

CIS IBM Db2 13 for z/OS Benchmark

v1.0.0 - 06-17-2022

Terms of Use

Please see the below link for our current terms of use:

<https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/>

Table of Contents

Terms of Use	1
Table of Contents	2
Overview	5
Intended Audience.....	5
Consensus Guidance	6
Typographical Conventions.....	7
Recommendation Definitions.....	8
Title	8
Assessment Status.....	8
Automated	8
Manual.....	8
Profile	8
Description.....	8
Rationale Statement	8
Impact Statement.....	9
Audit Procedure.....	9
Remediation Procedure.....	9
Default Value.....	9
References	9
CIS Critical Security Controls® (CIS Controls®).....	9
Additional Information.....	9
Profile Definitions	10
Acknowledgements	11
Recommendations	12
1 Installation and Configuration	12
1.1 Installation protection	13
1.1.1 Ensure that Db2 system data sets are protected (Manual)	14
1.1.2 Ensure that Db2 USS file system is protected (Manual)	16
1.1.3 Secure installation process (Manual)	17
1.2 Security system parameters configuration.....	18
1.2.1 Ensure that RACF changes are accepted immediately (Manual).....	19
1.2.2 Ensure that authorization is enabled (Manual).....	21
1.2.3 Ensure that the default authorization IDs are changed from the installation defined (Manual)	22
1.2.4 Ensure that generic error codes are returned for remote security errors (Manual)	24
1.2.5 Separate security administration from system administration (Manual)	25
2 Secure the database.....	27

2.1 Secure database access	28
2.1.1 Ensure subsystem access is protected (Manual)	29
2.1.2 Ensure secure authentication is enabled for remote access (Manual)	30
2.1.3 Secure access by using Multi-Factor Authentication (MFA) (Manual)	32
2.1.4 Secure all remote connections by using SSL (Manual)	34
2.1.5 Secure remote connections by using TCP/IP Network Access control with the RACF SERVAUTH class (Manual)	36
2.1.6 Secure connections by using trusted contexts (Manual)	38
2.1.7 Secure object ownership by using Db2 roles (Manual)	40
2.1.8 Secure application access by using package controls (Manual)	42
2.1.9 Ensure that grant authorization IDs are defined in RACF (Manual)	44
2.2 Secure database catalog access	45
2.2.1 Ensure that access to the catalog tables in the communications database (CDB) is restricted (Manual)	46
2.2.2 Ensure that access to SYSIBM.SYSAUDITPOLICIES is restricted (Manual)	49
2.2.3 Ensure that access to SYSIBM.SYSCOLAUTH is restricted (Manual)	51
2.2.4 Ensure that access to SYSIBM.SYSCOLUMNS is restricted (Manual)	53
2.2.5 Ensure that access to trusted context tables is restricted (Manual)	55
2.2.6 Ensure that access to SYSIBM.SYSCONTROLS is restricted (Manual)	57
2.2.7 Ensure that access to SYSIBM.SYSDATABASE is restricted (Manual)	59
2.2.8 Ensure that access to SYSIBM.SYSDBAUTH is restricted (Manual)	61
2.2.9 Ensure that access to dynamic query-related tables is restricted (Manual)	63
2.2.10 Ensure that access to SYSIBM.SYSINDEXES is restricted (Manual)	65
2.2.11 Ensure that access to SYSIBM.SYSOBJROLEDEP is restricted (Manual)	67
2.2.12 Ensure that access to package-related tables is restricted (Manual)	69
2.2.13 Ensure that access to SYSIBM.SYSPACKAUTH is restricted (Manual)	71
2.2.14 Ensure that access to SYSIBM.SYSPARMS is restricted (Manual)	73
2.2.15 Ensure that access to SYSIBM.SYSPLAN is restricted (Manual)	75
2.2.16 Ensure that access to SYSIBM.SYSPLANAUTH is restricted (Manual)	77
2.2.17 Ensure that access to SYSIBM.SYSQUERY is restricted (Manual)	79
2.2.18 Ensure that access to SYSIBM.SYSRESAUTH is restricted (Manual)	81
2.2.19 Ensure that access to SYSIBM.SYSROLES is restricted (Manual)	83
2.2.20 Ensure that access to SYSIBM.SYSROUTINEAUTH is restricted (Manual)	85
2.2.21 Ensure that access to SYSIBM.SYSROUTINES is restricted (Manual)	87
2.2.22 Ensure that access to SYSIBM.SYSROUTINESTEXT is restricted (Manual)	89
2.2.23 Ensure that access to SYSIBM.SYSSCHEMAAUTH is restricted (Manual)	91
2.2.24 Ensure that access to SYSIBM.SYSSEQUENCEAUTH is restricted (Manual)	93
2.2.25 Ensure that access to SYSIBM.SYSSEQUENCES is restricted (Manual)	95
2.2.26 Ensure that access to SYSIBM.SYSSTMT is restricted (Manual)	97
2.2.27 Ensure that access to SYSIBM.SYSSTOGROUP is restricted (Manual)	99
2.2.28 Ensure that access to SYSIBM.SYSTABAUTH is restricted (Manual)	101
2.2.29 Ensure that access to SYSIBM.SYSTABLES is restricted (Manual)	103
2.2.30 Ensure that access to SYSIBM.SYSTABLESPACE is restricted (Manual)	105
2.2.31 Ensure that access to SYSIBM.SYSTRIGGERS is restricted (Manual)	107
2.2.32 Ensure that access to SYSIBM.SYSUSERAUTH is restricted (Manual)	109
2.2.33 Ensure that access to variable-related tables is restricted (Manual)	111
2.2.34 Ensure that access to SYSIBM.SYSVARIABLEAUTH is restricted (Manual)	113
2.2.35 Ensure that access to SYSIBM.SYSVIEWS is restricted (Manual)	115
2.3 Secure database pseudo catalog tables	117
2.3.1 Ensure that access to the program authorization table is restricted (Manual)	118
2.3.2 Ensure that access to the REST services definition table is restricted (Manual)	120
2.3.3 Ensure that access to the query accelerator tables is restricted (Manual)	122

2.3.4 Ensure that access to profile tables is restricted (Manual)	124
2.3.5 Ensure that access to SQL Data Insights tables is restricted (Manual).....	126
2.4 Secure database authorities	128
2.4.1 Secure SYSADM authority access (Manual).....	129
2.4.2 Secure SYSCTRL authority access (Manual)	131
2.4.3 Secure SYSOPR authority access (Manual)	133
2.4.4 Secure system DBADM authority access (Manual)	135
2.4.5 Secure DATAACCESS authority access (Manual)	137
2.4.6 Secure ACCESSCTRL authority access (Manual).....	139
2.4.7 Secure PACKADM authority access (Manual)	141
2.4.8 Secure SQLADM authority access (Manual).....	143
2.4.9 Secure database DBADM authority access (Manual)	145
2.4.10 Secure database DBCTRL authority access (Manual).....	147
2.4.11 Secure database DBMAINT authority access (Manual)	149
2.5 Encryption	151
2.5.1 Ensure that data is encrypted at rest and in-flight (Manual)	152
2.5.2 Secure sensitive data in memory (Manual)	154
2.6 Privacy Controls	155
2.6.1 Secure row access using row permission (Manual)	156
2.6.2 Secure column values using column mask (Manual)	157
3 Audit	158
3.1 Audit considerations	159
3.1.1 Ensure that audit tracing is enabled during Db2 start up (Manual)	160
3.1.2 Ensure that critical audit traces are always enabled (Manual)	162
3.1.3 Ensure that authorization failures are audited (Manual).....	164
3.1.4 Enable audit policies to audit installation system administrator and system operator access (Manual)	165
3.1.5 Enable auditing of system administrator access (Manual)	167
3.1.6 Enable auditing of database administrator access (Manual)	169
Appendix: Summary Table	171
Appendix: Change History	177

Overview

All CIS Benchmarks focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system for vulnerabilities and quickly updating with the latest security patches
- Monitoring applications and libraries for vulnerabilities and quickly updating with the latest security patches

In the end, the CIS Benchmarks are designed as a key **component** of a comprehensive cybersecurity program.

This document provides prescriptive guidance for establishing a secure configuration posture for IBM® Db2® 13 for z/OS®. This benchmark assumes that the client is using IBM RACF® as their external security manager (ESM).

Refer to <https://www.ibm.com/legal/copytrade> for listing of United States trademarks owned by IBM and related information.

To obtain the latest version of this guide, please visit <http://workbench.cisecurity.org>. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This benchmark is 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

Consensus Guidance

This CIS Benchmark was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit <https://workbench.cisecurity.org/>.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
<code>Stylized Monospace font</code>	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
<code>Monospace font</code>	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<i><italic font in brackets></i>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
<i>Italic font</i>	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) "5.1 - Establish Secure Configurations" and (v8) "4.1 - Establish and Maintain a Secure Configuration Process" so individual recommendations will not be mapped to these safeguards.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

Items in this profile intend to:

- be practical and prudent;
- provide a clear security benefit; and
- not inhibit the utility of the technology beyond acceptable means.

- **Level 2**

This profile extends the "Level 1 - Server" profile. Items in this profile exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is paramount.
- acts as defense in depth measure.
- may negatively inhibit the utility or performance of the technology.

Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Contributor

Shaun Kelley

Tracee Tao

Gayathiri Chandran

Yong Kwon

Editor

Eric Pinnell

Recommendations

1 Installation and Configuration

This section provides guidance on securing the system data sets and configuring the security system parameters.

1.1 Installation protection

This section provides guidance for securing the installation process.

1.1.1 Ensure that Db2 system data sets are protected (Manual)

Profile Applicability:

- Level 1

Description:

The Db2 data sets that contain system and configuration information, and log data must be protected from unauthorized modifications or deletions. These data sets can be accessed outside of Db2.

It is recommended that the following Db2 data sets are protected in RACF:

```
- HLQ.SDSNLOAD
- HLQ.SDSNLOD2
- HLQ.SDSNEXIT
- HLQ.DSNDBC.*
- HLQ.DSNDBD.*
- HLQ.BSDS*
- HLQ.LOGCOPY*
- HLQ.ARCHLOG*
- SYS1.PROCLIB
```

Note: HLQ is the high-level qualifier.

The RACF protection profile must have the following characteristics:

```
- UACC(NONE)
- No ID(*) on the access list
- Not in WARNING mode
- READ access permitted only to users who are required to have access
```

Rationale:

Failure to properly restrict access to the Db2 system and log data sets can result in a loss of system integrity or data.

Audit:

For each data set on the protection list, issue the following RACF commands to determine the protection profiles in place and evaluate access control to those resources.

```
LISTDSN DATASET('<dataset name>')
```




Remediation:

1. Create a protection profile for each of the data set in the list above.
2. Specify UACC(NONE) or no ID(*) to prevent universal access.
3. Permit READ, ALTER, CONTROL access based on roles and responsibilities and conform to least access needed.

For example, issue the following RACF commands to create generic profiles for active log data sets and assign access control to Db2 started tasks.

```
ADDSD 'DSNC000.LOGCOPY*' UACC(NONE)
PERMIT 'DSNC000.LOGCOPY*' ID(SYSDSP) ACCESS(ALTER)
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

1.1.2 Ensure that Db2 USS file system is protected (Manual)

Profile Applicability:

- Level 1

Description:

The USS file system that contains Db2 product code, such as the IBM Data Server Driver for JDBC and SQLJ, Db2 supplied Java classes, Db2 Java stored procedures support code, and native DLL libraries must be protected from unauthorized modifications or deletions.

The Db2 product code files are installed and stored under the default pathname, `/usr/lpp/db2x10`, where 'x' is the release indicator.

Rationale:

The USS file systems that contain system and product code must be restricted to authorized personnel and audited. Failure to protect can result in a loss of system services.

Audit:




Starting with the directory with pathname `/usr/lpp/db2x10` (where 'x' represents the release indicator) and for each of the sub-directories, issue the following command to review the directory and file permissions.

```
ls -l [pathname]
```

Remediation:

Issue the `chmod` command to change the access permission as needed.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

1.1.3 Secure installation process (Manual)

Profile Applicability:

- Level 1

Description:

The installation SYSOPR authority can be used for the installation and migration of a Db2 subsystem. The installation SYSOPR authority is not allowed access to non-system objects or user data in the subsystem.

Rationale:

Using the installation SYSOPR authority instead of the installation SYSADM authority prevents unauthorized access to user objects during installation or migration.

Audit:

Run the DSNTJ6Z job to obtain the current values of the `SYSTEM OPERATOR 1`, `SYSTEM OPERATOR 2` subsystem parameters. Verify that one of the authorization IDs that is used for installation or migration has the installation SYSOPR authority.




Remediation:

1. Edit the DSNTIJUZ job and modify the values for the `SYSTEM OPERATOR 1` or `SYSTEM OPERATOR 2` subsystem parameter as needed.
2. Submit DSNTIJUZ to assemble the subsystem parameter.
3. Issue the `-SET SYSPARM` command or stop and restart Db2 for the change to take effect.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=13-required-authorization-installation-migration>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

1.2 Security system parameters configuration

This section provides guidance for configuring the security-related system parameters.

1.2.1 Ensure that RACF changes are accepted immediately (Manual)

Profile Applicability:

- Level 1

Description:

The `AUTHEXIT_CACHEREFRESH` subsystem parameter refreshes the global authentication cache entries for user profile changes in RACF and authorization cache entries for external security users for resource and user profile changes. It is recommended that this security subsystem parameter is set to `ALL`.

Rationale:

Removing the cache entries prevents users whose profiles are changed in RACF from accessing Db2 resources.

Audit:

Run the `DSNTEJ6Z` job to obtain the current value of the `AUTHEXIT_CACHEREFRESH` subsystem parameter. Verify that the value is set to `ALL`.

Remediation:

1. Edit the `DSNTIJUZ` job and set the `DSN6SPRM.AUTHEXIT_CACHEREFRESH` parameter to `ALL`.
2. Submit `DSNTIJUZ` to assemble the subsystem parameter.
3. Stop and restart Db2 for the change to take effect.




Default Value:

<code>DSN6SPRM.AUTHEXIT_CACHEREFRESH=NONE</code>
--

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=dpp-auth-exit-cache-refr-authexit-cacherefresh-subsystem-parameter>
2. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=samples-job-dsntej6z>
3. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=uspadv-job-dsntijuz-define-db2-data-only-subsystem-parameter-module>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.2 <u>Establish an Access Revoking Process</u> Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.			

1.2.2 Ensure that authorization is enabled (Manual)

Profile Applicability:

- Level 1

Description:

The `AUTH` subsystem parameter controls authorization checking in Db2. It is recommended that this parameter is set to `YES`.

Rationale:

Disabling all authorization checking opens all Db2 access to `PUBLIC`.

Audit:

Run the `DSNTEJ6Z` job to obtain the current value of the `AUTH` subsystem parameter. Verify that the value is set to `YES`.

Remediation:

1. Edit the `DSNTIJUZ` job and set the `DSN6SPRM.AUTH` parameter to `YES`.
2. Submit `DSNTIJUZ` to assemble the subsystem parameter.
3. Issue the `-SET SYSPARM` command or stop and restart Db2 to activate the change.




Default Value:

`DSN6SPRM.AUTH=YES`

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=panel-use-protection-field-auth-subsystem-parameter>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

1.2.3 Ensure that the default authorization IDs are changed from the installation defined (Manual)

Profile Applicability:

- Level 1

Description:

The following subsystem parameters specify default authorization IDs. It is recommended to change the installation-specified default values and ensure the authorization IDs are defined in RACF.

- `SYSTEM ADMIN 1` – Specifies the first of two authorization IDs to which installation `SYSADM` authority is assigned.
- `SYSTEM ADMIN 2` - Specifies the second of two authorization IDs to which installation `SYSADM` authority is assigned.
- `SYSTEM OPERATOR 1` - Specifies the first of two authorization IDs to which installation `SYSOPR` authority is assigned.
- `SYSTEM OPERATOR 2` - Specifies the second of two authorization IDs to which installation `SYSOPR` authority is assigned.
- `SECURITY ADMIN 1` - Specifies the first of two authorization IDs or roles to which security administrator authority is assigned.
- `SECURITY ADMIN 2` - Specifies the second of two authorization IDs or roles to which security administrator authority is assigned.
- `UNKNOWN AUTHID` – Specifies the authorization ID that is to be used if RACF is not available for batch access and `USER=` is not specified in the `JOB` statement.

Rationale:

The installation default settings are often well known and can make the system vulnerable to attacks.

Audit:

Run the `DSNTEJ6Z` job to obtain the current values of the `SYSTEM ADMIN 1`, `SYSTEM ADMIN 2`, `SYSTEM OPERATOR 1`, `SYSTEM OPERATOR 2`, `SECURITY ADMIN 1`, `SECURITY ADMIN 2`, and `UNKNOWN AUTHID` subsystem parameters. Verify that the default values are changed.

Remediation:

1. Edit the DSNTIJUZ job and set the default values for `SYSTEM ADMIN 1`, `SYSTEM ADMIN 2`, `SYSTEM OPERATOR 1`, `SYSTEM OPERATOR 2`, `SECURITY ADMIN 1`, `SECURITY ADMIN 2`, and `UNKNOWN AUTHID` subsystem parameters.
2. Submit DSNTIJUZ to assemble the subsystem parameters.
3. Issue the `-SET SYSPARM` command or stop and restart Db2 to activate the changes.




Default Value:

```
SYSTEM ADMIN 1 - SYSADM
SYSTEM ADMIN 2 - SYSADM
SYSTEM OPERATOR 1 - SYSOPR
SYSTEM OPERATOR 2 - SYSOPR
SECURITY ADMIN 1 - SECADM
SECURITY ADMIN 2 - SECADM
UNKNOWN AUTHID - IBMUSER
```

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=session-dsntipp1-protection-panel-2>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

1.2.4 Ensure that generic error codes are returned for remote security errors (Manual)

Profile Applicability:

- Level 1

Description:

The `EXTSEC` subsystem parameter specifies whether detailed reason codes are returned to a DRDA client when a DDF connection request fails due to security errors. It is recommended to set the value to `NO` to return generic error codes to the clients.

Rationale:

The detailed error codes can expose the reason for a potential fraudulent logon attempt.

Audit:

Run the `DSNTEJ6Z` job to obtain the current value of the `EXTSEC` subsystem parameter. Verify that the value is set to `NO`.

Remediation:

1. Edit the `DSNTIJUZ` job and set the `DSN6SYSP.EXTSEC` parameter to `NO`.
2. Submit `DSNTIJUZ` to assemble the subsystem parameter.
3. Issue the `-SET SYSPARM` command or stop and restart Db2 to activate the change.

Default Value:

<code>DSN6SYSP.EXTSEC = YES</code>

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=2-extended-security-field-extsec-subsystem-parameter>

1.2.5 Separate security administration from system administration (Manual)

Profile Applicability:

- Level 1

Description:

The `SEPARATE_SECURITY` subsystem parameter allows you to separate security administrator duties from the Db2 system administrator duties when using native Db2 authorization. It is recommended to set `SEPARATE_SECURITY=YES`. When `SEPARATE_SECURITY` is set to `YES`, SECADM authority is required for security administration.

Db2 authorization that uses an external security mechanism for access control separates security administration from Db2 system administration.

Rationale:

Separating security administration from system administration enforces separation of duties. It can help simplify system administration and strengthen security administration.

Audit:

Run the DSNTIJ6Z job to obtain the current value of the `SEPARATE_SECURITY` subsystem parameter. Verify that the value is set to `YES`.

Remediation:

1. Ensure that the current SQLID is one of the authorization IDs of the process for applications that use SYSADM authority to set current SQLID.
2. Ensure that the binder has BINDAGENT privilege from the owner for the bind and rebind processes that use SYSADM, SYSCTRL, or system DBADM authority to specify the `OWNER` keyword.
3. Edit the DSNTIJUZ job and set the `DSN6SPRM.SEPARATE_SECURITY` parameter to `YES`.
4. Submit DSNTIJUZ to assemble the subsystem parameter.
5. Either issue the `-SET SYSPARM` command or stop and restart Db2 to activate the changes.




Default Value:

DSN6SPRM.SEPARATE_SECURITY = NO

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=2-separate-security-field-separate-security-subsystem-parameter>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2 Secure the database

This section provides guidance on securely connecting to and accessing a Db2 subsystem. It also provides guidance on securing access by administrative authorities and protecting data with encryption and privacy controls.

2.1 Secure database access

This section provides guidance on how to securely access Db2.

2.1.1 Ensure subsystem access is protected (Manual)

Profile Applicability:

- Level 1

Description:

The profiles specified in the DSNR RACF resource class control access to a Db2 for z/OS subsystem from another environment. It is recommended that you activate the DSNR class and define a profile with a name in the form of *subsystem.environment* for each subsystem and environment combination that you want to use. Permit profile access only to the users who are allowed to access Db2 from a specific environment.

Rationale:

Subsystem access control prevents users from connecting to Db2 from an unauthorized environment for malicious purposes.

Audit:

The RACF `RLIST` command displays the list of users or groups who have access to the corresponding profile for subsystem access in the DSNR class.

```
RLIST DSNR subsystem.environment ALL
```

Review the output to make sure that access is permitted according to the rules of your organization.

Ensure that you specify UACC(NONE) and no ID(*) to prevent universal access.




Remediation:

Permit users access to the corresponding profile for subsystem access based on the rules of your organization.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=racf-naming-protected-access-profiles>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.1.2 Ensure secure authentication is enabled for remote access (Manual)

Profile Applicability:

- Level 1

Description:

The `TCPALVER` subsystem parameter specifies the type of security credentials to accept for TCP/IP connection requests. It is recommended that you set the parameter to `SERVER_ENCRYPT` and require encrypted security credentials. With the required permissions to use the RACF passticket service, you can use RACF passticket to connect to Db2.

Rationale:

Non-encrypted user ID and password can expose their security credentials on the network.

Audit:

1. Run the DSNTEJ6Z job to obtain the current value of the `TCPALVER` subsystem parameter.
2. Verify that the parameter is set to `SERVER_ENCRYPT`.

Remediation:

1. Configure your remote systems and clients to use secure credentials.
2. Turn on IFCID 365 trace to audit authentication information for remote connections.
3. Edit the DSNTIJUZ job and set `DSN6FAC.TCPALVER=SERVER_ENCRYPT`.
4. Submit DSNTIJUZ to assemble the zparm.
5. Issue the `-SET SYSPARM` command or stop and restart Db2 for the change to take effect.




Default Value:

DSN6FAC TCPALVER = No

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=2-tcpip-already-verified-field-tcpalver-subsystem-parameter>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.1.3 Secure access by using Multi-Factor Authentication (MFA) (Manual)

Profile Applicability:

- Level 1

Description:

A multi-factor authentication system requires that multiple authentication factors be presented during logon to verify a user's identity. Each authentication factor must be from a separate category of credential types. Requiring multiple authentication factors improves the security of the user account.

You can set `AUTHEXIT_CACHEREFRESH`, `MFA_AUTHCACHE_UNUSED_TIME` system parameters to enable MFA for distributed clients that require multiple connections to perform a task in Db2.

It is recommended that you configure MFA for administrator access.

Rationale:

By requiring multiple authentication factors, the security of a user's account cannot be compromised if one of the factors is exposed.

Audit:

1. Determine if a MFA product is installed and user profiles are provisioned with MFA in compliance with the security policies of your organization.
2. If you use the IBM Z Multi-Factor Authentication product, verify that the RACF MFADEF class is active, and the user profile includes an active MFA factor type for user IDs that are provisioned for MFA.







Remediation:

1. Follow the instructions in [IBM Z Multi-Factor Authentication Installation and Customization](#) to install and customize MFA.
2. For user IDs that are provisioned for MFA, provide MFA login instructions.

References:

1. <https://www.ibm.com/docs/en/zos/2.5.0?topic=users-multi-factor-authentication-zos>
2. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=mitbcr-enabling-caching-mfa-based-authentication-credentials-clients-sysplex-workload-balancing>
3. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=mitbcr-enabling-caching-mfa-racf-passtickets-credentials-clients-without-sysplex-workload-balancing>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.4 <u>Require MFA for Remote Network Access</u> Require MFA for remote network access.			
v8	6.5 <u>Require MFA for Administrative Access</u> Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.			

2.1.4 Secure all remote connections by using SSL (Manual)

Profile Applicability:

- Level 1

Description:

The z/OS communications server for TCP/IP supports the Application Transport Transparent Layer Security (AT-TLS) function. AT-TLS performs TLS on behalf of Db2. It invokes the z/OS system SSL in the TCP layer of the TCP/IP stack and protects the transmission of data. It is recommended to configure AT-TLS to use SSL connections to secure all Db2 remote access.

To ensure that all access to Db2 uses SSL communications, set the TCP/IP `PORT` field to the same value as the `SECURE PORT` field. Also, set the static and dynamic subsetting location aliases to the same value as the `PORT` and `SECPORT` fields.

Rationale:

SSL secures your network connections and encrypts the data on the network. Failure to properly secure the network can result in data loss.

Audit:

1. See "[Encrypting your data with Secure Socket Layer \(SSL\) support](#)" and "[IBM Db2 for z/OS: Configuring TLS/SSL for Secure Client/Server Communications](#)" for more information.
2. To allow only SSL connections to Db2, verify that the `TCP/IP PORT` field is set to the same value as the `SECURE PORT` field and that both static and dynamic subsetting location aliases are defined with the same value as `PORT` and `SECPORT`.



Remediation:

Update the port values by using either the `DSNJ003` utility (DDF statement) or the `MODIFY DDF` command.

References:

1. <https://www.redbooks.ibm.com/abstracts/redp4799.html?Open>
2. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=pdter-encrypting-your-data-secure-socket-layer-ssl-support>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			

2.1.5 Secure remote connections by using TCP/IP Network Access control with the RACF SERVAUTH class (Manual)

Profile Applicability:

- Level 1

Description:

The z/OS communications server TCP/IP network access control provides the ability to control access to Db2 from a range of IP addresses that are defined as a security zone. When these controls are enabled, Db2 requires that the z/OS user ID of each Db2 client be permitted access to the RACF SERVAUTH class resource that represents the network security zone from which the client is connecting. If the user ID does not have the permission, then its login to Db2 will fail. It is recommended that you configure TCP/IP network access control with RACF SERVAUTH class to protect Db2 from unauthorized access.

Rationale:

The TCP/IP network access control with RACF SERVAUTH class protects access to Db2 by allowing users to connect only from approved part of the network.

Audit:

1. Review your TCP/IP profile data set for the `NETACCESS` statement definition and determine if the security zones are defined correctly. You can use the `NETSTAT CONFIG` (TSO) or `netstat -x f` (USS) command to display the current TCP/IP configuration, including the `NETACCESS` rules. Both of the commands in the example below display the current configuration for the TCP/IP stack named `TCPIP2`:

```
(TSO) NETSTAT CONFIG TCP TCPIP2
(USS) netstat -f -p tcpip2
```

2. Issue the RACF `RLIST` command to display the list of users or groups that have access to the corresponding profile for the TCP network zone access in the RACF SERVAUTH class.

```
RLIST SERVAUTH EZB.NETACCESS.sysname.tcpname.zonename ALL
```

Review the output to make sure the Db2 DIST address space user ID is permitted access and the user IDs for each authorized client are permitted access according to the organization rules.

Verify that `UACC(NONE)` is specified to prevent universal access to the RACF SERVAUTH class resource.

Remediation:

1. Configure the TCP/IP network access control by using the `NETACCESS` statement in your TCP/IP profile.
2. Permit users access to the corresponding profile for the TCP network security zone access in the RACF SERVAUTH class based on the rules of your organization.




Default Value:

TCP/IP network access controls are disabled by default.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=access-permitting-from-remote-requesters>
2. <https://www.ibm.com/docs/en/zos/2.5.0?topic=protection-network-access-control>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.1.6 Secure connections by using trusted contexts (Manual)

Profile Applicability:

- Level 1

Description:

Trusted context provides the capability to enforce the security attributes for a connection, switch users in the connection with optional authentication, and acquire one or more privileges that are not available outside of the trusted context. It is recommended that you enable trusted context for connections that use shared IDs.

Rationale:

Creating trusted contexts to enforce connection attributes such as encryption and assigning privileges to roles limit the scope of user access to a specific connection. Additionally, it ensures user accountability.

Audit:

1. Issue the following SQL statement to verify that a trusted context is enabled.

```
SELECT NAME, CONTEXTID, SYSTEMAUTHID, DEFAULTROLE, OBJECTOWNERTYPE,  
ENABLED, ALLOWPUBLIC, AUTHENTICATEPUBLIC FROM SYSIBM.SYSCONTEXT;  
SELECT CONTEXTID, NAME, VALUE FROM SYSIBM.SYSCTXTTRUSTATTRS;  
SELECT CONTEXTID, AUTHID, AUTHENTICATE, ROLE FROM SYSIBM.SYSCONTEXTAUTHIDS;
```

2. Review the trusted context definition.






Remediation:

Create and enable trusted contexts based on the rules of your organization.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=facilities-managing-access-through-trusted-contexts>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			

2.1.7 Secure object ownership by using Db2 roles (Manual)

Profile Applicability:

- Level 1

Description:

Db2 roles can be used to control access to enterprise objects in a way that parallels the structure of the enterprise. It is recommended that you use roles to separate object ownership from individual users and manage context-specific access outside of user privileges.

Rationale:

Assigning object ownership to a role prevents authorization IDs from obtaining implicit ownership privileges.

Audit:

1. Issue the following SQL statement to verify that roles are defined and associated with trusted contexts.

```
SELECT NAME FROM SYSIBM.SYSROLES;  
SELECT NAME, CONTEXTID, SYSTEMAUTHID, DEFAULTROLE, OBJECTOWNERTYPE,  
ENABLED, ALLOWPUBLIC, AUTHENTICATEPUBLIC FROM SYSIBM.SYSCONTEXT;  
SELECT CONTEXTID, AUTHID, AUTHENTICATE, ROLE FROM SYSIBM.SYSCONTEXTAUTHIDS;
```

2. Review the roles and trusted contexts definition.







Remediation:

1. Create roles and trusted contexts and assign roles as object owners based on the rules of your organization.
2. Issue the `SQL TRANSFER OWNERSHIP` statement to transfer the ownership of existing database and system objects to roles.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=statements-create-role>
2. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=statements-transfer-ownership>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.1 Establish and Maintain a Data Management Process</u> Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<u>3.3 Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.1.8 Secure application access by using package controls (Manual)

Profile Applicability:

- Level 1

Description:

The `BIND` options, `ENABLE` and `DISABLE` determine the connection types for a specific plan or package. It is recommended that you use these options to control the connection types for applications.

Rationale:

Restricting applications to use approved connection types prevents unauthorized access.

Audit:

1. Issue the following SQL statement to determine the approved connection types for a specific package or a plan.

```
SELECT PKS.SYSTEM, PKS.ENABLE, PKS.CNAME
FROM SYSIBM.SYSPACKAGE PK, SYSIBM.SYSPKSYSTEM PKS
WHERE PK.COLLID = PKS.COLLID AND PK.NAME = PKS.NAME;
SELECT PLS.SYSTEM, PLS.ENABLE, PLS.CNAME
FROM SYSIBM.SYSPLAN PL, SYSIBM.SYSPLSYSTEM PLS
WHERE PL.NAME = PLS.NAME;
```

2. Review the output.

Remediation:

Issue the `BIND PACKAGE / BIND PLAN / REBIND PACKAGE / REBIND PLAN` command with the `ENABLE` and `DISABLE` option to specify an approved connection type based on the rules of your organization.




Default Value:

Package and plan controls are enabled for all valid connection types.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=services-enable-disable-bind-options>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.1.9 Ensure that grant authorization IDs are defined in RACF (Manual)

Profile Applicability:

- Level 1

Description:

When Db2 native security is used for access control, you can grant privileges to users or groups using the SQL `GRANT` statement. If privileges are granted to an authorization-name, it is recommended that you also define the grantee users or groups in RACF.

Rationale:

Defining an authorization ID in RACF provides user accountability and prevents unauthorized access through orphan grantees.

Audit:

Issue the RACF `LISTGRP` and `LISTUSER` commands to determine if the authorization IDs are defined in RACF and review the output.




Remediation:

Issue the RACF `ADDUSER` and `ADDGROUP` commands to define the authorization IDs in RACF.

References:

1. <https://www.ibm.com/docs/en/zos/2.5.0?topic=reference-racf-command-syntax>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.1 <u>Establish an Access Granting Process</u> Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.			

2.2 Secure database catalog access

This section provides guidance for securing access to the catalog tables by authorized users, groups, or Db2 roles.

2.2.1 Ensure that access to the catalog tables in the communications database (CDB) is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The communications database (CDB) is a set of Db2 catalog tables that can be configured to control aspects of outbound and inbound connection requests. The SYSIBM.LOCATIONS table and SYSIBM.USERNAMES table are configured for using TCP/IP or SNA protocol. The following tables are configured specifically to use TCP/IP protocol:

- SYSIBM.IPLIST
- SYSIBM.IPNames

The following tables are configured specifically to use SNA protocol:

- SYSIBM.LULIST
- SYSIBM.LUMODES
- SYSIBM.LUNAMES
- SYSIBM.MODESELECT

`PUBLIC` should be restricted from inserting, updating, deleting, or accessing these tables.

Note: VTAM (SNA connection) is deprecated. You can disable SNA connections by setting IPNames in the bootstrap data set (BSDS).

Rationale:

`PUBLIC` access to these tables exposes connection information for remote Db2 access, which can compromise the security of the server.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if `PUBLIC` has access:

```
SELECT GRANTEE, TCREATOR, TTNAME FROM SYSIBM.SYSTABAUTH
WHERE TCREATOR = 'SYSIBM' AND
TTNAME IN ('LOCATIONS', 'IPNAMES', 'IPLIST', 'LUNAMES', 'LULIST',
          'LUMODES', 'MODESELECT', 'USERNAMES')
AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, `PUBLIC` has `SELECT`, `INSERT`, `UPDATE`, or `DELETE` privilege and the remediation steps should be followed.

For external security users:

Issue the `RACF RLIST` command to list the profiles that control access to the tables in the communications database in the `MDSNTB` class. Examine the universal access (`UACC`) and user (`USER`) settings for the profiles that control access to the communications database tables. If the `UACC` setting is `READ` or the `USER` setting is `*`, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the `SQL REVOKE` statement to revoke access from `PUBLIC`.




For external security users:

- Issue the `RACF RALTER` command to update the profiles and change the `UACC` setting to `NONE`.
- Issue the `RACF PERMIT` command to remove the `ID(*)` and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-locations>
2. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-usernames>
3. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-iplist>
4. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-ipnames>
5. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-lulist>
6. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-lumodes>
7. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-lunames>
8. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-modeselect>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.2 Ensure that access to SYSIBM.SYSAUDITPOLICIES is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSAUDITPOLICIES table contains all audit policies. PUBLIC should be restricted from accessing this table.

Rationale:

Exposing sensitive information about the auditing security on Db2 servers can compromise security. Access to the audit policies can enable attackers to avoid detection.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'SYSAUDITPOLICIES' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF RLIST command to list the profile that controls access to the SYSIBM.SYSAUDITPOLICIES table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSAUDITPOLICIES table. If the UACC setting is READ or the USER setting is *, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSAUDITPOLICIES FROM PUBLIC;
```




For external security users:

- Issue the RACF RALTER command to update the profile and change the UACC setting to NONE.
- Issue the RACF PERMIT command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysauditpolicies>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.3 Ensure that access to SYSIBM.SYSCOLAUTH is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSCOLAUTH table records the UPDATE or REFERENCES privileges that are held by users on individual columns of a table or view. PUBLIC should be restricted from accessing this table.

Rationale:

This table contains the column privileges granted to a user or role and can be used as an attack vector. Exposing who has access to a particular column of a table or view can enable attackers to identify those user IDs to gain access to the columns.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'SYSCOLAUTH' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF `RLIST` command to list the profile that controls access to the SYSIBM.SYSCOLAUTH table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSCOLAUTH table. If the UACC setting is `READ` or the USER setting is `*`, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSCOLAUTH FROM PUBLIC;
```




For external security users:

- Issue the RACF `RALTER` command to update the profile and change the UACC setting to `NONE`.
- Issue the RACF `PERMIT` command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-syscolauth>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.4 Ensure that access to SYSIBM.SYSCOLUMNS is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSCOLUMNS table contains one row for every column of each table and view. PUBLIC should be restricted from accessing this table.

Rationale:

This table contains sensitive column information about tables or views. Restricting access to table or view information from PUBLIC reduces the risk to your organization's data.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'SYSCOLUMNS' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF RLIST command to list the profile that controls access to the SYSIBM.SYSCOLUMNS table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSCOLUMNS table. If the UACC setting is READ or the USER setting is *, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSCOLUMNS FROM PUBLIC;
```




For external security users:

- Issue the RACF RALTER command to update the profile and change the UACC setting to NONE.
- Issue the RACF PERMIT command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-syscolumns>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.5 Ensure that access to trusted context tables is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The following tables are related to trusted context and contain details about trusted context, attributes for trusted context, and the authids that are allowed to use the trusted context.

- SYSIBM.SYSCONTEXT
- SYSIBM.SYSCONTEXTAUTHIDS
- SYSIBM.SYSCTXTRUSTATTRS

`PUBLIC` should be restricted from accessing these tables.

Rationale:

These tables contain sensitive information about trusted context definitions. Exposing trusted context definition can provide attackers with information that can be used to gain access to the server.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if `PUBLIC` has access:

```
SELECT GRANTEE, TCREATOR, TTNAME FROM SYSIBM.SYSTABAUTH
WHERE TCREATOR = 'SYSIBM' AND
TTNAME IN ('SYSCONTEXT', 'SYSCONTEXTAUTHIDS', 'SYSCTXTRUSTATTRS') AND
GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, `PUBLIC` has `SELECT` privilege and the remediation steps should be followed.

For external security users:

Issue the `RACF RLIST` command to list the profiles that control access to the trusted context tables in the `MDSNTB` class. Examine the universal access (`UACC`) and user (`USER`) settings for the profiles that control access to the trusted context tables. If the `UACC` setting is `READ` or the `USER` setting is `*`, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the SQL REVOKE statement to revoke access from PUBLIC.




For external security users:

- Issue the RACF `RALTER` command to update the profiles and change the UACC setting to `NONE`.
- Issue the RACF `PERMIT` command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-syscontext>
2. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-syscontextauthids>
3. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysctxtrustatts>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.6 Ensure that access to SYSIBM.SYSCONTROLS is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSCONTROLS table contains row permissions and column masks. PUBLIC should be restricted from accessing this table.

Rationale:

This table contains sensitive information. No PUBLIC access should be allowed to reduce the risk to your organization's data.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'SYSCONTROLS' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF RLIST command to list the profile that controls access to the SYSIBM.SYSCONTROLS table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSCONTROLS table. If the UACC setting is READ or the USER setting is *, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSCONTROLS FROM PUBLIC;
```




For external security users:

- Issue the RACF RALTER command to update the profile and change the UACC setting to NONE.
- Issue the RACF PERMIT command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-syscontrols>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.7 Ensure that access to SYSIBM.SYSDATABASE is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSDATABASE table records database information. PUBLIC should be restricted from accessing this table.

Rationale:

This table contains database information. Exposing database information can enable attackers to gain access to data in the server.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'SYSDATABASE' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF `RLIST` command to list the profile that controls access to the SYSIBM.SYSDATABASE table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSDATABASE table. If the UACC setting is `READ` or the USER setting is `*`, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSDATABASE FROM PUBLIC;
```




For external security users:

- Issue the RACF `RALTER` command to update the profile and change the UACC setting to `NONE`.
- Issue the RACF `PERMIT` command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysdatabase>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.8 Ensure that access to SYSIBM.SYSDBAUTH is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSDBAUTH table records the privileges that are held by users over databases. PUBLIC should be restricted from accessing this table.

Rationale:

This table contains all the grants over databases and may be used as an attack vector. Exposing who has access to databases can enable attackers to gain access to databases.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'SYSDBAUTH' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF RLIST command to list the profile that controls access to the SYSIBM.SYSDBAUTH table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSDBAUTH table. If the UACC setting is READ or the USER setting is *, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSDBAUTH FROM PUBLIC;
```




For external security users:

- Issue the RACF RALTER command to update the profile and change the UACC setting to NONE.
- Issue the RACF PERMIT command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysdbauth>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.9 Ensure that access to dynamic query-related tables is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The following tables contain information related to the stabilization of access paths for dynamic SQL statements and dependencies for dynamic query packages:

- SYSIBM.SYSDYNQRY
- SYSIBM.SYSDYNQRYDEP
- SYSIBM.SYSDYNQRY_TXTL

`PUBLIC` should be restricted from accessing these tables.

Rationale:

Exposing dynamic SQL statements and dynamic queries can enable attackers to gain access to your organization's data.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if `PUBLIC` has access:

```
SELECT GRANTEE, TCREATOR, TTNAME FROM SYSIBM.SYSTABAUTH WHERE TCREATOR =  
'SYSIBM' AND  
TTNAME IN ('SYSDYNQRY', 'SYSDYNQRYDEP', 'SYSDYNQRY_TXTL') AND  
GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, `PUBLIC` has `SELECT` privilege and the remediation steps should be followed.

For external security users:

Issue the `RACF RLIST` command to list the profiles that control access to the dynamic query-related tables in the `MDSNTB` class. Examine the universal access (`UACC`) and user (`USER`) settings for the profiles that control access to these tables. If the `UACC` setting is `READ` or the `USER` setting is `*`, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the `SQL REVOKE` statement to revoke access from `PUBLIC`.




For external security users:

- Issue the RACF `RALTER` command to update the profiles and change the UACC setting to `NONE`.
- Issue the RACF `PERMIT` command to remove the `ID(*)` and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysdynqry>
2. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysdynqrydep>
3. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysdynqry-txtl>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.10 Ensure that access to SYSIBM.SYSINDEXES is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSINDEXES table records one row for every index. PUBLIC should be restricted from accessing this table.

Rationale:

This table contains all index information and can be used as an attack vector. Exposing index information can enable attackers to gain access to your organization's data.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'SYSINDEXES' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF `RLIST` command to list the profile that controls access to the SYSIBM.SYSINDEXES table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSINDEXES table. If the UACC setting is `READ` or the USER setting is `*`, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSINDEXES FROM PUBLIC;
```




For external security users:

- Issue the RACF `RALTER` command to update the profile and change the UACC setting to `NONE`.
- Issue the RACF `PERMIT` command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysindexes>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.11 Ensure that access to SYSIBM.SYSOBJROLEDEP is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSOBJROLEDEP table lists the dependent objects for each role. PUBLIC should be restricted from accessing this table.

Rationale:

PUBLIC should not see the dependent objects for roles because doing so can expose those dependent objects to attackers. Exposing dependent objects for roles can enable attackers to gain access to the objects.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'SYSOBJROLEDEP' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF RLIST command to list the profile that controls access to the SYSIBM.SYSOBJROLEDEP table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSOBJROLEDEP table. If the UACC setting is READ or the USER setting is *, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSOBJROLEDEP FROM PUBLIC;
```




For external security users:

- Issue the RACF RALTER command to update the profile and change the UACC setting to NONE.
- Issue the RACF PERMIT command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysobjroleddep>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.12 Ensure that access to package-related tables is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The following tables contain information related to packages, dependencies of packages on objects, and statements in the packages:

- SYSIBM.SYSPACKAGE
- SYSIBM.SYSPACKCOPY
- SYSIBM.SYSPACKDEP
- SYSIBM.SYSPACKLIST
- SYSIBM.SYSPACKSTMT
- SYSIBM.SYSPACKSTMT_STMB
- SYSIBM.SYSPACKSTMT_STMT

`PUBLIC` should be restricted from accessing these tables.

Rationale:

Exposing the package information and statements in the package can enable attackers to gain access to your organization's data.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if `PUBLIC` has access:

```
SELECT GRANTEE, TCREATOR, TTNAME FROM SYSIBM.SYSTABAUTH WHERE TCREATOR =  
'SYSIBM' AND  
TTNAME LIKE 'SYSPACK%' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, `PUBLIC` has `SELECT` privilege and the remediation steps should be followed.

For external security users:

Issue the `RACF RLIST` command to list the profiles that control access to the package-related tables in the `MDSNTB` class. Examine the universal access (UACC) and user (USER) settings for the profiles that control access to these tables. If the UACC setting is `READ` or the USER setting is `*`, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the `SQL REVOKE` statement to revoke access from `PUBLIC`:




For external security users:

- Issue the RACF `RALTER` command to update the profiles and change the UACC setting to `NONE`.
- Issue the RACF `PERMIT` command to remove the `ID(*)` and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-syspackage>
2. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-syspackcopy>
3. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-syspackdep>
4. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-syspacklist>
5. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-syspackstmt>
6. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-syspackstmt-stmb>
7. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-syspackstmt-stmt>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.13 Ensure that access to SYSIBM.SYSPACKAUTH is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSPACKAUTH table contains the package privileges that are granted to an authorization ID or a role. PUBLIC should be restricted from accessing this table.

Rationale:

The list of all users with access to a package should not be exposed to PUBLIC. Exposing the users who have access to packages can enable attackers to gain access to your organization's data.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'SYSPACKAUTH' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF RLIST command to list the profile that controls access to the SYSIBM.SYSPACKAUTH table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSPACKAUTH table. If the UACC setting is READ or the USER setting is *, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSPACKAUTH FROM PUBLIC;
```




For external security users:

- Issue the RACF RALTER command to update the profile and change the UACC setting to NONE.
- Issue the RACF PERMIT command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-syspackauth>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.14 Ensure that access to SYSIBM.SYSPARMS is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSPARMS table contains a row for each parameter of a routine or multiple rows for table parameters (one for each column of the table). PUBLIC should be restricted from accessing this table.

Rationale:

Routine or table parameters should not be exposed to PUBLIC. Exposing routine or table parameters can enable attackers to gain access to data.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'SYSPARMS' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF RLIST command to list the profile that controls access to the SYSIBM.SYSPARMS table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSPARMS table. If the UACC setting is READ or the USER setting is *, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSPARMS FROM PUBLIC;
```




For external security users:

- Issue the RACF RALTER command to update the profile and change the UACC setting to NONE.
- Issue the RACF PERMIT command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysparms>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.15 Ensure that access to SYSIBM.SYSPLAN is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSPLAN table contains each application plan. PUBLIC should be restricted from accessing this table.

Rationale:

The names of plans can be used as an entry point if a vulnerable plan exists. Exposing plan information can enable attackers to execute plans to gain access to data.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'SYSPLAN' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF `RLIST` command to list the profile that controls access to the SYSIBM.SYSPLAN table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSPLAN table. If the UACC setting is `READ` or the USER setting is `*`, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSPLAN FROM PUBLIC;
```




For external security users:

- Issue the RACF `RALTER` command to update the profile and change the UACC setting to `NONE`.
- Issue the RACF `PERMIT` command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysplan>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.16 Ensure that access to SYSIBM.SYSPLANAUTH is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSPLANAUTH table records the privileges that are held by users over application plans. PUBLIC should be restricted from accessing this table.

Rationale:

The list of all users who have access to a plan should not be exposed to PUBLIC. Exposing this list can enable attackers to gain access to your organization's data.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'SYSPLANAUTH' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF RLIST command to list the profile that controls access to the SYSIBM.SYSPLANAUTH table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSPLANAUTH table. If the UACC setting is READ or the USER setting is *, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSPLANAUTH FROM PUBLIC;
```




For external security users:

- Issue the RACF RALTER command to update the profile and change the UACC setting to NONE.
- Issue the RACF PERMIT command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysplanauth>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.17 Ensure that access to SYSIBM.SYSQUERY is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSQUERY table identifies an SQL statement. PUBLIC should be restricted from accessing this table.

Rationale:

PUBLIC should not have access to the SQL statement information. Exposing SQL statement information can enable attackers to gain access to your organization's data.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME= 'SYSQUERY' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF `RLIST` command to list the profile that controls access to the SYSIBM.SYSQUERY table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSQUERY table. If the UACC setting is `READ` or the USER setting is `*`, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSQUERY FROM PUBLIC;
```




For external security users:

- Issue the RACF `RALTER` command to update the profile and change the UACC setting to `NONE`.
- Issue the RACF `PERMIT` command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysquery>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.18 Ensure that access to SYSIBM.SYSRESAUTH is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSRESAUTH table contains a list of all users that have various privileges on an object (collections, distinct types, etc.). PUBLIC should be restricted from accessing this table.

Rationale:

PUBLIC should not have access to this list of users. Exposing who has access to resources can enable attackers to gain access to your organization's data.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'SYSRESAUTH' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF RLIST command to list the profile that controls access to the SYSIBM.SYSRESAUTH table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSRESAUTH table. If the UACC setting is READ or the USER setting is *, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSRESAUTH FROM PUBLIC;
```




For external security users:

- Issue the RACF RALTER command to update the profile and change the UACC setting to NONE.
- Issue the RACF PERMIT command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysresauth>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.19 Ensure that access to SYSIBM.SYSROLES is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSROLES table contains all available roles. PUBLIC should be restricted from accessing this table.

Rationale:

PUBLIC should not have access to the roles. Exposing role information can enable attackers to gain access to your organization's data.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'SYSROLES' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF `RLIST` command to list the profile that controls access to the SYSIBM.SYSROLES table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSROLES table. If the UACC setting is `READ` or the USER setting is `*`, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSROLES FROM PUBLIC;
```




For external security users:

- Issue the RACF `RALTER` command to update the profile and change the UACC setting to `NONE`.
- Issue the RACF `PERMIT` command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysroles>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.20 Ensure that access to SYSIBM.SYSROUTINEAUTH is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSROUTINEAUTH table records the privileges that are held by users on routines (function or stored procedure). PUBLIC should be restricted from accessing this table.

Rationale:

PUBLIC should not have access to the privileges that are held by users. Exposing who has access to routines can enable attackers to gain access to your organization's data.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'SYSROUTINEAUTH' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF RLIST command to list the profile that controls access to the SYSIBM.SYSROUTINEAUTH table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSROUTINEAUTH table. If the UACC setting is READ or the USER setting is *, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSROUTINEAUTH FROM PUBLIC;
```




For external security users:

- Issue the RACF RALTER command to update the profile and change the UACC setting to NONE.
- Issue the RACF PERMIT command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysroutineauth>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.21 Ensure that access to SYSIBM.SYSROUTINES is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSROUTINES table contains routines (user-defined function, cast function, or stored procedure). PUBLIC should be restricted from accessing this table.

Rationale:

PUBLIC should not have access to routine definitions. Preventing PUBLIC to access routine information reduces the risk to your organization's data.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'SYSROUTINES' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF RLIST command to list the profile that controls access to the SYSIBM.SYSROUTINES table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSROUTINES table. If the UACC setting is READ or the USER setting is *, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSROUTINES FROM PUBLIC;
```




For external security users:

- Issue the RACF RALTER command to update the profile and change the UACC setting to NONE.
- Issue the RACF PERMIT command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysroutines>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.22 Ensure that access to SYSIBM.SYSROUTINESTEXT is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSROUTINESTEXT table is an auxiliary table for the TEXT column of the SYSIBM.SYSROUTINES table and is required to hold the LOB data. PUBLIC should be restricted from accessing this table.

Rationale:

PUBLIC should not have access to a table holding the LOB data. Exposing LOB data can enable attackers to gain access to your organization's data.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'SYSROUTINESTEXT' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF RLIST command to list the profile that controls access to the SYSIBM.SYSROUTINESTEXT table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSROUTINESTEXT table. If the UACC setting is READ or the USER setting is *, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSROUTINESTEXT FROM PUBLIC;
```




For external security users:

- Issue the RACF RALTER command to update the profile and change the UACC setting to NONE.
- Issue the RACF PERMIT command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysroutinestext>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.23 Ensure that access to SYSIBM.SYSSCHEMAAUTH is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSSCHEMAAUTH table contains a list of all users who have one or more privileges or access to a particular schema. PUBLIC should be restricted from accessing this table.

Rationale:

PUBLIC should not have access to this list of users. Preventing PUBLIC to access sensitive information reduces the risk to your organization's data.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'SYSSCHEMAAUTH' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF RLIST command to list the profile that controls access to the SYSIBM.SYSSCHEMAAUTH table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSSCHEMAAUTH table. If the UACC setting is READ or the USER setting is *, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSSCHEMAAUTH FROM PUBLIC;
```




For external security users:

- Issue the RACF RALTER command to update the profile and change the UACC setting to NONE.
- Issue the RACF PERMIT command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysschemaauth>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.24 Ensure that access to SYSIBM.SYSSEQUENCEAUTH is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSSEQUENCEAUTH table contains users, groups, or roles that have been granted one or more privileges on a sequence. PUBLIC should be restricted from accessing this table.

Rationale:

PUBLIC should not have access to this information. Exposing user's privileges over sequences can enable attackers to gain access to your organization's data.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'SYSSEQUENCEAUTH' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF RLIST command to list the profile that controls access to the SYSIBM.SYSSEQUENCEAUTH table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSSEQUENCEAUTH table. If the UACC setting is READ or the USER setting is *, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSSEQUENCEAUTH FROM PUBLIC;
```




For external security users:

- Issue the RACF RALTER command to update the profile and change the UACC setting to NONE.
- Issue the RACF PERMIT command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-syssequenceauth>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.25 Ensure that access to SYSIBM.SYSSEQUENCES is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSSEQUENCES table contains sequence definition. PUBLIC should be restricted from accessing this table.

Rationale:

PUBLIC should not have access to sequence information. Exposing sequence information can enable attackers to gain access to your organization's data.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE CREATOR = 'SYSIBM' AND  
TTNAME = 'SYSSEQUENCES' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF RLIST command to list the profile that controls access to the SYSIBM.SYSSEQUENCES table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSSEQUENCES table. If the UACC setting is READ or the USER setting is *, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSSEQUENCES FROM PUBLIC;
```




For external security users:

- Issue the RACF RALTER command to update the profile and change the UACC setting to NONE.
- Issue the RACF PERMIT command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-syssequences>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.26 Ensure that access to SYSIBM.SYSSTMT is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSSTMT table contains all SQL statements for each DBRM. PUBLIC should be restricted from accessing this table.

Rationale:

PUBLIC should not have access to these SQL statements. Preventing PUBLIC to access sensitive information reduces risk to your organization's data.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'SYSSTMT' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF RLIST command to list the profile that controls access to the SYSIBM.SYSSTMT table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSSTMT table. If the UACC setting is READ or the USER setting is *, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSSTMT FROM PUBLIC;
```




For external security users:

- Issue the RACF RALTER command to update the profile and change the UACC setting to NONE.
- Issue the RACF PERMIT command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysstmt>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.27 Ensure that access to SYSIBM.SYSSTOGROUP is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSSTOGROUP table contains one row for each storage group. PUBLIC should be restricted from accessing this table.

Rationale:

PUBLIC should not have access to storage group information. Exposing storage group information can enable attackers to gain access to your organization's data.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'SYSSTOGROUP' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF RLIST command to list the profile that controls access to the SYSIBM.SYSSTOGROUP table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSSTOGROUP table. If the UACC setting is READ or the USER setting is *, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSSTOGROUP FROM PUBLIC;
```




For external security users:

- Issue the RACF RALTER command to update the profile and change the UACC setting to NONE.
- Issue the RACF PERMIT command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysstogroup>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.28 Ensure that access to SYSIBM.SYSTABAUTH is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSTABAUTH table contains users or groups that have been granted one or more privileges on a table or view. PUBLIC should be restricted from accessing this table.

Rationale:

PUBLIC should not have access to the grants of tables and views. Exposing access information to tables or views can enable attackers to gain access to your organization's data.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'SYSTABAUTH' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF RLIST command to list the profile that controls access to the SYSIBM.SYSTABAUTH table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSTABAUTH table. If the UACC setting is READ or the USER setting is *, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSTABAUTH FROM PUBLIC;
```




For external security users:

- Issue the RACF RALTER command to update the profile and change the UACC setting to NONE.
- Issue the RACF PERMIT command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-systabauth>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.29 Ensure that access to SYSIBM.SYSTABLES is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSTABLES table contains definition for each table, view, or alias. PUBLIC should be restricted from accessing this table.

Rationale:

PUBLIC should not have access to table, view, or alias definitions. Preventing PUBLIC to access sensitive information reduces the risk to your organization's data.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'SYSTABLES' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF RLIST command to list the profile that controls access to the SYSIBM.SYSTABLES table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSTABLES table. If the UACC setting is READ or the USER setting is *, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSTABLES FROM PUBLIC;
```




For external security users:

- Issue the RACF RALTER command to update the profile and change the UACC setting to NONE.
- Issue the RACF PERMIT command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-systables>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.30 Ensure that access to SYSIBM.SYSTABLESPACE is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSTABLESPACE table contains one row for each table space. PUBLIC should be restricted from accessing this table.

Rationale:

PUBLIC should not have access to table space information. Exposing table space information can enable attackers to gain access to your organization's data.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'SYSTABLESPACE' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF RLIST command to list the profile that controls access to the SYSIBM.SYSTABLESPACE table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSTABLESPACE table. If the UACC setting is READ or the USER setting is *, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSTABLESPACE FROM PUBLIC;
```




For external security users:

- Issue the RACF RALTER command to update the profile and change the UACC setting to NONE.
- Issue the RACF PERMIT command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-systablespace>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.31 Ensure that access to SYSIBM.SYSTRIGGERS is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSTRIGGERS table contains one row for each trigger. PUBLIC should be restricted from accessing this table.

Rationale:

PUBLIC should not have access to trigger information. Exposing information on triggers can enable attackers to gain access to your organization's data.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'SYSTRIGGERS' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF RLIST command to list the profile that controls access to the SYSIBM.SYSTRIGGERS table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSTRIGGERS table. If the UACC setting is READ or the USER setting is *, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSTRIGGERS FROM PUBLIC;
```




For external security users:

- Issue the RACF RALTER command to update the profile and change the UACC setting to NONE.
- Issue the RACF PERMIT command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-systriggers>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.32 Ensure that access to SYSIBM.SYSUSERAUTH is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSUSERAUTH table records the system privileges that are held by users. PUBLIC should be restricted from accessing this table.

Rationale:

PUBLIC should not have access to system privileges held by users. Preventing PUBLIC to access sensitive information reduces the risk to your organization's data.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'SYSUSERAUTH' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF RLIST command to list the profile that controls access to the SYSIBM.SYSUSERAUTH table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSUSERAUTH table. If the UACC setting is READ or the USER setting is *, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSUSERAUTH FROM PUBLIC;
```




For external security users:

- Issue the RACF RALTER command to update the profile and change the UACC setting to NONE.
- Issue the RACF PERMIT command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysuserauth>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.33 Ensure that access to variable-related tables is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The following tables contain information related to global variables:

- SYSIBM.SYSVARIABLES
- SYSIBM.SYSVARIABLES_DESC
- SYSIBM.SYSVARIABLES_TEXT

`PUBLIC` should be restricted from accessing these tables.

Rationale:

Restricting `PUBLIC` access to global variable information reduces the risk to your organization's data.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if `PUBLIC` has access:

```
SELECT GRANTEE, TCREATOR, TTNAME FROM SYSIBM.SYSTABAUTH WHERE TCREATOR =  
'SYSIBM' AND  
TTNAME LIKE 'SYSVARIABLES%' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, `PUBLIC` has `SELECT` privilege and the remediation steps should be followed.

For external security users:

Issue the `RACF RLIST` command to list the profiles that control access to global variable-related tables in the `MDSNTB` class. Examine the universal access (`UACC`) and user (`USER`) settings for the profiles that control access to these tables. If the `UACC` setting is `READ` or the `USER` setting is `*`, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the `SQL REVOKE` statement to revoke access from `PUBLIC`:




For external security users:

- Issue the RACF `RALTER` command to update the profiles and change the UACC setting to `NONE`.
- Issue the RACF `PERMIT` command to remove the `ID(*)` and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysvariables>
2. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysvariables-desc>
3. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysvariables-text>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.34 Ensure that access to SYSIBM.SYSVARIABLEAUTH is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSVARIABLEAUTH table contains the granted privileges on a global variable for users, groups, or roles. PUBLIC should be restricted from accessing this table.

Rationale:

Restricting PUBLIC access to global variable information reduces the risk to your organization's data.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'SYSVARIABLEAUTH' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF RLIST command to list the profile that controls access to the SYSIBM.SYSVARIABLEAUTH table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSVARIABLEAUTH table. If the UACC setting is READ or the USER setting is *, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC.

```
REVOKE ALL ON SYSIBM.SYSVARIABLEAUTH FROM PUBLIC;
```




For external security users:

- Issue the RACF RALTER command to update the profile and change the UACC setting to NONE.
- Issue the RACF PERMIT command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysvariableauth>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.2.35 Ensure that access to SYSIBM.SYSVIEWS is restricted (Manual)

Profile Applicability:

- Level 1

Description:

The SYSIBM.SYSVIEWS table contains one or more rows for each view, materialized query table, or user-defined SQL function. PUBLIC should be restricted from accessing this table.

Rationale:

PUBLIC should not have access to this information. Preventing PUBLIC to access sensitive information reduces the risk to your organization's data.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'SYSVIEWS' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has SELECT privilege and the remediation steps should be followed.

For external security users:

Issue the RACF RLIST command to list the profile that controls access to the SYSIBM.SYSVIEWS table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profile that controls access to the SYSIBM.SYSVIEWS table. If the UACC setting is READ or the USER setting is *, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke access from PUBLIC:

```
REVOKE ALL ON SYSIBM.SYSVIEWS FROM PUBLIC;
```




For external security users:

- Issue the RACF RALTER command to update the profile and change the UACC setting to NONE.
- Issue the RACF PERMIT command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysviews>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.3 Secure database pseudo catalog tables

This section provides guidance for ensuring that the access to the pseudo catalog tables is held by authorized users, groups, or Db2 roles.

2.3.1 Ensure that access to the program authorization table is restricted (Manual)

Profile Applicability:

- Level 1

Description:

When program authorization is used, the SYSIBM.DSNPROGAUTH table controls whether a program can use a plan for execution.

PUBLIC should be restricted from accessing this table.

Rationale:

PUBLIC access to this table exposes the control information that indicates whether a program is allowed to use a plan for execution.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'DSNPROGRAUTH' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has access and the remediation steps should be followed.

For external security users:

Issue the RACF RLIST command to list the profile that controls access to the SYSIBM.DSNPROGAUTH table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profiles that control access to the program authorization table. If the UACC setting is READ or the USER setting is *, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the SQL REVOKE statement to revoke access from PUBLIC.




For external security users:

- Issue the RACF RALTER command to update the profile and change the UACC setting to NONE.
- Issue the RACF PERMIT command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=authorization-table-spaces-indexes-program>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.3.2 Ensure that access to the REST services definition table is restricted (Manual)

Profile Applicability:

- Level 1

Description:

When Db2 REST services are used, the SYSIBM.DSNSERVICE table is used to describe REST services and to associate them with corresponding packages.

PUBLIC should be restricted from accessing this table.

Rationale:

PUBLIC access to this table exposes the REST services and their package association.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if PUBLIC has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME = 'DSNSERVICE' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, PUBLIC has access and the remediation steps should be followed.

For external security users:

Issue the RACF `RLIST` command to list the profile that controls access to the SYSIBM.DSNSERVICE table in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profiles that control access to the REST services table. If the UACC setting is `READ` or the USER setting is `*`, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the `SQL REVOKE` statement to revoke access from PUBLIC.




For external security users:

- Issue the RACF `RALTER` command to update the profile and change the UACC setting to `NONE`.
- Issue the RACF `PERMIT` command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=services-enabling-db2-rest>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.3.3 Ensure that access to the query accelerator tables is restricted (Manual)

Profile Applicability:

- Level 1

Description:

When a query accelerator is used, the following tables are used by Db2 to control the acceleration behavior:

- SYSACCEL.SYSACCELERATORS
- SYSACCEL.SYSACCELERATEDTABLES
- SYSACCEL.SYSACCELERATEDPACKAGES
- SYSACCEL.SYSACCELERATEDTABLESAUTH

`PUBLIC` should be restricted from accessing these tables.

Rationale:

`PUBLIC` access to these tables exposes the accelerator server definition, accelerator behavior, and access information and can lead to inconsistent behavior between Db2 and the accelerator.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if `PUBLIC` has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSACCEL' AND  
TTNAME LIKE 'SYSACCEL%' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, `PUBLIC` has access and the remediation steps should be followed.

For external security users:

Issue the `RACF RLIST` command to list the profiles that control access to the accelerator tables in the `MDSNTB` class. Examine the universal access (UACC) and user (USER) settings for the profiles that control access to the accelerator tables. If the UACC setting is `READ` or the USER setting is `*`, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the `SQL REVOKE` statement to revoke access from `PUBLIC`.




For external security users:

- Issue the RACF `RALTER` command to update the profiles and change the UACC setting to `NONE`.
- Issue the RACF `PERMIT` command to remove the `ID(*)` and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=accelerators-tables-that-support-query-acceleration>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.3.4 Ensure that access to profile tables is restricted (Manual)

Profile Applicability:

- Level 1

Description:

When profiles are used for monitoring and controlling Db2 in specific application contexts, the following tables are used to define the profiles, provide the filtering criteria, and specify the action that Db2 takes for the processes that meet the filtering criteria:

- SYSIBM.DSN_PROFILE_TABLE
- SYSIBM.DSN_PROFILE_HISTORY
- SYSIBM.DSN_PROFILE_ATTRIBUTES
- SYSIBM.DSN_PROFILE_ATTRIBUTES_HISTORY

`PUBLIC` should be restricted from accessing these tables.

Rationale:

`PUBLIC` access to these tables exposes the profile definitions to monitor and control threads and connections from various applications.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if `PUBLIC` has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSIBM' AND  
TTNAME LIKE 'DSN_PROFILE%' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, `PUBLIC` has access and the remediation steps should be followed.

For external security users:

Issue the `RACF RLIST` command to list the profile that controls access to the profile tables in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profiles that control access to the profile tables. If the UACC setting is `READ` or the USER setting is `*`, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the `SQL REVOKE` statement to revoke access from `PUBLIC`.




For external security users:

- Issue the RACF `RALTER` command to update the profiles and change the UACC setting to `NONE`.
- Issue the RACF `PERMIT` command to remove the `ID(*)` and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-profile>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.3.5 Ensure that access to SQL Data Insights tables is restricted (Manual)

Profile Applicability:

- Level 1

Description:

SQL Data Insights (DI) brings deep learning AI capabilities into Db2. When SQL Data Insights capability is used, the following tables are used to define and store the metadata for AI objects, object models, and tables:

- SYSAIDB.SYSAIOBJECTS
- SYSAIDB.SYSAICONFIGURATIONS
- SYSAIDB.SYSAICOLUMNCONFIG
- SYSAIDB.SYSAIMODELS
- SYSAIDB.SYSAIDCOLUMNCENTERS
- SYSAIDB.SYSAITRAININGJOBS

`PUBLIC` should be restricted from accessing these tables.

Rationale:

`PUBLIC` access to these tables exposes the AI object definition, object models, and training jobs.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check if `PUBLIC` has access:

```
SELECT GRANTEE FROM SYSIBM.SYSTABAUTH WHERE TCREATOR = 'SYSAIDB' AND  
TTNAME LIKE 'SYSAI%' AND GRANTEE = 'PUBLIC';
```

Output that contains zero rows is considered a successful finding. Otherwise, `PUBLIC` has access and the remediation steps should be followed.

For external security users:

Issue the `RACF RLIST` command to list the profile that controls access to the SQL Data Insights tables in the MDSNTB class. Examine the universal access (UACC) and user (USER) settings for the profiles that control access to the SQL DI tables. If the UACC setting is `READ` or the USER setting is `*`, consult with your security administrator for the proper value and follow the remediation steps.

Remediation:

For Db2 internal security users:

Issue the `SQL REVOKE` statement to revoke access from `PUBLIC`.




For external security users:

- Issue the RACF `RALTER` command to update the profiles and change the UACC setting to `NONE`.
- Issue the RACF `PERMIT` command to remove the `ID(*)` and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=running-ai-queries-sql-data-insights>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.4 Secure database authorities

This section provides guidance for ensuring that administrator authority is held by authorized users, groups, or Db2 roles.

2.4.1 Secure SYSADM authority access (Manual)

Profile Applicability:

- Level 1

Description:

The SYSADM authority defines the system administrator authority. It is recommended that the SYSADM authority be granted to an authorization ID or a role.

Rationale:

Allowing SYSADM authority for `PUBLIC` jeopardizes the Db2 system and organizational data. If an account that possesses this authority is compromised or used in a malicious manner, the confidentiality, integrity, and availability of data in the Db2 subsystem will be at increased risk.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check SYSADM authority access:

```
SELECT GRANTEE, GRANTEETYPE FROM SYSIBM.SYSUSERAUTH WHERE SYSADMAUTH IN ('G', 'Y');
```

If `PUBLIC` has SYSADM access, follow the remediation steps.

Review the access list to ensure that the grants are aligned with your organization's access policies.

For external security users:

Issue the RACF `RLIST` command to list the profile that controls access to the SYSADM authority in the DSNADM class.

- Examine the universal access (UACC) and user (USER) settings for the profile. If the UACC setting is `READ` or the USER setting is `*`, consult with your security administrator for the proper value and follow the remediation steps.
- Review the access list to ensure that the permits are aligned with your organization's access policies.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke SYSADM authority from PUBLIC:

```
REVOKE SYSADM FROM PUBLIC;
```




For external security users:

- Issue the RACF `RALTER` command to update the UACC setting to `NONE`.
- Issue the RACF `PERMIT` command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=authorities-sysadm>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.4.2 Secure SYSCTRL authority access (Manual)

Profile Applicability:

- Level 1

Description:

The SYSCTRL authority defines the system control authority. It is recommended that the SYSCTRL authority be granted to an authorization ID or a role.

Rationale:

Allowing SYSCTRL authority for `PUBLIC` jeopardizes the Db2 system and organizational data. If an account that possesses this authority is compromised or used in a malicious manner, the confidentiality, integrity, and availability of the Db2 subsystem will be at increased risk.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check SYSCTRL authority access:

```
SELECT GRANTEE, GRANTEETYPE FROM SYSIBM.SYSUSERAUTH WHERE SYSCTRLAUTH IN ('G', 'Y');
```

If `PUBLIC` has SYSCTRL access, follow the remediation steps.

Review the access list to ensure that the grants are aligned with your organization's access policies.

For external security users:

Issue the RACF `RLIST` command to list the profile that controls access to the SYSCTRL authority in the DSNADM class.

- Examine the universal access (UACC) and user (USER) settings for the profile. If the UACC setting is `READ` or the USER setting is `*`, consult with your security administrator for the proper value and follow the remediation steps.
- Review the access list to ensure that the permits are aligned with your organization's access policies.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke SYSCTRL access from PUBLIC:

```
REVOKE SYSCTRL FROM PUBLIC;
```




For external security users:

- Issue the RACF `RALTER` command to update the UACC setting to `NONE`.
- Issue the RACF `PERMIT` command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=authorities-sysctrl>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.4.3 Secure SYSOPR authority access (Manual)

Profile Applicability:

- Level 1

Description:

The SYSOPR authority defines the system operator authority that allows its holder to issue most of the Db2 commands. It is recommended that the SYSOPR authority be granted to an authorization ID or a role.

Rationale:

Allowing SYSOPR authority for `PUBLIC` can jeopardize the Db2 subsystem.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check SYSOPR authority access:

```
SELECT GRANTEE, GRANTEETYPE FROM SYSIBM.SYSUSERAUTH WHERE SYSOPRAUTH IN ('G', 'Y');
```

If `PUBLIC` has SYSOPR access, follow the remediation steps.

Review the access list to ensure that the grants are aligned with your organization's access policies.

For external security users:

Issue the RACF `RLIST` command to list the profile that controls access to the SYSOPR authority in the DSNADM class.

- Examine the universal access (UACC) and user (USER) settings for the profile. If the UACC setting is `READ` or the USER setting is `*`, consult with your security administrator for the proper value and follow the remediation steps.
- Review the access list to ensure that the permits are aligned with your organization's access policies.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke SYSOPR access from `PUBLIC`:

```
REVOKE SYSOPR FROM PUBLIC;
```




For external security users:

- Issue the RACF `RALTER` command to update the UACC setting to `NONE`.
- Issue the RACF `PERMIT` command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=authorities-sysopr>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.4.4 Secure system DBADM authority access (Manual)

Profile Applicability:

- Level 1

Description:

The system DBADM authority defines privileges on databases in the Db2 system. It allows an administrator to manage databases across a Db2 subsystem. It is recommended that the system DBADM authority be granted to an authorized ID or a role.

Rationale:

If an account that possesses this authority is compromised or used in a malicious manner, the confidentiality, integrity, and availability of data in the Db2 subsystem will be at increased risk.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check system DBADM authority access:

```
SELECT GRANTEE, GRANTEETYPE FROM SYSIBM.SYSUSERAUTH WHERE SDBADMAUTH = 'Y';
```

Review the access list to ensure that the grants are aligned with your organization's access policies.

For external security users:

Issue the RACF `RLIST` command to list the profile that controls access to the system DBADM authority in the DSNADM class.

- Examine the universal access (UACC) and user (USER) settings for the profile. If the UACC setting is `READ` or the USER setting is `*`, consult with your security administrator for the proper value and follow the remediation steps.
- Review the access list to ensure that the permits are aligned with your organization's access policies.

Remediation:

For Db2 internal security users:

Issue the `SQL REVOKE` statement to revoke system DBADM access from any unauthorized ID or role.




For external security users:

- Issue the RACF `RALTER` command to update the UACC setting to `NONE`.
- Issue the RACF `PERMIT` command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=authorities-system-dbadm>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.4.5 Secure DATAACCESS authority access (Manual)

Profile Applicability:

- Level 1

Description:

The DATAACCESS authority defines the data access authority. It allows its holder to access and update data in user tables, views, and materialized query tables in a Db2 subsystem. It also allows its holder to execute plans, packages, functions, and procedures. It is recommended that the DATAACCESS authority be granted to an authorized ID or a role.

Rationale:

If an account that possesses this authority is compromised or used in a malicious manner, the confidentiality, integrity, and availability of data in the Db2 subsystem will be at increased risk.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check DATAACCESS authority access:

```
SELECT GRANTEE, GRANTEETYPE FROM SYSIBM.SYSUSERAUTH WHERE DATAACCESSAUTH = 'Y';
```

Review the access list to ensure that the grants are aligned with your organization's access policies.

For external security users:

Issue the RACF `RLIST` command to list the profile that controls access to the DATAACCESS authority in the DSNADM class.

- Examine the universal access (UACC) and user (USER) settings for the profile. If the UACC setting is `READ` or the USER setting is `*`, consult with your security administrator for the proper value and follow the remediation steps.
- Review the access list to ensure that the permits are aligned with your organization's access policies.

Remediation:

For Db2 internal security users:

Issue the `SQL REVOKE` statement to revoke DATAACCESS access from any unauthorized ID or role.




For external security users:

- Issue the RACF `RALTER` command to update the UACC setting to `NONE`.
- Issue the RACF `PERMIT` command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=authorities-dataaccess>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.4.6 Secure ACCESSCTRL authority access (Manual)

Profile Applicability:

- Level 1

Description:

The ACCESSCTRL authority defines the access control authority. It allows its holder to grant explicit privileges to authorization IDs or roles by issuing SQL `GRANT` statements. It enables its holder to grant privileges on most objects and resources. It is recommended that the ACCESSCTRL authority be granted to an authorized ID or a role.

Rationale:

If an account that possesses this authority is compromised or used in a malicious manner, the confidentiality, integrity, and availability of data in the Db2 subsystem will be at increased risk.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check ACCESSCTRL authority access:

```
SELECT GRANTEE, GRANTEETYPE FROM SYSIBM.SYSUSERAUTH WHERE ACCESSCTRLAUTH = 'Y';
```

Review the access list to ensure that the grants are aligned with your organization's access policies.

For external security users:

Issue the RACF `RLIST` command to list the profile that controls access to the ACCESSCTRL authority in the DSNADM class.

- Examine the universal access (UACC) and user (USER) settings for the profile. If the UACC setting is `READ` or the USER setting is `*`, consult with your security administrator for the proper value and follow the remediation steps.
- Review the access list to ensure that the permits are aligned with your organization's access policies.

Remediation:

For Db2 internal security users:

Issue the SQL `REVOKE` statement to revoke ACCESSCTRL access from any unauthorized ID or role.




For external security users:

- Issue the RACF `RALTER` command to update the UACC setting to `NONE`.
- Issue the RACF `PERMIT` command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=authorities-accessctrl>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.4.7 Secure PACKADM authority access (Manual)

Profile Applicability:

- Level 1

Description:

The PACKADM authority defines certain privileges on collections and packages. It has the package privileges on all packages in specific collections and the `CREATE IN` privilege on these collections. It is recommended that the PACKADM authority be granted to an authorized ID or a role.

Rationale:

Allowing PACKADM authority for `PUBLIC` jeopardizes the Db2 system and organizational data. If an account that possesses this authority is compromised or used in a malicious manner, Db2 data will be at increased risk.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check PACKADM authority access:

```
SELECT GRANTEE, GRANTEETYPE, NAME FROM SYSIBM.SYSRESAUTH WHERE OBTYPE = 'C'  
AND  
QUALIFIER = 'PACKADM';
```

If `PUBLIC` has PACKADM access, follow the remediation steps.

Review the access list to ensure that the grants are aligned with your organization's access policies.

For external security users:

Issue the RACF `RLIST` command to list the profile that controls access to the PACKADM authority in the DSNADM class.

- Examine the universal access (UACC) and user (USER) settings for the profile. If the UACC setting is `READ` or the USER setting is `*`, consult with your security administrator for the proper value and follow the remediation steps.
- Review the access list to ensure that the permits are aligned with your organization's access policies.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke PACKADM access from PUBLIC:

```
REVOKE PACKADM FROM PUBLIC;
```




For external security users:

- Issue the RACF `RALTER` command to update the UACC setting to `NONE`.
- Issue the RACF `PERMIT` command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=authorities-packadm>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.4.8 Secure SQLADM authority access (Manual)

Profile Applicability:

- Level 1

Description:

The SQLADM authority includes certain system privileges that allow its holder to issue SQL `EXPLAIN` statements, execute the `PROFILE` commands, run the `RUNSTATS` and `MODIFY STATISTICS` utilities on all user databases, and execute stored procedures or functions and any packages that are executed within the routines. It is recommended that the SQLADM authority be granted to an authorized ID or a role.

Rationale:

Allowing SQLADM authority for `PUBLIC` jeopardizes the Db2 system and organizational data. If an account that possesses this authority is compromised or used in a malicious manner, Db2 data will be at increased risk.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check SQLADM authority access:

```
SELECT GRANTEE, GRANTEETYPE FROM SYSIBM.SYSUSERAUTH WHERE SQLADMAUTH IN ('G', 'Y');
```

If `PUBLIC` has SQLADM access, follow the remediation steps.

Review the access list to ensure that the grants are aligned with your organization's access policies.

For external security users:

Issue the RACF `RLIST` command to list the profile that controls access to the SQLADM authority in the MDSNSM class.

- Examine the universal access (UACC) and user (USER) settings for the profile. If the UACC setting is `READ` or the USER setting is `*`, consult with your security administrator for the proper value and follow the remediation steps.
- Review the access list to ensure that the permits are aligned with your organization's access policies.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke SQLADM access from PUBLIC:

```
REVOKE SQLADM FROM PUBLIC;
```




For external security users:

- Issue the RACF `RALTER` command to update the UACC setting to `NONE`.
- Issue the RACF `PERMIT` command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=authorities-sqladm>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.4.9 Secure database DBADM authority access (Manual)

Profile Applicability:

- Level 1

Description:

The DBADM authority defines privileges on a database. Its holder can access any tables in a specific database by using SQL statements. It is recommended that the DBADM authority be granted to an authorized ID or a role.

Rationale:

Allowing DBADM authority for `PUBLIC` jeopardizes the Db2 system and organizational data. If an account that possesses this authority is compromised or used in a malicious manner, Db2 data will be at increased risk.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check DBADM authority access:

```
SELECT GRANTEE, GRANTEETYPE, NAME FROM SYSIBM.SYSDBAUTH WHERE DBADMAUTH IN ('G', 'Y');
```

If `PUBLIC` has DBADM access, follow the remediation steps.

Review the access list to ensure that the grants are aligned with your organization's access policies.

For external security users:

Issue the RACF `RLIST` command to list the profile that controls access to the DBADM authority in the DSNADM class.

- Examine the universal access (UACC) and user (USER) settings for the profile. If the UACC setting is `READ` or the USER setting is `*`, consult with your security administrator for the proper value and follow the remediation steps.
- Review the access list to ensure that the permits are aligned with your organization's access policies.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke DBADM access from PUBLIC:

```
REVOKE DBADM FROM PUBLIC;
```




For external security users:

- Issue the RACF `RALTER` command to update the UACC setting to `NONE`.
- Issue the RACF `PERMIT` command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=authorities-dbadm>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.4.10 Secure database DBCTRL authority access (Manual)

Profile Applicability:

- Level 1

Description:

The DBCTRL authority defines privileges on a database. It includes the DBMAINT privileges on a specific database. A user with the DBCTRL authority can run utilities that can change the data. It is recommended that the DBCTRL authority be granted to an authorized ID or a role.

Rationale:

Allowing DBCTRL authority for `PUBLIC` jeopardizes the Db2 system and organizational data. If an account that possesses this authority is compromised or used in a malicious manner, Db2 data will be at increased risk.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check DBCTRL authority access:

```
SELECT GRANTEE, GRANTEETYPE, NAME FROM SYSIBM.SYSDBAUTH WHERE DBCTRLAUTH IN ('G','Y');
```

If `PUBLIC` has DBCTRL access, follow the remediation steps.

Review the access list to ensure that the grants are aligned with your organization's access policies.

For external security users:

Issue the RACF `RLIST` command to list the profile that controls access to the DBCTRL authority in the DSNADM class.

- Examine the universal access (UACC) and user (USER) settings for the profile. If the UACC setting is `READ` or the USER setting is `*`, consult with your security administrator for the proper value and follow the remediation steps.
- Review the access list to ensure that the permits are aligned with your organization's access policies.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke DBCTRL access from PUBLIC:

```
REVOKE DBCTRL FROM PUBLIC;
```




For external security users:

- Issue the RACF `RALTER` command to update the UACC setting to `NONE`.
- Issue the RACF `PERMIT` command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=authorities-dbctrl>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.4.11 Secure database DBMAINT authority access (Manual)

Profile Applicability:

- Level 1

Description:

The DBMAINT authority defines certain privileges on a database. Its holder can grant the privileges on a specific database to an ID and can perform actions such as creating objects within that database. It is recommended that the DBMAINT authority be granted to an authorized ID or a role.

Rationale:

Allowing DBMAINT authority for `PUBLIC` jeopardizes the Db2 system and organizational data. If an account that possesses this authority is compromised or used in a malicious manner, Db2 data will be at increased risk.

Audit:

For Db2 internal security users:

Issue the following SQL statement to check DBMAINT authority access:

```
SELECT GRANTEE, GRANTEETYPE, NAME FROM SYSIBM.SYSDBAUTH WHERE DBMAINTAUTH IN ('G','Y');
```

If `PUBLIC` has DBMAINT access, follow the remediation steps.

Review the access list to ensure that the grants are aligned with your organization's access policies.

For external security users:

Issue the RACF `RLIST` command to list the profile that controls access to the DBMAINT authority in the DSNADM class.

- Examine the universal access (UACC) and user (USER) settings for the profile. If the UACC setting is `READ` or the USER setting is `*`, consult with your security administrator for the proper value and follow the remediation steps.
- Review the access list to ensure that the permits are aligned with your organization's access policies.

Remediation:

For Db2 internal security users:

Issue the following SQL statement to revoke DBMAINT access from PUBLIC:

```
REVOKE DBMAINT FROM PUBLIC;
```




For external security users:

- Issue the RACF `RALTER` command to update the UACC setting to `NONE`.
- Issue the RACF `PERMIT` command to remove the ID(*) and specify users or groups.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=authorities-dbmain>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.5 Encryption

This section provides guidance for encrypting Db2 data and in-memory data.

2.5.1 Ensure that data is encrypted at rest and in-flight (Manual)

Profile Applicability:

- Level 1

Description:

Db2 for z/OS uses z/OS DFSMS data set encryption to transparently encrypt Db2 data sets. DFSMS data set encryption can be used to encrypt various types of Db2 data sets including Db2-managed table space and index space data sets, log data sets, and data sets that are used by Db2 utilities.

DFSMS data set encryption uses a key label to encrypt and decrypt the data. A key label identifies a protected data key in the Integrated Cryptographic Service Facility (ICSF) key repository.

Encrypting the data sets can help with certain compliance regulations and can also protect against insider threats from within the operating system.

Rationale:

Encrypting the Db2 for z/OS data sets prevents malicious users from accessing the data.

Audit:



Check whether the Db2 data sets are encrypted by using the following options:

- The `REPORT TABLESPACESET` utility
- The `ADMIN_DS_LIST` Db2-supplied stored procedure
- For current active log data sets, the `DISPLAY LOG` command
- For current archive log data sets, the `DISPLAY ARCHIVE` command
- DFSMS interfaces such as IDCAMS LISTCAT and SMF records

Remediation:

Use the instructions in [Encrypting data with z/OS data set encryption](#) to encrypt the various types of data sets.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			

2.5.2 Secure sensitive data in memory (Manual)

Profile Applicability:

- Level 1

Description:

The `ENCRYPT_DATAKEY` built-in function can be used to encrypt data at the column level. The `DECRYPT_DATAKEY_datatype` built-in functions can be used to decrypt data. It is recommended to encrypt sensitive data at the column level.

Rationale:

If the columns are not encrypted, sensitive data can be exposed in memory.

Audit:

Identify the columns that contain sensitive data in a table. Query the columns to verify that the data is encrypted.

Remediation:

Use the `ENCRYPT_DATAKEY` and `DECRYPT_DATAKEY_datatype` built-in functions to encrypt and decrypt the columns that contain sensitive data.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=eydtbif-defining-columns-data-encrypted-using-encrypt-datakey-built-in-function>

2.6 Privacy Controls

This section provides guidance for enabling row permissions and column masks.

2.6.1 Secure row access using row permission (Manual)

Profile Applicability:

- Level 1

Description:

A row permission defines a row access control rule that specifies the conditions under which a user, group, or role can access rows of data in a table. It is recommended to enable row permission for tables that contain sensitive data and allow access to users according to your organization's security and database access policies. Also, review the access control rule regularly for gaps.

Rationale:

Lack of row permission controls can allow all authorized users access to all the rows in the table. This lack of control can increase the risk of privacy concerns with your organization's protected data.

Audit:

Issue the following SQL statement and review the output to verify that the row permissions are enabled and that they comply with your organization's existing security policy:

```
SELECT * FROM SYSIBM.SYSCONTROLS WHERE CONTROL_TYPE = 'R';
```




Remediation:

Issue the `SQL CREATE PERMISSION` statement to create a row permission for row access control according to your organization's policy. Issue the `SQL ALTER TABLE` statement with the `ACTIVATE ROW ACCESS CONTROL` option to activate the row permissions.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=masks-row-permission>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

2.6.2 Secure column values using column mask (Manual)

Profile Applicability:

- Level 1

Description:

A column mask defines a column access control rule that specifies the conditions under which a user, group, or role can receive the masked values that are returned for a column. Enabling column masking is recommended for tables that contain sensitive data to mask out column values that are returned, according to your organization's security and database access policies. Also, review the access control rule regularly for gaps.

Rationale:

Lack of masking the column values can allow all authorized users access to all the column values in the table. This lack of control can increase the risk of privacy violations with your organization's protected data.

Audit:

Issue the following SQL statement and review the output to verify that column masks are enabled and that they comply with your organization's existing security policy:

```
SELECT * FROM SYSIBM.SYSCONTROLS WHERE CONTROL_TYPE = 'M';
```




Remediation:

Issue the `SQL CREATE MASK` statement to create a column mask for column access control according to your organization's policy. Issue the `SQL ALTER TABLE` statement with the `ACTIVATE COLUMN ACCESS CONTROL` option to activate the column masks.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=masks-column-mask>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

3 Audit

This section describes how to enable auditing to determine whether the security plan is working and to audit administrator authority access.

3.1 Audit considerations

The audit trace collects information about Db2 security controls and can be used to ensure that data access is allowed only for authorized purposes. Audit traces can help trigger events for changes to data objects, table DML, utilities, and user access.

3.1.1 Ensure that audit tracing is enabled during Db2 start up (Manual)

Profile Applicability:

- Level 1

Description:

It is recommended that audit traces that are critical for protecting the security of the system and data should be specified to start during Db2 start up. You can specify that audit traces are started during Db2 start up by using either of the following options:

- Specifying the audit classes by using the `AUDIT TRACE` subsystem parameter
- Defining audit policies by specifying a `SYSAUDITPOLICIES - DB2START` column value of 'Y', 'S', or 'T'

Rationale:

Enabling audit traces to audit critical information is crucial for securing and discovering issues within your databases. Lack of critical audit data can cause issues to go undiscovered. Lack of audit tracing might prevent you from providing proof of compliance with security laws, regulations, and other requirements.

Audit:

1. Run the DSNTEJ6Z job to obtain the current value of the `AUDITST` subsystem parameter. Verify that the value is set to the list of classes that are required to be started during Db2 start up.
2. Issue the following SQL statement to verify whether the required audit policies are defined to be started during Db2 start up:

```
SELECT * FROM SYSIBM.SYSAUDITPOLICIES WHERE DB2START IN ('Y','S','T');
```




Remediation:

1. Edit the DSNTIJUZ job and set the `DSN6SYSP.AUDITST` subsystem parameter to the required list of classes. Submit DSNTIJUZ to assemble the subsystem parameter. The specified list of classes will be automatically started during Db2 restart.
2. Define new audit policies or update existing audit policies to start automatically during Db2 start up by specifying the `DB2START` column value of 'Y', 'S', or 'T'.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysauditpolicies>
2. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=policy-creating-activating-audit-policies>
3. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=panel-audit-trace-field-auditst-subsystem-parameter>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

3.1.2 *Ensure that critical audit traces are always enabled* (Manual)

Profile Applicability:

- Level 1

Description:

Audit traces that are critical for protecting the security of the system and data should not be stopped without special permission from an external security product such as RACF or without using security administrator authority.

Tamper-proof audit policies, which require special authorization from an external security product such as RACF to modify or stop, are provided for this purpose. They are identified as having the `DB2START` column as 'T' in the SYSAUDITPOLICIES table.

Secure audit policies are another type of audit policy that can be stopped only by the SECADM authority. They are identified as having the `DB2START` column as 'S' in the SYSAUDITPOLICIES table.

Both the tamper-proof and secure policies are started automatically during Db2 start up.

Rationale:

If critical audit policies are stopped, important audit data could be lost. It's crucial that these policies can be stopped or modified only by a user with the required permission to the audit policy profile in an external security product, such as RACF or the SECADM authority. Loss of critical audit data can put the processing environment and organizational data at risk.

Audit:

Issue the following SQL statement to verify that tamper-proof or secure audit policies are defined to audit critical data:

```
SELECT AUDITPOLICYNAME FROM SYSIBM.SYSAUDITPOLICIES WHERE DB2START IN ('T','S');
```




Remediation:

According to your organization's policies, define new audit policies or update existing audit policies to be defined as secure or tamper-proof by specifying the `DB2START` column value of 'S', or 'T'. For tamper-proof audit policies, perform additional steps in RACF, as required.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=db2-audit-policy>
2. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysauditpolicies>
3. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=policy-creating-activating-audit-policies>
4. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=policy-updating-tamper-proof-audit-policies>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

3.1.3 Ensure that authorization failures are audited (Manual)

Profile Applicability:

- Level 1

Description:

Audit trace CLASS 1 (IFCID140) audits access attempts that were denied due to inadequate authorization. If this audit traces is not enabled, issues can go undiscovered, and compromises and other incidents can occur without being quickly detected.

Rationale:

Auditing authorization failures can help detect unauthorized activities quickly to avoid system or data being compromised. Undetected failed authorization attempts can increase risk to the system and data.

Audit:

Display the IFCID140 trace:

```
-DISPLAY TRACE (AUDIT)
```

Review the output to make sure IFCID140 trace is enabled.




Remediation:

Enable IFCID140 trace either by issuing the `START TRACE` command or through the audit policy `CHECKING` category.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=commands-display-trace-db2>
2. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=trace-audit-classes>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

3.1.4 Enable audit policies to audit installation system administrator and system operator access (Manual)

Profile Applicability:

- Level 1

Description:

Installation system administrators and installation system operators perform Db2 installation and migration. The installation system administrator role also includes most of the administrative authority, which can perform important tasks such as starting and stopping Db2, controlling traces, accessing all data, and granting and revoking privileges from other users.

Rationale:

Auditing tasks performed by an installation system administrator and installation system operator can help detect unauthorized or malicious activities intended to do harm to Db2 data or the processing environment. Tasks performed by the installation system administrator or installation system operator could impact the Db2 system and organization data. Such activities must be closely monitored.

Audit:

Issue the following SQL statement to verify that audit policy is enabled to audit installation SYSADM, installation SYSOPR, or all authorities in `SYSADMIN` category:

```
SELECT AUDITPOLICYNAME FROM SYSIBM.SYSAUDITPOLICIES WHERE SYSADMIN IN ('I', 'R', '*');
```




Remediation:

Enable AUDITPOLICIES with the `SYSADMIN` category to audit installation SYSADM and installation SYSOPR authorities.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysauditpolicies>
2. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=policy-auditing-use-administrative-authority>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

3.1.5 Enable auditing of system administrator access (Manual)

Profile Applicability:

- Level 1

Description:

System administrator authorities perform system administrator tasks and include administrative authorities such as SYSADM, SYSCTRL, and SYSOPR. The SYSADM authority has access to all data.

Rationale:

Auditing tasks that are performed by system administrators can help detect unauthorized or malicious activities intended to do harm to Db2 data or the processing environment. Tasks performed by system administrators can impact the Db2 system and organizational data. Such activities must be closely monitored.

Audit:

For Db2 internal security users:

Issue the following SQL statement to verify that the audit policy is enabled to audit SYSADM, SYSCTRL, SYSOPR or all authorities in `SYSADMIN` category:

```
SELECT AUDITPOLICYNAME FROM SYSIBM.SYSAUDITPOLICIES  
WHERE SYSADMIN IN ('L','O','S','*');
```

For external security users:

Ensure that SMF 80 trace is `ON` and the Db2 administrator profiles in RACF have `AUDIT(ALL)` specified.

Remediation:

For Db2 internal security users:

Enable `AUDITPOLICIES` with the `SYSADMIN` category to audit SYSADM, SYSCTRL, and SYSOPR authorities.




For external security users:

Specify `AUDIT(ALL)` for the Db2 administrator profiles in RACF and start SMF 80 trace.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysauditpolicies>
2. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=policy-auditing-use-administrative-authority>
3. <https://www.ibm.com/docs/en/zos/2.5.0?topic=records-record-type-80-racf-processing-record>
4. <https://www.ibm.com/docs/en/zos/2.5.0?topic=syntax-rdefine-define-general-resource-profile>
5. <https://www.ibm.com/docs/en/zos/2.5.0?topic=guide-setting-listing-audit-controls>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

3.1.6 Enable auditing of database administrator access (Manual)

Profile Applicability:

- Level 1

Description:

Database administrators manage databases and objects in a database or all databases in the system. Security administrators manage security objects and access control.

Rationale:

Auditing tasks performed by database administrators and security administrators can help detect unauthorized or malicious activities that are intended to do harm to Db2 data or the processing environment.

Audit:

For Db2 internal security users:

Issue the following SQL statement to verify that the audit policy is enabled to audit system DBADM, DATAACCESS, ACCESSCTRL, SECADM, database DBADM, DBCTRL, and DBMAINT authorities, or all authorities in the `DBADMIN` category:

```
SELECT AUDITPOLICYNAME FROM SYSIBM.SYSAUDITPOLICIES  
WHERE DBADMIN IN ('B','C','D','E','G','M','T','*');
```

For external security users:

Ensure that SMF 80 trace is `ON` and the Db2 administrator profiles in RACF have `AUDIT(ALL)` specified.

Remediation:

For Db2 internal security users:

Enable `AUDITPOLICIES` with the `DBADMIN` category to audit system DBADM, DATAACCESS, ACCESSCTRL, SECADM, database DBADM, DBCTRL, and DBMAINT authorities.




For external security users:

Specify `AUDIT(ALL)` for the Db2 administrator profiles in RACF and start SMF 80 trace.

References:

1. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=tables-sysauditpolicies>
2. <https://www.ibm.com/docs/en/db2-for-zos/13?topic=policy-auditing-use-administrative-authority>
3. <https://www.ibm.com/docs/en/zos/2.5.0?topic=records-record-type-80-racf-processing-record>
4. <https://www.ibm.com/docs/en/zos/2.5.0?topic=syntax-rdefine-define-general-resource-profile>
5. <https://www.ibm.com/docs/en/zos/2.5.0?topic=guide-setting-listing-audit-controls>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	Installation and Configuration		
1.1	Installation protection		
1.1.1	Ensure that Db2 system data sets are protected (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2	Ensure that Db2 USS file system is protected (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3	Secure installation process (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.2	Security system parameters configuration		
1.2.1	Ensure that RACF changes are accepted immediately (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2	Ensure that authorization is enabled (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.3	Ensure that the default authorization IDs are changed from the installation defined (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.4	Ensure that generic error codes are returned for remote security errors (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.5	Separate security administration from system administration (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2	Secure the database		
2.1	Secure database access		
2.1.1	Ensure subsystem access is protected (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Ensure secure authentication is enabled for remote access (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.3	Secure access by using Multi-Factor Authentication (MFA) (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.1.4	Secure all remote connections by using SSL (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.5	Secure remote connections by using TCP/IP Network Access control with the RACF SERVAUTH class (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.6	Secure connections by using trusted contexts (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.7	Secure object ownership by using Db2 roles (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.8	Secure application access by using package controls (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.9	Ensure that grant authorization IDs are defined in RACF (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Secure database catalog access		
2.2.1	Ensure that access to the catalog tables in the communications database (CDB) is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	Ensure that access to SYSIBM.SYSAUDITPOLICIES is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	Ensure that access to SYSIBM.SYSCOLAUTH is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.4	Ensure that access to SYSIBM.SYSCOLUMNS is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.5	Ensure that access to trusted context tables is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.6	Ensure that access to SYSIBM.SYSCONTROLS is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.7	Ensure that access to SYSIBM.SYSDATABASE is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.8	Ensure that access to SYSIBM.SYSDBAUTH is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.2.9	Ensure that access to dynamic query-related tables is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.10	Ensure that access to SYSIBM.SYSINDEXES is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.11	Ensure that access to SYSIBM.SYSOBJROLEDEP is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.12	Ensure that access to package-related tables is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.13	Ensure that access to SYSIBM.SYSPACKAUTH is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.14	Ensure that access to SYSIBM.SYSPARMS is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.15	Ensure that access to SYSIBM.SYSPLAN is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.16	Ensure that access to SYSIBM.SYSPLANAUTH is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.17	Ensure that access to SYSIBM.SYSQUERY is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.18	Ensure that access to SYSIBM.SYSRESAUTH is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.19	Ensure that access to SYSIBM.SYSROLES is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.20	Ensure that access to SYSIBM.SYSROUTINEAUTH is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.21	Ensure that access to SYSIBM.SYSROUTINES is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.22	Ensure that access to SYSIBM.SYSROUTINESTEXT is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.2.23	Ensure that access to SYSIBM.SYSSCHEMAAUTH is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.24	Ensure that access to SYSIBM.SYSSEQUENCEAUTH is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.25	Ensure that access to SYSIBM.SYSSEQUENCES is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.26	Ensure that access to SYSIBM.SYSSTMT is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.27	Ensure that access to SYSIBM.SYSSTOGROUP is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.28	Ensure that access to SYSIBM.SYSTABAUTH is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.29	Ensure that access to SYSIBM.SYSTABLES is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.30	Ensure that access to SYSIBM.SYSTABLESPACE is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.31	Ensure that access to SYSIBM.SYSTRIGGERS is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.32	Ensure that access to SYSIBM.SYSUSERAUTH is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.33	Ensure that access to variable-related tables is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.34	Ensure that access to SYSIBM.SYSVARIABLEAUTH is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.35	Ensure that access to SYSIBM.SYSVIEWS is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Secure database pseudo catalog tables		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.1	Ensure that access to the program authorization table is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	Ensure that access to the REST services definition table is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3	Ensure that access to the query accelerator tables is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.4	Ensure that access to profile tables is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.5	Ensure that access to SQL Data Insights tables is restricted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Secure database authorities		
2.4.1	Secure SYSADM authority access (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2	Secure SYSCTRL authority access (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.3	Secure SYSOPR authority access (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.4	Secure system DBADM authority access (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.5	Secure DATAACCESS authority access (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.6	Secure ACCESSCTRL authority access (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.7	Secure PACKADM authority access (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.8	Secure SQLADM authority access (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.9	Secure database DBADM authority access (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.10	Secure database DBCTRL authority access (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.11	Secure database DBMAINT authority access (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Encryption		
2.5.1	Ensure that data is encrypted at rest and in-flight (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.5.2	Secure sensitive data in memory (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.6	Privacy Controls		
2.6.1	Secure row access using row permission (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.6.2	Secure column values using column mask (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3	Audit		
3.1	Audit considerations		
3.1.1	Ensure that audit tracing is enabled during Db2 start up (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2	Ensure that critical audit traces are always enabled (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3	Ensure that authorization failures are audited (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.4	Enable audit policies to audit installation system administrator and system operator access (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.5	Enable auditing of system administrator access (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.6	Enable auditing of database administrator access (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: Change History

Date	Version	Changes for this version
Jun 1, 2022	1.0.0	Draft published for consensus review
Jun 17, 2022	1.0.0	Published