Auditee's Guide - CheckAud for SAP Systems 21.0

Document version: AG.CASA.21.0.2003.01

A product of IBS Schreiber GmbH
# Table of contents

## Chapter I Usage of the Auditee's Guide CheckAud 21.0

I - 1 Live data presentation of CheckAud 21.0 ................................................................. 6
I - 2 Authorization audit with CheckAud 21.0 ................................................................. 6

## Chapter II Rights required in the SAP system

II - 1 Table set AUTH ............................................................................................................. 8
II - 2 Table set IBS_AUTH_ADVANCED ............................................................................ 8
II - 3 Table set IBS_BW ....................................................................................................... 9
II - 4 Table set IBS_CO ....................................................................................................... 9
II - 5 Table set IBS_FI ....................................................................................................... 9
II - 6 Table set IBS_GDPR ................................................................................................ 10
II - 7 Table set IBS_MM .................................................................................................... 10
II - 8 Table set IBS_HCM ............................................................................................... 10
II - 9 Table set IBS_ISU .................................................................................................... 10
II - 10 Table set IBS_SD .................................................................................................... 11
II - 11 Table set IBS_SYSTEM ........................................................................................ 11
II - 12 Authorizations for reading parameter values .......................................................... 11
II - 13 Authorizations for reading the default org level values ......................................... 12
II - 14 Authorization for reading anonymized user statistics .......................................... 12
II - 15 Predefined SAP role for the RFC interface user (Scan-User) ................................. 12

## Chapter III Installing CheckScan 21.0

13

## Chapter IV CheckScan 21.0

IV - 1 Creating a new system connection .......................................................................... 20
  1.1 Select the table sets ................................................................................................... 21
  1.2 Reading out parameters .......................................................................................... 22
  1.3 Reading out default values for org levels .............................................................. 23
IV - 2 Creating a snapshot ............................................................................................... 24
Chapter I - Usage of the Auditee's Guide CheckAud 21.0
I Usage of the Auditee's Guide CheckAud 21.0

This document describes the technical preliminaries for a scan with CheckAud 21.0 in preparation for a live data demonstration of CheckAud 21.0 or for an authorization audit.

I - 1 Live data presentation of CheckAud 21.0

What you will get
- you'll get a live summary, which security gaps you may have concerning your SAP authorization concept
- this audit will take about 2 hours and will take place at your site
- we'll check, if your authorization concept fits legal or your internal audit requirements
- this audit will be done by a qualified consultant
- you'll learn about the advantages using the audit software CheckAud®
- there are no obligations

How does it work
- you make an appointment with our sales department
- you prepare the needed SAP data using our CheckAud® scan module
- you deliver the created SAP data during the appointment at your site, there is no need to send us any information earlier
- during the presentation, our consultant will use the created SAP data for analysis using CheckAud®
- with predefined authorization checks our consultant will prepare results and reports including a risk assessment and possible solutions
- you'll receive detailed results in form of reports and tabular listings
- after the presentation, all used and created data referring your company will be deleted safely

In preparation for the live presentation of CheckAud® it is necessary, that all data will be created before the actual appointment!

I - 2 Authorization audit with CheckAud 21.0

For preparation of an authorization audit please follow the steps below to install the Scan module and to create a snapshot. One of our consultants will contact you in time to provide you with detailed information.
Chapter II - Rights required in the SAP system
## Rights required in the SAP system

### II - 1 Table set AUTH

Users log onto the SAP system with CheckScan 21.0 via the RFC interface. Note that CheckScan supports only release level 7.00 or later of the software component SAP_BASIS. Users need a user account (system user) with the following rights:

#### Authorization object: S_RFC

**Activity:** 16

**RFC_NAME:**
- AUTH_TRACE_GET_USOBHASH
- DDIF_FIELDINFO_GET
- EM_GET_NUMBER_OF_ENTRIES
- GET_SYS_COMP_REL
- RFCPING
- RFC_FUNCTION_SEARCH
- RFC_GET_FUNCTION_INTERFACE
- RFC_METADATA_GET
- RFC_METADATA_GET_TIMESTAMP
- RFC_PING
- RFC_READ_TABLE
- RFC_SYSTEM_INFO
- SYSTEM_RESET_RFC_SERVER

**RFC_TYPE:** FUNC

#### Authorization object: S_TABU_NAM

**Activity:** 03

**Table:**
- AGR_1016
- AGR_AGRS
- AGR_DEFINE
- AGR_FLAGS
- AGR_TEXTS
- AGR_USERS
- CVERS
- CVERS_REF
- DD02L
- DD02T
- DD03L
- DD03M
- DD03T
- DD04T
- DEVACCESS
- PRGN_CUST
- T055
- T055F
- T055G
- T055T
- T77S0
- TAPPL_LOCK
- TDDAT
- TOBC
- TOBCT
- TOBJ
- TOBJ_CHK_CTRL_R
- TOBJ_OFF
- TRDIR
- TSTC
- TSTCT
- USER_ADDR
- USGRP_USER
- USGRPT
- USOBAUTHINACTIVE
- USORG
- USR_CUST
- USR02
- USR06
- USR10
- USR11
- USR13
- USR21
- USREFUS
- UST04
- UST10C
- UST10S
- UST12
- WDY_COMPONENT

1 As per SAP Note 460089 (Minimum authorization profile for external RFC programs), authorization for the function module SYSTEM_RESET_RFC_SERVER is always required

https://launchpad.support.sap.com/#/notes/460089

To read more table sets in addition to the standard table set AUTH, separate authorizations are required for each individual table set in the SAP system. The permissions required for each table set are listed below:

### II - 2 Table set IBS_AUTH_ADVANCED

#### Authorization object: S_TABU_NAM

**Activity:** 03

**Table:**
II - 3  Table set IBS_BW

Authorization object: S_TABU_NAM
Activity: 03
Table: RSECBIAU, RSECTXT, RSECUSERAUTH

II - 4  Table set IBS_CO

Authorization object: S_TABU_NAM
Activity: 03
Table: CEPC, CSKS, TKA01, TKA02

II - 5  Table set IBS_FI

Authorization object: S_TABU_NAM
Activity: 03
Table: FM01, FM01T, NRIV, T001, T001B, T003, T003T, T004, T004T, T010P, T014T, T043, T880, TGSB, TGSBT, TNROT, TNRO
## Chapter II - Rights required in the SAP system

### II - 6 Table set IBS_GDPR

<table>
<thead>
<tr>
<th>Authorization object: S_TABU_NAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity: 03</td>
</tr>
<tr>
<td>Table:</td>
</tr>
<tr>
<td>SX_C_ATTR, SX_C_CLASS, SX_C_EXIT, SX_X_ATTR_T, SXF_SW_BF, SXF_SWITCH_STATE, SXF_SWITCH_T, T77PADDUR_DEF, T77PADDUR_KEY, T77PADDURATION</td>
</tr>
</tbody>
</table>

### II - 7 Table set IBS_MM

<table>
<thead>
<tr>
<th>Authorization object: S_TABU_NAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity: 03</td>
</tr>
<tr>
<td>Table:</td>
</tr>
<tr>
<td>T001L, T024E, T024W, T025, T030, T134</td>
</tr>
</tbody>
</table>

### II - 8 Table set IBS_HCM

<table>
<thead>
<tr>
<th>Authorization object: S_TABU_NAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity: 03</td>
</tr>
<tr>
<td>Table:</td>
</tr>
</tbody>
</table>

### II - 9 Table set IBS_ISU

<table>
<thead>
<tr>
<th>Authorization object: S_TABU_NAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity: 03</td>
</tr>
<tr>
<td>Table:</td>
</tr>
<tr>
<td>EDSC, EPREI, ETRF, ETTA, TE069, TE218, TE265, TE408, TE669</td>
</tr>
</tbody>
</table>
II - 10 Table set IBS_SD

Authorization object: S_TABU_NAM
Activity: 03
Table:
TVKO, TVKOT, TVKWZ, TVTW, TVTWT

II - 11 Table set IBS_SYSTEM

Authorization object: S_TABU_NAM
Activity: 03
Table:
ADIRACCESS, CCCFLOW, DD02L, DD09L, DLV_SYSTC, ORGCRACT, PAT03, RFCDES,
RFCDOC, RFCSYSACL, RFCTRUST, RSAUPROF, SEC_POLICY_ATTR, SEC_POLICY_RT,
SXPGCOSTAB, T000, TADIR, TBRG, TBRG_AUTH, TBRG_AUTHT, TBRGT, TCDOB , TMSCSYS,
TMSPCONF, TPLOG, TRNSPACE, TRNSPACETT, USR01, USR05, USR40, USR41_MLD

II - 12 Authorizations for reading parameter values

This function will only be available since SAP Releases 7.40!

Authorization object: S_RFC
Activity: 16
RFC_NAME: PFL_GET_SERVER_PARAM_VALUES
RFC_TYPE: FUNC

Authorization object: S_TABU_NAM
Activity: 03
Table:
DOKIL, DOKTL, TPFET, TPFHT, TPFID

Authorization object: S_RZL_ADM
Activity: 03
Chapter II - Rights required in the SAP system

II - 13 Authorizations for reading the default org level values

<table>
<thead>
<tr>
<th>Authorization object: S_TABU_NAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity: 03</td>
</tr>
<tr>
<td>Table:</td>
</tr>
</tbody>
</table>

II - 14 Authorization for reading anonymized user statistics

<table>
<thead>
<tr>
<th>Authorization object: S_RFC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity: 16</td>
</tr>
<tr>
<td>RFC_NAME: SWNC_COLLECTOR_GET_AGGREGATES</td>
</tr>
<tr>
<td>RFC_TYPE: FUNC</td>
</tr>
</tbody>
</table>

II - 15 Predefined SAP role for the RFC interface user (Scan-User)

In the customer section of the www.checkaud.de website, you can download a predefined role for scan users. This SAP role includes the necessary authorizations for the SAP communication user that is used for scanning the SAP systems to be checked. The authorizations are limited to access of remote-capable SAP function modules, as well as to the SAP tables that are relevant for authorization evaluation.

The customer section on www.checkaud.de provides the individual SAP roles for the newly added table sets in CheckScan for download.

Note:
Note that older SAP systems do not offer any functions for maintaining function modules. The authorizations are based on function groups. The roles provided in the customer area on www.checkaud.de are based on the provision of authorizations via function modules. If you experience problems when creating snapshots in older SAP systems, check whether the roles that you imported are complete. It is entirely possible that the imported roles were not created completely in the SAP system. In this case, we recommend that you use the authorizations via the function groups.
Chapter III - Installing CheckScan 21.0
III Installing CheckScan 21.0

The data capture module from the SAP system, the scan module, is provided separately as an installation package. Proceed as follows for the installation:

You can select your desired language for the installation:

Choose Next to begin the installation with the setup wizard

Confirm the notes to the actual release with Next:
Chapter III - Installing CheckScan 21.0

Figure 3 - Notes to the release

Select the radio button *I accept the terms in the licensing agreement*

Figure 4 - Accept license agreements

Choose *Next*

The following dialog asks, how the installation should be executed, only for the logged on user or for all users on this computer:
You can select the installation path of your choice. As a default option, the scan module is installed under:

`C:\Program Files\CheckAud GRC Software\for SAP Systems\CheckScan`

Choose Install to start the installation.
Chapter III - Installing CheckScan 21.0

Figure 7 - Completing the preparations for the installation

Figure 8 - Performing the installation

Successfully completed CheckScan installation:

Figure 9 - Installation complete
Chapter IV - CheckScan 21.0
Creating a new system connection

**Note:** To create system connections, you need detailed information about the SAP source systems to be exported (TCP/IP address, DNS address or SAProuter string, message server, server group, client, system number, etc.). This information should be available from SAP Basis administration.

You can use the button ![Create new system](image) to create a new connection to a SAP source system. Previously created source systems can be exported or imported using the ![Import/Export](image) button. In this way, information about SAP source systems can be exchanged between different scan module installations.

This button can still be used to load the `SAPLOGON.INI` of an existing SAP LogOn installation. In the process, the connection information available in `SAPLOGON.INI` is copied and must only be supplemented by the client or the SAP communication user's logon information.

The following dialog box for establishing a new system connection is displayed:

**Figure 10 - Entering the connection information for an SAP system**

<table>
<thead>
<tr>
<th>Description</th>
<th>User-defined description of the source system to be created</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Choose between a connection via application service or groups/server selection</td>
</tr>
<tr>
<td>Server</td>
<td>TCP/IP address or DNS address of the SAP host</td>
</tr>
<tr>
<td>SAProuter-String</td>
<td>Alternative connection via the SAProuter string</td>
</tr>
<tr>
<td>System number</td>
<td>Instance number of the SAP source system</td>
</tr>
<tr>
<td>System-ID</td>
<td>System designation of the SAP source system</td>
</tr>
<tr>
<td>Client</td>
<td>Client to be read out from the SAP source system</td>
</tr>
</tbody>
</table>
Credentials
Name and password of the SAP communication user for logging the scan module onto the source system (alternatively, the SAP standard user saved to the settings can be enabled here using the flag)

Safe password
As long as this flag has not been enabled, each time a snapshot is created, a prompt for the SAP communication user's password will appear

You can use the button 🔄Test to check whether it is possible to connect to the source system using the saved information.

IV - 1.1 Select the table sets

On the 🔄Table sets tab, you can select additional table sets that are also relevant to this system connection in addition to the mandatory table set AUTH. The table sets:

- IBS_AUTH_ADVANCED,
- IBS_BW,
- IBS_FI,
- IBS_GDPR
- IBS_HCM,
- IBS_ISU,
- IBS.MM,
- IBS_SD and
- IBS_SYSTEM

are provided as predefined additional options. Your own table sets are displayed dynamically in the main menu item Table Sets (Tabellen-Sets) and on this tab.

The figure below shows the additional selection of the table set IBS_AUTH_ADVANCED:
Use the Save button to save the new system connection. In the Table Set column in the SAP source system overview, you can see which table sets have been enabled.

**IV - 1.2 Reading out parameters**

In addition to table sets, the Table sets tab also contains additional options for the information to be read out:
To check the parameters of an SAP system in CheckAud, the parameters must be read out. Readouts of parameter values are activated by default in CheckScan. As well as the existing authorizations for the AUTH table set, additional authorizations are required to read out the parameter values. You can read out system parameters only with SAP Release 7.40 or later. For older releases, it is not possible to read out parameter evaluations in CheckAud even when the option is set.

**IV - 1.3 Reading out default values for org levels**

In addition to table sets, the tab also contains additional options for the information to be read out:

![Figure 13 - Reading out default values for org levels](image)

To be able to use the default values for organization levels (e.g. for company code BUKRS) in CheckAud, these values must also be read out. Readouts of the default values for org levels are activated by default in CheckScan. Additional authorizations are required on top of the existing authorizations for the AUTH table set.

**Note**: If the readout of the SAP system results in longer runtimes, this option for reading out the org levels can be disabled to improve the runtimes. As a result, however, the default values for org levels cannot be provided during the evaluation and must be entered manually.
Creating a snapshot

To create snapshots of the required SAP source systems, one or more system connections must be marked with a flag in the list or group view:

If several systems are marked for snapshots, the scan module reads them out sequentially and the relevant snapshots are saved in the target directory listed.

If necessary, the snapshots can also be encrypted using a password. This password is requested when the snapshot is imported to the evaluation module database.

Choose the button to create the snapshot. A dialog box for saving the snapshot file opens:
The name of the file to be saved is composed as follows:

SystemID_Client_Date_Time.casnapshot
After you start the scan, the system selection is deactivated and the lower area displays the tables to be scanned and the estimated time required to complete the scan. Once the scan is successfully completed, a results window is displayed:

![Snapshot created](image)

**Figure 18 - Results window for the successful scan**

**Note:**

A ![icon] icon in the results window indicates that some optional tables were not included in the snapshot. However, the snapshot was created successfully. If you place the mouse cursor on the icon that is displayed, a window appears that shows the tables that were skipped in the associated table set.

Please be prepared to deliver the snapshot file (*.casnapshot) during the presentation via USB flash drive.