## Introduction

Securing business systems, especially SAP systems, is vital in today's dynamic technology environment. Essential to the operations of many companies, SAP systems safeguard valuable data and manage critical business processes. However, they are exposed to a constantly evolving threat landscape, making appropriate risk assessment and management essential for any security strategy.

Having valuable information is vital for good control, monitoring the state of security, and preventing the delivery of privileges that may constitute risks. CentinelBox delivers this information in more than 100 reports, of which we have selected the most used and chosen by our clients.

Information for Managers and Executives

Understanding security concepts has never been so simple: with three reports, every executive or manager without needing to know SAP System security concepts will be able to identify if there are problems that need to be resolved:

First report:
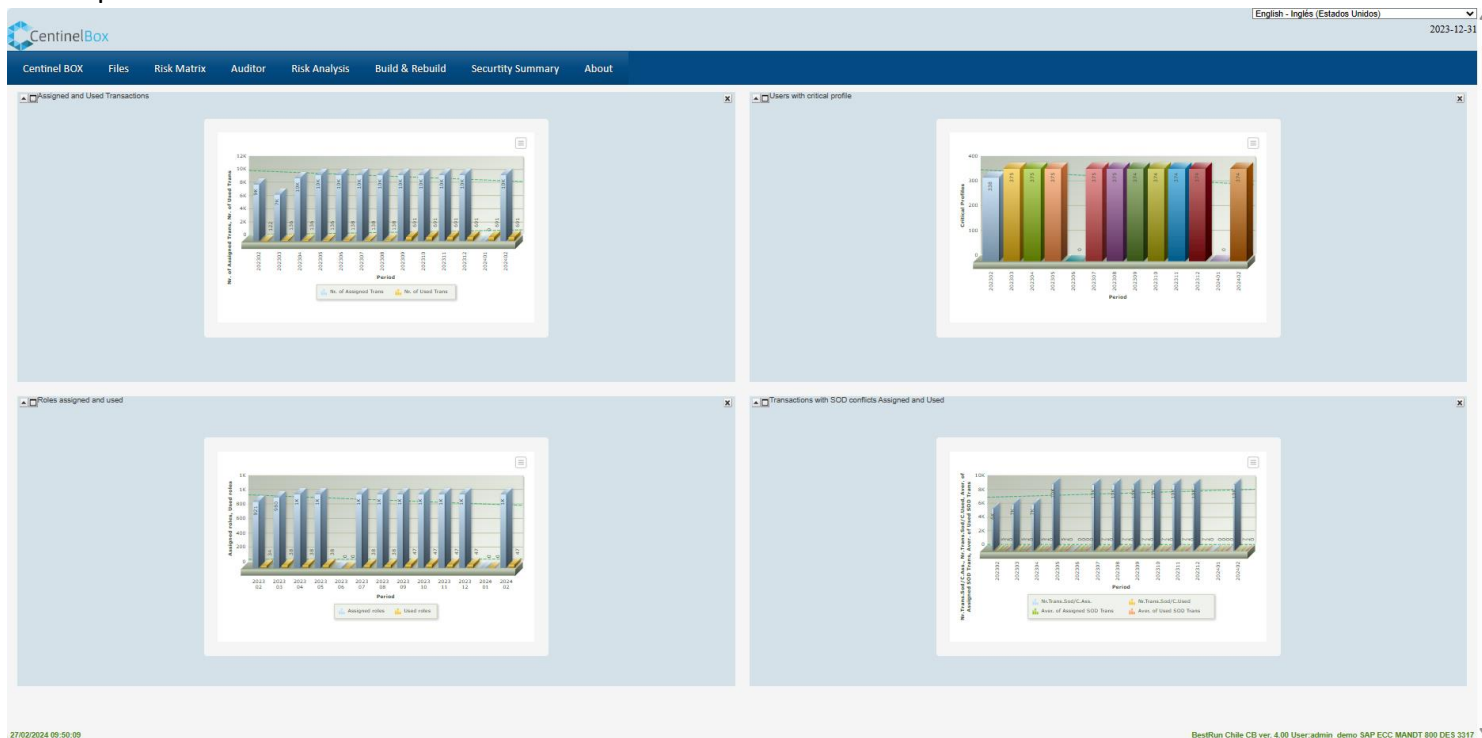
The first graph shows the gap between the number of transactions allocated and those used. This difference should not be more than 30%.

The graph of user accounts with a critical profile shows the number of these assigned, which should be zero!

The graph of assigned roles compared to those used should not present a gap greater than 30%.

The graph of assigned SOD conflicts compared to those used can show a real problem due to the risks they entail and the undesired effect of the over-allocation of transactions shown in the first graph.

CentinelBox

Second report:

FAST CHECKLIST with 18 controls, in which the complexity of the technical terminology does not matter; only if there are values in red should you worry and ask for solutions!

	FAST CHECKLIST			2024/02 al 27-02-2024	
			⬇ Export ▾		
Id.	Checklist	Qty	Observation		Select
1	New user accounts		No new accounts created in the period		⊕
2	New user accounts without roles	389			⊕
3	Non-current user accounts with assigned roles	267			⊕
4	User accounts not valid not blocked	326			⊕
5	New user accounts without logging into the system	2.126			⊕
6	User accounts with critical profiles assigned with use of Trans in dialogue	11			⊕
7	User accounts with critical authorization objects assigned	195			⊕
8	System update		There are no modification(s) to the system		⊕
9	Assigned transactions		Review transaction usage by range		⊕
10	Used transactions		Review transaction usage by range		⊕
11	Transactions with SOD Conflict assigned		Review Conflicting SOD Transaction Allocation by range		⊕
12	Used transactions with SOD conflicts		Review Conflicting Transaction Usage SOD by range		⊕
13	Assigned Critical Transactions		Review allocation of critical transactions by range		⊕
14	Used Critical transactions used		Review usage of critical transactions by range		⊕
15	Roles assigned without prior risk simulation		Role assignment is not detected without risk simulation		⊕
16	Non-current roles used		Use of not valid roles is not detected		⊕
17	Profiles assigned without roles and transactions used		Use of transactions is not detected.There are 7155 assigned profiles without their roles.		⊕
18	New customer transactions (Y/Z)		No new transactions are detected in the period.		⊕

Go to [1] View [20 ▾] ⏮ ◀ [1] ▶ ⏭ [1 to 18 of 18]

Third report:

Comparative table of critical variables of system security management, in which the complexity of the technical terminology does not matter; only if there are values in red should you worry and ask for solutions!

	Period Comparison Chart												27-02-2024
			⚙ Exportar ▾										Back
	Control	02/2024	01/2024	12/2023	11/2023	10/2023	09/2023	08/2023	07/2023	06/2023	05/2023	04/2023	03/2023
1	Number of Current Users	3.860	0	3.860	3.860	3.863	3.865	3.866	3.866	0	3.867	3.868	3.868
2	Number of non-current users	342	0	342	342	339	337	336	336	0	335	334	334
3	Total Assigned Transactions	10.109	0	10.109	10.109	10.109	10.109	10.109	10.109	0	10.109	9.655	7.125
4	Total Used Transactions	691	691	691	691	691	691	138	138	136	136	136	136
5	Average Assigned Transactions	28	0	28	28	27	27	27	27	0	27	27	27
6	Average UsedTransactions	1	0	1	1	1	1	0	0	0	0	0	0
7	Roles with SOD conflicts assigned	511	0	511	511	511	511	511	511	0	513	373	373
8	Transactions with SOD conflicts assigned (total)	9.569	0	9.569	9.569	9.569	9.569	9.569	9.569	0	9.673	6.744	6.744
9	Transactions with SOD conflicts assigned (different)	3.742	0	3.742	3.742	3.742	3.742	3.742	3.742	0	3.778	2.473	2.473
10	Average Transactions with SOD conflicts assigned	2	0	2	2	2	2	2	2	0	2	2	2
11	Roles with SOD conflicts used	7	0	7	7	7	7	7	7	0	5	5	5
12	Transactions with SOD conflicts used (total)	7	0	7	7	7	7	7	7	0	5	5	5
13	Transactions with SOD conflicts used (different)	7	0	7	7	7	7	7	7	0	5	5	5
14	Average Transactions with SOD conflicts used	0	0	0	0	0	0	0	0	0	0	0	0
15	Critical Functions assigned	40	0	40	40	16	40	40	40	0	40	39	39
16	Average Critical Functions assigned	1	0	1	1	0	1	1	1	0	1	1	1
17	Critical Functions used	28	28	28	28	28	28	16	16	1	16	16	16
18	Average Critical Functions used	0	0	0	0	0	0	0	0	0	0	0	0
19	Assigned roles	1.023	0	1.023	1.023	1.023	1.023	1.023	1.023	0	1.023	1.023	980
20	Average Assigned roles	3	0	3	3	3	3	3	3	0	3	3	3
21	Used roles	47	0	47	47	47	47	38	38	0	38	38	38
22	Average used roles	0	0	0	0	0	0	0	0	0	0	0	0
23	Number of users with Critical Profile assigned (not blocked)	374	0	374	374	374	374	375	375	0	375	375	375

Detection assigned and use of critical transactions.

Using the drill-down options, you can navigate and detect the usage and assignment of critical transactions grouped by business process and functions.

Assigned Critical Funct.

Quick search 🔍   ⚙ Export ▾

BP Code	Bs. Process Name	Qty Functions	Nr. User Assign.	Nr.Trans.Assign	Detail of Functions
BC	Basis	8	448	113	➕
FI AP	FI - Accounts payable	3	113	6	➕
FI AR	FI - Accounts receivable	7	82	15	➕
FI GL	FI - General Ledger	6	99	18	➕
FI TR	FI - Treasury	3	50	5	➕
HCM	Human Capital Management	4	136	15	➕
MM	Material Management	6	236	24	➕
PM	Plaint maintenance	1	6	1	➕
SD	Sales and distribution	2	11	13	➕

Critical Funcions Used

Quick search 🔍   ⚙ Export ▾

BP Code	BP Name	Qty Functions	Nr. User Use	Nr.Trans.Used	Detail of Functions
BC	Basis	8	26	43	➕
FI AP	FI - Accounts payable	4	32	6	➕
FI AR	FI - Accounts receivable	3	9	5	➕
FI GL	FI - General Ledger	4	25	9	➕
FI TR	FI - Treasury	1	5	2	➕
HCM	Human Capital Management	3	5	5	➕
MM	Material Management	5	59	13	➕

Detection of assigned and use of SOD conflicting transactions.

Using the drill-down options, you can navigate and detect the use and assignment of conflicting transactions by segregation of duties grouped by business process and functions.

SOD Conflicts (assigned) — 2024/02

	Risk Id - SOD	BP 1	Function 1	BP 2	Function 2	Risk Level	Status	Qty Users w/SOD Trans	Qty Trans w/SOD Confl.	Users	Risks
1	6	CO	Cost Center Posting Transfer: Cancel	CO	Cost Class Closing Period: Display	Medium	Active	1	1	➕	ⓘ
2	8	CO	Cost Center Accounting Primary Costs : Cancel	CO	Cost Class Documents Report: INFO System	Medium	Active	1	2	➕	ⓘ
3	11	CO	Cost Center Accounting Primary Costs : Cancel	CO	Cost Class Period Closure: Lock Period	Medium	Active	1	1	➕	ⓘ
4	12	CO	Cost Center Accounting Primary Costs : Cancel	CO	Cost Class Closing Period: Display	Medium	Active	1	1	➕	ⓘ
5	13	CO	Cost Center Posting Transfer: Cancel	CO	Cost Center Posting Transfer: Register	Medium	Active	4	1	➕	ⓘ
6	14	CO	Cost Center Posting Transfer: Cancel	CO	Cost Center Accounting Primary Costs : Enter	Medium	Active	2	1	➕	ⓘ
7	15	CO	Cost Center Posting Transfer: Cancel	CO	Cost Center Customer Order Ip Transfers: Register	Medium	Active	1	1	➕	ⓘ
8	16	CO	Cost Center Accounting Primary Costs : Cancel	CO	Cost Center Posting Transfer: Register	Medium	Active	2	1	➕	ⓘ
9	17	CO	Cost Center Accounting Primary Costs : Cancel	CO	Cost Center Accounting Primary Costs : Enter	Medium	Active	2	1	➕	ⓘ
10	18	CO	Cost Center Accounting Primary Costs : Cancel	CO	Cost Center Customer Order Ip Transfers: Register	Medium	Active	1	1	➕	ⓘ

Go to 1 View 10 |◄ ◄ 1 2 3 4 5 ► ►| [1 to 10 of 511]

SOD Conflicts (used) — 2024/02

	Risk Id - SOD	BP 1	Function 1	BP 2	Function 2	Risk Level	Status	Qty Users w/SOD Trans	Qty Trans w/SOD Confl.	Users	Risks
1	145	FI AP	Master Creditors (Central): Create and Modify	MM	Purchase Order: Create and Modify	Medium	Active	1	1	➕	ⓘ
2	146	FI AP	Master Creditors (Central): Create and Modify	MM	Purchase Order: Release	High	Active	1	1	➕	ⓘ
3	209	FI AP	Creditors Invoices Logistics: Income	MM	Purchase Order: Create and Modify	Low	Active	1	1	➕	ⓘ
4	210	FI AP	Creditors Invoices Logistics: Income	MM	Materials: Goods Receipt	High	Active	1	1	➕	ⓘ
5	642	MM	Purchase Order: Create and Modify	MM	Purchase Order: Release	High	Active	1	1	➕	ⓘ
6	851	BC	Customer Management (Constituents)	BC	Base Development	Medium	Active	1	1	➕	ⓘ
7	852	BC	Security Administration:Role Management	BC	Base Development	Medium	Active	1	1	➕	ⓘ

Risk matrix with five components:

- ✓ SOD risk matrix with 850 pre-loaded and configurable rules.

- ✓ Configurable critical transaction risk matrix with the initial loading of BASIS functions.

- ✓ Matrix of configurable critical profiles with 34 critical SAP standard profiles initial load.

- ✓ A matrix of critical authorisation objects configurable with initial loading is the most sought-after by auditors.

- ✓ A matrix of critical roles must be configured with the roles that must be monitored due to their transactions and access.

The direct benefit is achieving an implementation period in very short periods to have information for effective control of the system's security.

Detection of use of non-current role roles.

Common operating errors and lack of user master adjustment processes leave roles assigned to users, allowing them to use them without problems.

Detection of use of non-current role profiles.

Common operating errors and lack of user master adjustment processes leave profiles assigned to users, allowing them to use them without problems.

Sample report of a non-current role used:

Non-current roles used								Last 90 days until 27/02/24		
Users	Roles	Assigned from	Assigned up to	Transaction	Tansaction text	Critical trans.	Date	Time	Note	
MDGM_STEWARD	ZCJL_FINANCIAL	25-05-2012	31-12-2023	VKM1	Documentos comerciales bloqueados	Crit.	01-02-2024	12:00:05		
MDGM_STEWARD	ZCJL_FINANCIAL	25-05-2012	31-12-2023	VKM4	Documentos comerciales	Crit.	01-02-2024	12:05:00		

Go to 1 · View 15 · · · · · 1 · · · · [1 to 2 of 2]

Critical Authorizations Objects assigned

The authorisation objects define them as critical for the functionality they provide to the users assigned to them, allowing them to perform tasks that should be carried out under control.

The cases that are identified, using the drill-down options, you can navigate and detect their assignment to user accounts.

CRITICAL AUTHORIZATION OBJECTS ASSIGNED   2024-02-27

	Risk Id.	Risk description	Transactions	Users
+	1	S_DEVELOP & OBJTYPE=DEBUG & ACTVT=02		⊕
+	2	S_DEVELOP & OBJTYPE=FUGR	SE37	⊕
+	3	S_DEVELOP & OBJTYPE=TRAN	SE93	⊕
+	4	S_DEVELOP & OBJTYPE=TABLE	SE16	⊕
+	10	S_DEVELOP & OBJTYPE=DEBUG & ACTVT=16		⊕

CRITICAL AUTHORIZATION OBJECTS ASSIGNED: S_DEVELOP & OBJTYPE=DEBUG & ACTVT=02   2024-02-27

Users	Role	Transaction	Auth. Obj. 1	Field 1	Value 1	To 1	Auth. Obj. 2	Field 2	Value 2	To 2
ALL0010	Z_DEV		S_DEVELOP	OBJTYPE	*		S_DEVELOP	ACTVT	*	
ALL0011	Z_DEV		S_DEVELOP	OBJTYPE	*		S_DEVELOP	ACTVT	*	
ALL0014	Z_DEV		S_DEVELOP	OBJTYPE	*		S_DEVELOP	ACTVT	*	
ALL0016	Z_DEV		S_DEVELOP	OBJTYPE	*		S_DEVELOP	ACTVT	*	
ALL0019	Z_DEV		S_DEVELOP	OBJTYPE	*		S_DEVELOP	ACTVT	*	
ALL0026	Z_DEV		S_DEVELOP	OBJTYPE	*		S_DEVELOP	ACTVT	*	
ALL0027	Z_DEV		S_DEVELOP	OBJTYPE	*		S_DEVELOP	ACTVT	*	
ALL003	Z_DEV		S_DEVELOP	OBJTYPE	*		S_DEVELOP	ACTVT	*	
ALL0036	Z_DEV		S_DEVELOP	OBJTYPE	*		S_DEVELOP	ACTVT	*	
ALL005	Z_DEV		S_DEVELOP	OBJTYPE	*		S_DEVELOP	ACTVT	*	

Y/Z transactions: inventory and definition of authority check

The Y/Z transaction inventory and four elements of the most significant importance:

1. Know precisely how many Y/Z transactions have been created in the system

2. Know which ones are assigned

3. Know which ones have been used

4. And if your authority checks are defined in transaction SU24 (and therefore highly probable that they are not declared in the transaction)

CLIENT (Y/Z) TRANSACTIONS

Transaction	Tansaction text	Date (*)	Auth. Object registered	Assigned Trans	Tran. Used ↓↑
ZSYSINFO	Programm Z_SYSINFO	10-01-2022	No	Si	Si
Y001_EXPORT	Archiving Tables	26-10-2022	No	No	No
Y23_UP	PPM: Initiate Cost Upload	05-01-2022	No	No	No
YAB968000031000	Transaktion zur Aufgabe WS96800003	05-01-2022	No	No	No
YAB968000071000	Transaktion zur Aufgabe WS96800007	05-01-2022	No	No	No
YAB968000080001	Transaktion zur Aufgabe WS96800008	05-01-2022	No	No	No
YAKBC440_FLIGHTLIST	Anzeigen einer Flugliste	05-01-2022	No	No	No
YCAT	Schnelltransport CATT	05-01-2022	No	No	No
YCHDIALOG_C	Dialogprogrammierung Übung C	17-01-2022	No	No	No
YCHDIALOG_D	Dialogprogrammierung Übung D	17-01-2022	No	No	No

Tools for improvement and remediation projects

Five tools for highly automated and effective security improvement and remediation projects:

1. Create a role with only the transactions used by an account

   CentinelBox extracts the information of transactions used and their respective authorisation objects from the user who has assigned roles and creates a new role.

2. Create a role with only the transactions used in a role

   CentinelBox extracts the transaction information from a role by all the accounts assigned it and creates a new role with these transactions along with the respective authorisation objects.

3. Segregate a role based on assigned transactions

   CentinelBox will create new roles based on segregation of duties conflicts identified in the transactions assigned to a role.

4. Segregate a base role to the transactions used

   CentinelBox extracts information on transactions used in a role by all accounts assigned to it. It will create new roles based on segregation of duty conflicts identified in the transactions used in the role.

5. Role modification

   Roles individually

   ✓ Transactions
   ✓ Authorization objects
   ✓ Organizational levels

   Roles massively

   ✓ Authorization objects
   ✓ Organizational levels

Tools for role design and redesign projects

Five tools for security improvement and remediation projects to create sustainable roles over time:

1. Create roles based on functions

   CentinelBox, based on the transactions assigned to a function, creates new roles with their respective authorisation objects, which can be prepared and assigned values before sending them to SAP.

2. Role derivation

   CentinelBox creates derived roles from simple roles.

3. Create composite roles

   CentinelBox creates composite roles based on simple roles.

4. Assign roles

   CentinelBox bulk assigns roles to user accounts.

5. Unassign roles

   CentinelBox bulk reassigns roles to user accounts.