CIS Benchmarks across 25+ vendor product families.

[VIEW ALL CIS BENCHMARKS →](#)

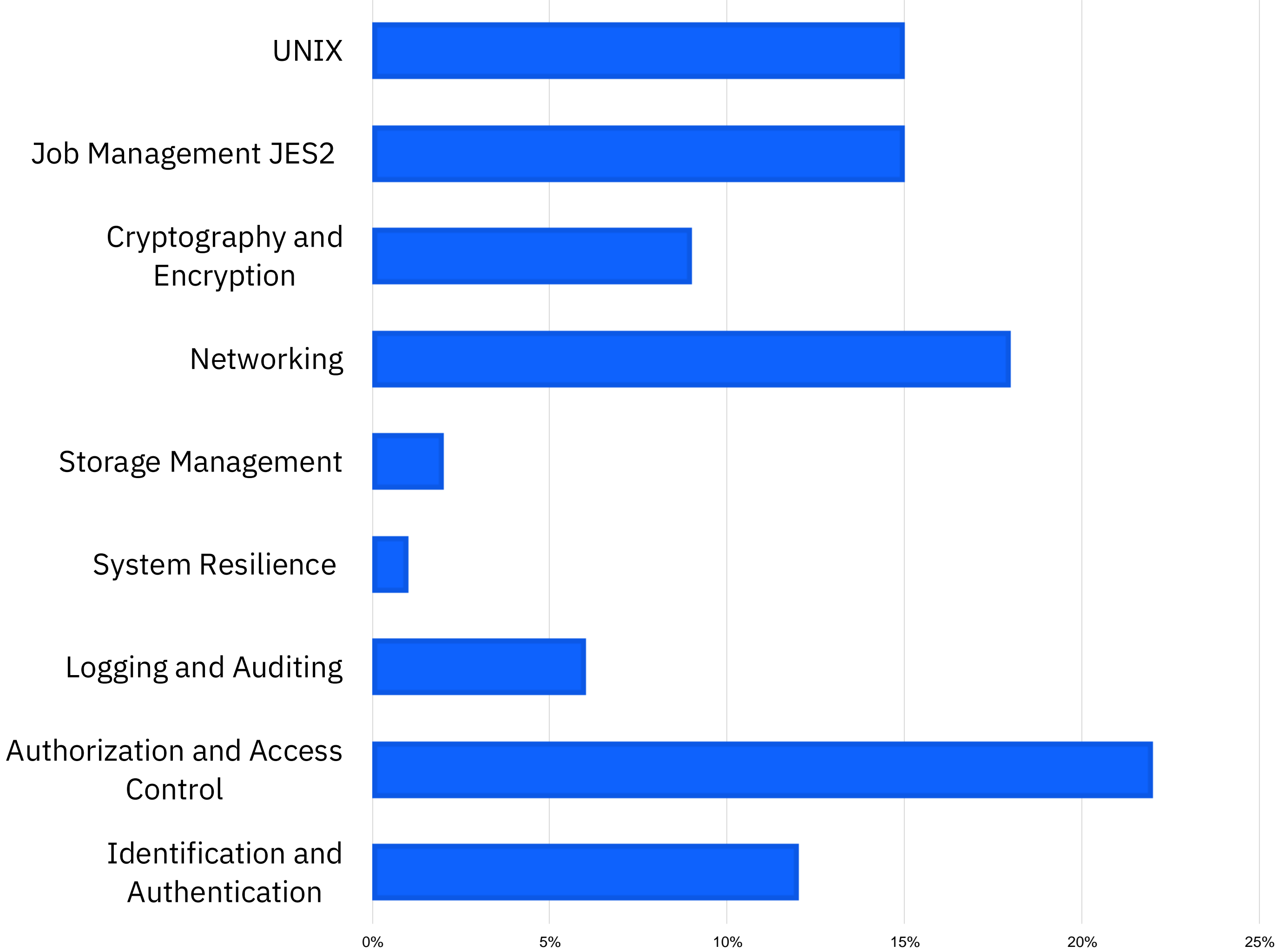
### View all active and archived CIS



# CIS Benchmark Recommendations

Most new controls (i.e., not STIG equivalent) added in Cryptography and Encryption, JES2, and UNIX sections

**219 controls**



# CIS Benchmark with RACF vs DISA STIG

- Industry-defined vs government-defined
- Based on STIG/NIST, but also developed by industry consensus and peer-reviewed
- Improvements to standard are more dynamic, everyone can submit a comment or request for enhancement:  
<https://workbench.cisecurity.org/registration>
- Establishes baseline of “best practices” vs prescriptive access controls
- DISA also has the Products STIG controls
- More ICSF recommendations (+13 new compared to 5 in DISA STIG)
- Protection of JESJOBS class profiles (15 new controls)
- More UNIX recommendations (+10 new recommendations)

# JESJOBS class profile controls not in DISA

8.3.1	Ensure that JESJOBS CLASS is set up
8.3.2	Ensure CANCEL JESJOBS profiles are protected
8.3.3	Awareness of the ENCRYPT JESJOBS profiles
8.3.4	Ensure GROUPREG JESJOBS profiles are protected
8.3.5	Ensure HOLD JESJOBS profiles are protected
8.3.6	Ensure JOBCLASS JESJOBS profiles are protected
8.3.7	Ensure JOBNFY JESJOBS profiles are protected
8.3.8	Ensure MODIFY JESJOBS profiles are protected
8.3.9	Ensure PURGE JESJOBS profiles are protected
8.3.10	Ensure RELEASE JESJOBS profiles are protected
8.3.11	Ensure REROUTE JESJOBS profiles are protected
8.3.12	Ensure SPIN JESJOBS profiles are protected
8.3.13	Ensure SPOOLIO JESJOBS profiles are protected
8.3.14	Ensure START JESJOBS profiles are protected
8.3.15	Ensure SUBMIT JESJOBS profiles are protected

# UNIX controls not in DISA

9.4	Ensure that RESTRICTED users cannot access UNIX files to which they are not explicitly permitted
9.17	Ensure that security commands in /etc/rc are safe
9.22	Ensure file permission for universal write is restricted
9.23	Ensure USS Telnet server is not active
9.24	Ensure rlogin is not active
9.25	Ensure changes to UNIX file security are logged
9.26	Ensure that programs cannot execute from the /tmp directory
9.27	Ensure that data sets containing user file systems do not have the user ID as the high-level qualifier
9.30	Ensure that file systems containing critical data are protected from access using profiles in the FSACCESS class
9.31	Ensure that file systems are mounted read-only wherever possible
9.32	Ensure that file systems are mounted with set-id files disabled wherever possible

# Interpreting a CIS Benchmark control

## Control identifier:

- 1. Identification and Authentication
- 2. System Settings
- 7. Ensure that CONSOLE resource...

## Profile Definitions:

Level 1: essential control; provides clear security benefit

Level 2: extended security on top of Level 1; not a standalone profile; for organizations that have an unusual high level of security

## Audit:

Security recommendations according to which zSecure evaluates the control and returns the finding status of the control (pass, fail, assert, etc.)

## 1.2.7 Ensure that CONSOLE resource class is ACTIVE (Manual)

### Profile Applicability:

- Level 1

### Description:

MCS consoles can be used to issue operator commands. Failure to control access to MCS consoles could result in unauthorized personnel issuing sensitive operator commands.

### Rationale:

Failure to control access to MCS consoles reduces the exposure that threatens the integrity and availability of the operating system environment and reduces compromises of confidential customer data.

### Audit:

Issue the `SETROPTS LIST` command and verify that the `CONSOLE` class is in the list of active classes.

```
SETROPTS LIST
```

### Remediation:

Issue the `SETROPTS` command to activate and `RACLIST` the `CONSOLE` class with this command:

```
SETROPTS CLASSACT(CONSOLE) RACLIST(CONSOLE)
```

# Interpreting a CIS Benchmark control

## References:

Majority (~74%) of CIS controls reference a DISA STIG rule (but that not mean that the requirements are identical!)

## Default Value:

The `CONSOLE` class is inactive.

## References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223659 Rule ID: SV-223659r604139\_rule STIG ID: RACF-ES-000110 Severity: CAT II

# CIS benchmark for RACF mapping to DISA z/OS STIG v8

CIS v1.0 Control ID	Control name	CIS CARLa member	CIS in relation to STIG	STIGv8 ID	STIG CARLa member
1.1.1	Ensure that the PASSWORD(INTERVAL) SETROPTS value is set to no longer than 90 days	CKAHR111	Partial STIG	RACF-ES-000800	CKAHE800
1.1.2	Ensure that the PASSWORD(HISTORY) SETROPTS value is set to at least 4	CKAHR112	Partial STIG	RACF-ES-000810	CKAHE810
1.1.3	Ensure that the PASSWORD(RULEn) SETROPTS value(s) is set	CKAHR113	Match STIG	RACF-ES-000770	CKAHE770
1.1.4	Ensure that the SETROPTS PASSWORD(MINCHANGE(n)) value will specify a minimum of 30 days	CKAHR114	Partial STIG	RACF-ES-000790	CKAHE790
1.1.5	Ensure that the PASSWORD(REVOKE) SETROPTS value is specified	CKAHR115	Partial STIG	RACF-ES-000480 RACF-ES-000490	CKAHE480
1.1.6	Ensure that the KDFAES algorithm is used to protect passwords in the system	CKAHE820	Match STIG	RACF-ES-000820	CKAHE820
1.1.7	Ensure that the PASSWORD(WARNING) SETROPTS value is set	CKAHR117	Partial STIG	RACF0470	CKAGR470
1.2.1	Ensure that Inactive users are revoked	CKAHR121	Partial STIG	RACF-ES-000760	CKAHE760
1.2.2	Ensure that STARTED class is used to assign users to Started Tasks	CKAHR122	Partial STIG	RACF-ES-000720	CKAHE720
1.2.3	Ensure user propagation is protected with the PROPCNTL class	CKAHE250	Match STIG	RACF-ES-000250	CKAHE250
1.2.4	Ensure that Job wait time option is set	CKAHR124	Partial STIG	RACF-OS-000010	C2RHO010
1.2.5	Ensure that started tasks defined with the trusted attribute are justified	CKAHR125	Partial STIG	RACF-ES-000130	CKAHE130
1.2.6	Ensure that the OPERCMDS resource class is ACTIVE and RACLISTed	CKAHR126	Match STIG	RACF-ES-000100	CKAHE100
1.2.7	Ensure that CONSOLE resource class is ACTIVE	CKAHE110	Match STIG	RACF-ES-000110	CKAHE110
1.2.8	Ensure that FACILITY resource class is ACTIVE and RACLISTED	CKAHR128	Partial STIG	RACF-ES-000090	CKAHE090
1.2.9	Ensure that inapplicable PPT entries have been invalidated	C2RHO290	Match STIG	RACF-OS-000290	C2RHO290
1.2.10	Ensure that LNKAUTH=APFTAB is specified in the IEASYSxx member(s) configuration	C2RHO300	Match STIG	RACF-OS-000300	C2RHO300
1.2.11	Ensure that the CONSOLxx members are configured	C2RHE680	Match STIG	RACF-ES-000680	C2RHE680
1.2.12	Ensure that no expired digital certificates are used	CKAHCE20	Match STIG	RACF-CE-000020	CKAHCE20
1.2.13	Ensure that RACF RVARYPW are set to non-default values	CKAHE550	Match STIG	RACF-ES-000550	CKAHE550
1.3.1	Ensure that the use of RACF SPECIAL Attribute is justified	CKAHE660	Match STIG	RACF-ES-000660	CKAHE660
1.3.2	Ensure that SYS1.UADS contains only emergency use user IDs	C2RHTS20	Match STIG	RACF-TS-000020	C2RHTS20
1.3.3	Ensure that MCS console user ID(s) is protected	CKAHE690	Match STIG	RACF-ES-000690	CKAHE690
1.3.4	Ensure that all STARTED class profiles specify PROTECTED user IDs	CKAHR134	Partial STIG	RACF-ES-000720	CKAHE720
2.1.1	Ensure that Maintenance user IDs are protected	CKAHR211	Partial STIG	RACF-ES-000850	CKAHE850
2.1.2	Ensure that access to active SMF collection files is controlled	CKAHR212	Partial STIG	RACF-ES-000540	CKAHE540
2.1.3	Ensure that the WHEN(PROGRAM) SETROPTS value is active	CKAHE610	Match STIG	RACF-ES-000610	CKAHE610
2.1.4	Ensure that the ICHDSM00 program is protected		NEW		

# CIS IBM Db2 for z/OS Benchmark (1.0.0)



# CIS IBM Db2 for z/OS Benchmark (1.0.0)

- Provides prescriptive guidance for establishing a secure configuration posture for IBM® Db2® for z/OS®.
- Intended for Db2 for z/OS system, database, and application administrators, security specialists, and auditors who plan to develop, deploy, assess, or secure solutions that incorporate IBM Db2 for z/OS.
- Can be downloaded via <http://workbench.cisecurity.org>.
- Peer-reviewed standard: expert community is encouraged to submit feedback and suggestions
- 78 recommendation (controls):
  - ❖ **Installation and Configuration:** Securing the system data sets and configuring the security system parameters
  - ❖ **Securing the database:** Securely connecting to and accessing the DB2 subsys, protecting data with encryption and privacy controls
  - ❖ **Audit:** Enabling auditing
- **!!Only available with zSCC licence via ISPF of ZSCC dashboard!!**

# CIS IBM Db2 for z/OS Benchmark (1.0.0) – SSE2 October 2024 (planned)

## zSecure Audit

```

                                     Z Security Compliance Center - Main menu
Option ==> _____
SE      Setup      Options and input data sets
RA      RACF       RACF Administration
AA      ACF2       ACF2 Administration
AU      Audit      Audit security and system resources
RE      Resource   Resource protection reports
EV      Events     Event reporting from SMF and other logs
CO      CARLa      Work with CARLa queries and libraries
IN      Information Information and documentation
LO      Local      Locally defined options
X       Exit       Exit this panel

Input complex:   PL87, NMPIPL87

Product/Release
5655-CC1 IBM Z Security and Compliance Center V1 for z/OS 3.2.E

```

```

                                     Z Security Compliance Center - Audit - Compliance
Option ==> _____
C       Configure  Configuration and site assertions
E       Evaluate   Run standard evaluation
H       History log Assertion, override, and configuration logs
S       Subsets    Rule subsets
T       Test rule  Single rule evaluation and configuration

```

# CIS IBM Db2 for z/OS Benchmark (1.0.0) – SSE2 October 2024 (planned)

## zSecure Audit

Z Security Compliance Center - Comp Row 1 to 15 of 38

Command ==> \_\_\_\_\_ Scroll ==> CSR

Subset name \_\_\_\_\_ (name for subset; ? for list of defined subsets)  
Description \_\_\_\_\_

Type **SAVE** to save, **RUN** to execute, **CONFIG** to configure, or **RESET** to remove all selections. Type **OPTIONS** to set the print/runtime options.  
Valid line commands: **S** (Show controls), **U** (Unselect all), **Z** (Select all), **A** (Run all controls in evaluation), **R** (Run selected controls in evaluation), **B** (Configure all controls in evaluation), **C** (Configure selected controls)  
Showing controls for: RACF

---

Evaluation	#Controls	#Selected
zOS_STIG	211	0
Prods_STIG	190	0
Db2_CIS	71	0
zOS_CIS	195	0
PCI-DSS	13	0
zSecure_STIG	12	0
Ab_AID_STIG	7	0
Auditor_STIG	3	0
CatSol_STIG	2	0
Com_Srv_STIG	3	0
CA1_TM_STIG	11	0

# CIS IBM Db2 for z/OS Benchmark (1.0.0) – SSE2 October 2024 (planned)

## zSecure Audit

OF OPTIONS to see the primary runtime options.

Valid line commands: **S** (Select), **U** (Unselect), **V** (View control member),  
**E** (Edit customization member), **R** (Run control), **C** (Configure control)

Control	Standard	Description	Member	CKACUST	S
— CIS-DB2-2.2.9	Db2_CIS	Dynamic query-related tbs	CKCHD229	_____	—
— CIS-DB2-2.2.10	Db2_CIS	SYSIBM.SYSINDEXES	CKCHD22A	_____	—
— CIS-DB2-2.2.11	Db2_CIS	SYSIBM.SYSOBJROLEDEP	CKCHD22B	_____	—
— CIS-DB2-2.2.12	Db2_CIS	Package-related tables	CKCHD22C	_____	—
— CIS-DB2-2.2.13	Db2_CIS	SYSIBM.SYSPACKAUTH	CKCHD22D	_____	—
— CIS-DB2-2.2.14	Db2_CIS	SYSIBM.SYSPARMS	CKCHD22E	_____	—
— CIS-DB2-2.2.15	Db2_CIS	SYSIBM.SYSPLAN	CKCHD22F	_____	—
— CIS-DB2-2.2.16	Db2_CIS	SYSIBM.SYSPLANAUTH	CKCHD22G	_____	—
— CIS-DB2-2.2.17	Db2_CIS	SYSIBM.SYSQUERY	CKCHD22H	_____	—
— CIS-DB2-2.2.18	Db2_CIS	SYSIBM.SYSRESAUTH	CKCHD22I	_____	—
— CIS-DB2-2.2.19	Db2_CIS	SYSIBM.SYSROLES	CKCHD22J	_____	—
— CIS-DB2-2.2.20	Db2_CIS	SYSIBM.SYSROUTINEAUTH	CKCHD22K	_____	—
— CIS-DB2-2.2.21	Db2_CIS	SYSIBM.SYSROUTINES	CKCHD22L	_____	—
— CIS-DB2-2.2.22	Db2_CIS	SYSIBM.SYSROUTINESTEXT	CKCHD22M	_____	—
— CIS-DB2-2.2.23	Db2_CIS	SYSIBM.SYSSCHEMAAUTH	CKCHD22N	_____	—
— CIS-DB2-2.2.24	Db2_CIS	SYSIBM.SYSSEQUENCEAUTH	CKCHD22O	_____	—
— CIS-DB2-2.2.25	Db2_CIS	SYSIBM.SYSSEQUENCES	CKCHD22P	_____	—
— CIS-DB2-2.2.26	Db2_CIS	SYSIBM.SYSSTMT	CKCHD22Q	_____	—
— CIS-DB2-2.2.27	Db2_CIS	SYSIBM.SYSSTOGROUP	CKCHD22R	_____	—
— CIS-DB2-2.2.28	Db2_CIS	SYSIBM.SYSTABAUTH	CKCHD22S	_____	—

# CIS IBM Db2 for z/OS Benchmark (1.0.0) – SSE2 October 2024 (planned)

## zSCC dashboard: Profiles

### Profiles

[View docs](#)

A profile is a collection of related controls. After you gather the configuration information of your resources and prepare your systems for scanning, you can create profiles to define the list of controls that you'd like to validate against.

Filters: [Clear filter](#)

Environment Type:  Profile family:  Category:

Search  Refresh Settings Create +

Name	Description	Type	Controls
<a href="#">Db2_zOS_CIS_1.0.0</a>	CIS IBM Db2 for z/OS Benchmark	Predefined	319
<a href="#">RACF_zOS_CIS_1.0.0</a>	CIS benchmark IBM z/OS V2R5 with RACF	Predefined	
<a href="#">RACF_zOS_CIS_1.1.0</a>	CIS benchmark IBM z/OS V2R5 with RACF	Predefined	

# Compliance standards no longer supported in zSecure Audit 3.1.0 AU.R

STIG version 6 - Refers only to the z/OS STIG; z/OS Products STIG v6 still available in AU.R

GSD - IBM standard often employed in outsourcing (ISeC/GSD331)

```
Menu          Options          Info          Commands          Setup
-----
Command ==>  _____ zSecure Admin+Audit for RACF - Compli Row 1 to 5 of 5
                                     Scroll ==> CSR
Subset name  _____ (name for subset; ? for list of defined subsets)
Description  _____

Type SAVE to save, RUN to execute, CONFIG to configure, or RESET
to remove all selections. Type OPTIONS to set the print/runtime options.
Valid line commands: S (Show rules), U (Unselect all), Z (Select all),
A (Run all rules in evaluation), R (Run selected rules in evaluation),
B (Configure all rules in evaluation), C (Configure selected rules in eval.)
Showing rules for: RACF
-----
Evaluation          #Rules  #Selected
-----
- STIG                377      0
- STIGv8              196      0
- PCI-DSS              14       0
- GSD                  57       0
- ZSECURE_EXTRA        9        0
***** Bottom of data *****
```

# GSD331 mapping to CIS Benchmark for RACF

## zSecure 3.1.0 Incompatibility Warnings

<b>GSD Control ID</b>	<b>Description</b>	<b>CIS Control ID</b>	<b>zSecure CARLa member (CIS control)</b>
F.1.1.1	SETOPTS PASSW INTERVAL(90)	1.1.1	CKAHR111
F.1.1.2	SETOPTS PASSW HISTORY(8)	1.1.2	CKAHR112
F.1.1.3	SETOPTS PASSW REVOKE(4)	1.1.5	CKAHR115
F.1.1.4	SETOPTS PASSW NORULES	1.1.3	CKAHE770
F.1.1.5	SETOPTS PASSW MINCHANGE(1)	1.1.4	CKAHR114
F.1.1.6	SETOPTS PASSW INACTIVE(180)	1.2.1	CKAHR121
F.1.1.7	RVARY PASSW changed	1.2.13	CKAHE550
F.1.4.1	SETOPTS BATCHALLRACF	8.4.2	CKAHE440
F.1.4.10	TAPEVOL class active	no equivalent	
F.1.4.11	UNIXPRIV class active	9.7	CKAHR97
F.1.4.12	OPERCMDSDS class RACLISTed	1.2.6	CKAHR126
F.1.4.13	UNIXPRIV class RACLISTed	no equivalent	
F.1.4.14	DATASET class GENERIC	2.2.2	CKAHR222
F.1.4.15.1	SETOPTS PROTECTALL FAIL	2.3.3	CKAHE570
F.1.4.15.2	SETOPTS WHEN(PROGRAM)	2.1.3	CKAHE610
F.1.4.16.1	RVARY SWITCH PASSW changed	1.2.13	CKAHE550

## zSecure Audit integration with IBM Z Security and Compliance Center (zSCC)

- We show full assessment of the following standards in the zSCC dashboard:
  - ✓ All separate z/OS Products STIG (previously bundled together)
  - ✓ zSecure STIG for RACF and ACF2 v1.1
  - ✓ RACF z/OS STIG versions 8.12,8.13,8.14,9.01
  - ✓ ACF2 z/OS STIG versions 8.12,8.13,8.14,8.15,9.01
  - ✓ z/OS RACF CIS Benchmark versions 1.0.0, 1.1.0
  - ✓ z/OS DB2 CIS Benchmark version 1.0.0 (Only with ZSCC licence)



# Digital Operational Resilience Act (DORA)

## IBM Z Security and Compliance Center (zSCC)



- legislative act, financial sector mainly
- focus on baseline security
- apply as of 17 January 2025
- overlapping requirement between standards and regulations (CIS, STIG, NIST, PCI-DSS, etc..etc..)
- zSCC as starting point with existing goals set

# Digital Operational Resilience Act (DORA) for zOS

Language English

## Profiles

A profile is a collection of related controls. After you gather the configuration information of your resources and prepare your systems for scanning, you can create profiles to define the list of controls that you'd like to validate against.

Filters:

Environment Type

All

Q dora

Name	Description	Type
<a href="#">Digital Operational Resilience Act(DORA) for zOS</a>	Digital Operational Resilience Act for zOS	Predefined

Items per page: 50 1-1 of 1 item

[Can't find the profile you're looking for?](#)

Compliance on IBM Z and LinuxONE

Dashboard

Assess

Scans

Configure

Scopes

Goals

Profiles

Settings

Access Management

User Settings

Manage Users

LDAP Settings

Profiles

Digital Operational Resilience Act(...)

Actions...

ID	Description
Article-6	Encryption and cryptographic controls
Article-7	Cryptographic key management
Article-11	Data and system security
Article-12	Logging
Article-13	Network security management
Article-14	Securing information in transit
Article-21	Access control
Article-23	Anomalous activities detection and criteria for ICT-related incidents
Article-35	Data system and network security

Items per page: 25 1-9 of 9 items 1

# Digital Operational Resilience Act(DORA) for zOS

Compliance on IBM Z and LinuxONE

Dashboard

Assess ^

Scans

Configure ^

Scopes

Goals

Profiles

Settings

Access Management ^

User Settings

Manage Users

LDAP Settings

Financial entities shall include in the policy on encryption and cryptographic controls criteria to select cryptographic techniques and use practices taking into account leading practices and standards. Should include in the policy on record the adoption of mitigation and monitoring measures. Should ensure any change in cryptography technology adopt mitigation and monitoring measures to remain resilient against cyber threats



Control ID	Severity	Status	Number of goals
Article-6.1	Critical	FAIL	124

Goals 
 Pass
  Fail
  Unable to validate
  Not applicable

ID: 4001001	Check whether all TCP/IP stacks have AT-TLS enabled	<input checked="" type="checkbox"/> 11	<input checked="" type="checkbox"/> 1	<input type="checkbox"/> 0	<input type="checkbox"/> 0	∨
ID: 4002006	Check whether FTP daemons are configured to use AT-TLS to encrypt FTP control and data connections	<input checked="" type="checkbox"/> 0	<input checked="" type="checkbox"/> 20	<input type="checkbox"/> 0	<input type="checkbox"/> 0	∨
ID: 4003001	Check whether the TELNETPARMS statements for all TN3270E servers have AT-TLS enabled on all ports	<input checked="" type="checkbox"/> 0	<input checked="" type="checkbox"/> 20	<input type="checkbox"/> 0	<input type="checkbox"/> 0	∨
ID: 4003002	Check whether the PARMSGROUP statements for all TN3270E servers specify connection type values that are consistent with AT-TLS use on all ports	<input checked="" type="checkbox"/> 0	<input checked="" type="checkbox"/> 0	<input type="checkbox"/> 20	<input type="checkbox"/> 0	∨
ID: 4004001	Check whether CSSMTP servers are configured to always use AT-TLS to encrypt connections to their target mail servers	<input checked="" type="checkbox"/> 0	<input checked="" type="checkbox"/> 2	<input type="checkbox"/> 0	<input type="checkbox"/> 0	∨
ID: 4049018	Check that weak algorithm DES56 is not in use	<input checked="" type="checkbox"/> 6	<input checked="" type="checkbox"/> 0	<input type="checkbox"/> 0	<input type="checkbox"/> 0	∨

zSecure AU.R  
ZSCC demo

# RACF User Group NY Conference



THANK YOU

謝謝

DZIĘKUJĘ CI    TARADH LEIBH    KEA LEBOHA

NGIYABONGA    БАЯРЛАЛАА    MISAOTRA ANAO

TEŞEKKÜR EDERİM    WHAKAWHETAI KOE

DANKIE    TERIMA KASIH    DANKON    TANK    TARADH LEAT

СПАСИБО    GRAZIE    MATUR NUWUN    ХВАЛА ВАМ    MULȚUMESC

РАКМЕТ СИЗГЕ    고맙습니다    GRAZIE    شكرا    HVALA    FAAFETAI

GO RAIBH MAITH AGAT    HVALA    ESKERRIK ASKO

БЛАГОДАРЯ    GRACIAS    MAHADSANID    THANK YOU    TEŞEKKÜR EDERİM

ТИ БЛАГОДАРАМ    DANKJE    ΕΥΧΑΡΙΣΤΩ    GRATIAS TIBI    OBRIGADO

TAK DANKE    AČIŪ    SALAMAT MAHALO IĀ 'ŌE    TAKK SKALDU HA    MERCI

РАHМАТ    MERCI    GRAZZI    PAKKA PÉR    ありがとうございます    DI OU MÈSI

HATUR NUHUN    PAХМАТ САГА    FALEMINDERIT    ありがとう    ĎAKUJEM

SIPAS JI WERE    TERIMA KASIH

CẢM ƠN BẠN    UA TSAUG RAU KOJ

WAZVIITA    ТИ БЛАГОДАРАМ

СИПОС