Get more free resources: www.sodcheck.com

The five steps of the CHECK Method

You are here

- **C** Capture Data
- **H** Highlight Conflicts
- **E** Examine Results
- **C** Confirm Safeguards
- **K** Keep a Record of Decisions

SOD Check
Segregation of Duties
www.sodcheck.com

How to Capture Data for a Segregation of Duties Review: Capture Data Worksheet

Step 1 of 5 in the CHECK Method: list the access files you asked for

Use this worksheet for one system and one review date. It tracks the files your system administrator runs. It does not find conflicts. That is the next step.

Step 1. Name your scope

#	Item	Why it matters	Your answer
1	**System and environment in scope**	Start with the system that handles payments or payroll. Finish one full pass, then add more.	
2	**Review date**	Every file should come from the same day, so the lists can be compared.	
3	**Names: Controller, system administrator, system owner**	The Controller sets the scope. The system administrator runs the files. The system owner approves the request.	

Step 2. Ask for five things

Report names differ from system to system, and one report may hold more than one item. Ask for the content, not a fixed report name.

#	Ask for	What it tells you	Check before you accept it	File name, run by, date
4	**User list with status**	Who has an account, and whether it is active	Includes the user types you agreed on. Inactive accounts are marked, not removed.	
5	**User-to-role list**	Which roles each person holds	User IDs match the user list.	
6	**Role-to-rights list**	What each role lets a person do	Covers the rights tied to your payment, vendor or payroll steps. Includes limits, such as an approval amount.	
7	**Custom roles and direct rights**	Access given outside the standard roles	Custom roles and one-off grants are listed, or the file says there are none.	
8	**System and date note**	Which system, which environment, which day	Every file shows the system name and the date it was run.	

Step 3. Check the files

#	Check	Why it matters	Yes or no, and a note
9	Do the role files use the same user IDs as the user list?	A mismatch can hide a role or a user.	
10	Are any role names or fields blank?	Blank fields hide rights. Note any gaps instead of quietly dropping records.	

#	Check	Why it matters	Yes or no, and a note
11	Did the administrator show 3 or 4 accounts on screen, and do they match the files?	A reasonableness check. It does not prove the files are complete.	
12	Will the files move only by your company's approved secure method?	Access files show who can do what. Never send them through a public web form.	

Step 4. Write down the limits and decide

#	Item	What to write	Your answer
13	**Systems left out**	Name each system you leave out and why, so the result is not overstated.	
14	**Service accounts and contractors**	Decide how to treat them and write it down.	
15	**Ready for Highlight Conflicts?**	Write who decided and the date. Capturing data does not find conflicts and does not show that anything is wrong.	

Who can help: the Controller (names the scope and reviews the results), the system administrator (runs the files and records the system and date), the system owner (approves the request) and the IT leader (helps find the right system administrator and arranges secure sharing). Never borrow someone else's login.

Internal controls and SOX simplified. | A2Q2 SOD Check | © 2026 A2Q2. All Rights Reserved. | LM-005 v5
More free resources: www.sodcheck.com