Get more free resources: www.sodcheck.com

The five steps of the CHECK Method

SOD Check
Segregation of Duties
www.sodcheck.com

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

What Approach Can I Use to Prepare or Perform Segregation of Duties Analysis

Five steps for running a segregation of duties review

Segregation of duties means no single person can start and finish a risky task alone. A second person, or a second step, sits in the middle. The goal is not to distrust people. The goal is to catch honest mistakes early and make wrong-doing harder.

This roadmap has a section for each of five steps. Each one shows what to do, who owns it, and what you should have when the step is done. It explains a review process. It is not an audit.

The five steps at a glance

#	Step	The question it answers	What you end up with
1	**Capture Data**	Who has access to what, in which systems, as of which date?	Dated lists of users, roles and rights.
2	**Highlight Conflicts**	Where can one person do two jobs that should be separate?	A list of potential conflicts, sorted by process.
3	**Examine Results**	What can each user with a potential conflict really do?	Facts, proof and open questions for each potential conflict.
4	**Confirm Safeguards**	Does another control cover the risk, and does it really run?	Proof that a safeguard ran, or a note that it is missing.
5	**Keep a Record of Decisions**	What did management decide, and why?	A log with an owner and a due date for every open item.

Get more free resources: www.sodcheck.com

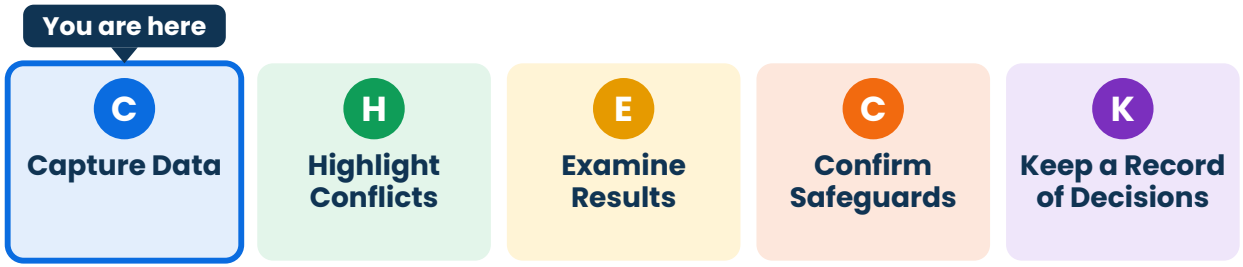
Before you start

- Start with one system and one date. Pick the system that handles payments or payroll.
- Name a system administrator and a system owner in IT, and a business owner in finance.
- Give every open item one person and one due date.
- A flagged potential conflict means "look here." It does not prove fraud or a failed control.

Who is who. The Controller explains the process and decides what the risk means for the company. A system administrator has elevated rights in a system, including the right to run reports. A system owner has the authority to approve changes to the system. Sometimes one person is both, but not always.

Get more free resources: www.sodcheck.com

The five steps of the CHECK Method



SOD Check
Segregation of Duties
www.sodcheck.com

Step 1 of 5: Capture Data

The question: who has access to what, in which systems, as of which date?

What to do

1. Name the system and the review date.
2. Ask for five things: a user list with status, a user-to-role list, a role-to-rights list with limits, custom roles and direct rights, and a note of the system and date on every file.
3. Check that the files use the same user IDs and have no blank role names.
4. Ask the system administrator to show three or four accounts on screen and compare them with the files.
5. Share the files only by your company's approved secure method.

Get more free resources: www.sodcheck.com

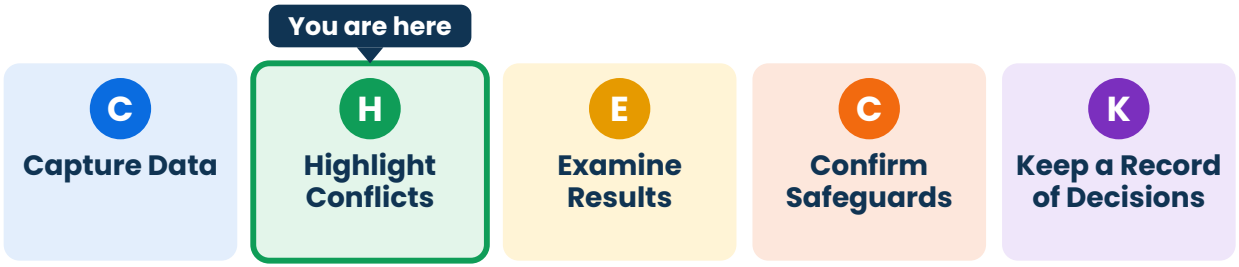
Who owns what

#	Person	Their part
1	**Controller**	Names the scope and the review date. Reviews the results.
2	**System administrator**	Runs the files. Records the system and date on each one.
3	**System owner**	Approves the request.

What this step does not do. It collects facts. It does not find conflicts and does not show that anything is wrong.
You are done with this step when you have: dated lists of users, roles and rights.

Get more free resources: www.sodcheck.com

The five steps of the CHECK Method



SOD Check
Segregation of Duties
www.sodcheck.com

Step 2 of 5: Highlight Conflicts

The question: where can one person do two jobs that should be separate?

What to do

1. Pick one process, such as payments, payroll or journal entries.
2. For that process ask four questions. Who can create or change? Who can approve? Who can release or pay? Who reviews?
3. Write each pair that one person should not hold alone as a short rule, for example "The same person should not be able to create a vendor and approve a payment."
4. Compare each user's rights with your rules. Look across two roles and inside one role. Count rights from roles and rights granted directly.
5. Group the potential conflicts by process. Mark High or Medium to decide what to look at first. Name one person to check each item.

Get more free resources: www.sodcheck.com

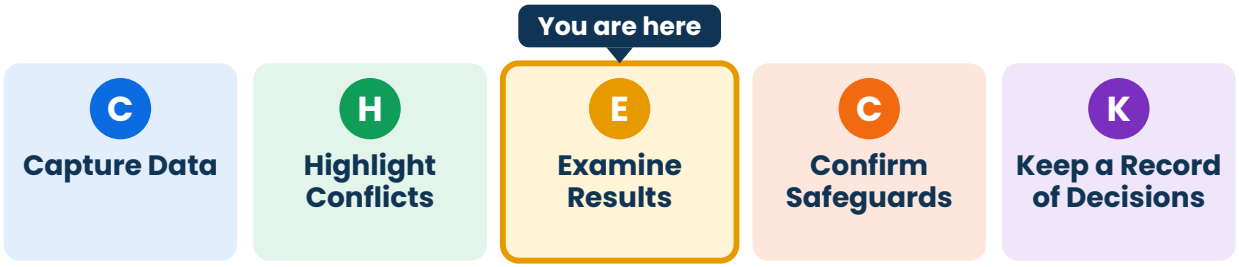
Who owns what

#	Person	Their part
1	**Controller**	Writes the rules. Decides which potential conflicts to look at first.
2	**System administrator**	Confirms what each right allows. Runs any extra reports.
3	**IT leader**	Helps find the right people. Arranges secure sharing.

What this step does not do. It finds possible conflicts. It does not show that anyone misused access. A long list of potential conflicts is not a score for fraud or weak controls.
You are done with this step when you have: a list of potential conflicts, sorted by process.

Get more free resources: www.sodcheck.com

The five steps of the CHECK Method



SOD Check
Segregation of Duties
www.sodcheck.com

Step 3 of 5: Examine Results

The question: what can each user with a potential conflict really do?

What to do

1. Start with the potential conflicts in your payment or payroll process.
2. For each potential conflict ask five questions. What can this user really do, counting every role? Are those rights active today? Does a limit apply? Why does this user need the access? Who else sees the work?
3. Ask the right person for each answer. Support each fact with proof. A spoken answer is a starting point.
4. Give each item a plain status: Needs review, Evidence pending, or Ready for the Controller's decision.
5. Give every missing answer to one person.

Get more free resources: www.sodcheck.com

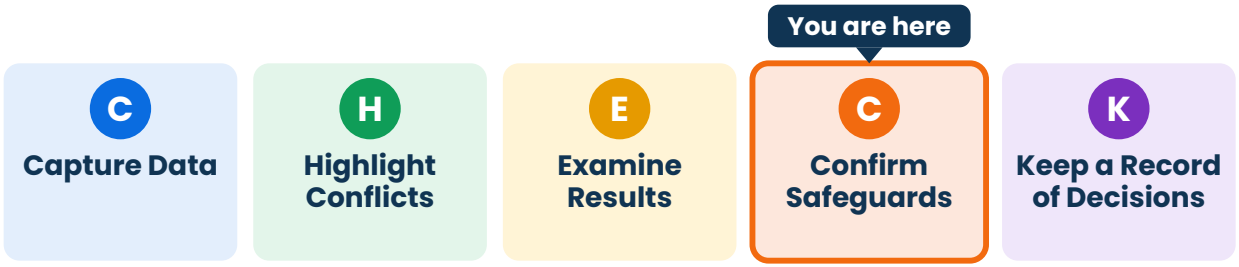
Who owns what

#	Person	Their part
1	**Controller**	Chooses which potential conflicts to examine first. Decides what the risk means once the facts are in.
2	**System administrator**	Confirms what each right allows and whether it is active.
3	**Process owner**	Explains the work and why the user has the access.

What this step does not do. It checks facts. It does not change any access, decide whether the risk is acceptable, or test the safeguards.
You are done with this step when you have: facts, proof and open questions for each potential conflict.

Get more free resources: www.sodcheck.com

The five steps of the CHECK Method



SOD Check
Segregation of Duties
www.sodcheck.com

Step 4 of 5: Confirm Safeguards

The question: does another control cover the risk, and does it really run?

What to do

1. Name the safeguard and who owns it. Examples are a second approval, an independent review, a report review or a system limit.
2. Ask four questions. Who does the check? How often? What do they look at? What record shows it took place?
3. Ask whether the record covers the dates and transactions in question, and whether the checker is a different person from the user who did the work.
4. A written policy shows the plan. A record from the right period shows it ran.
5. If proof is weak or missing, write down the gap and who follows up. Do not assume the safeguard failed.

Get more free resources: www.sodcheck.com

Who owns what

#	Person	Their part
1	**Controller**	Decides whether the safeguard is enough for the business risk, and writes down the reason.
2	**Process owner**	Explains how the check works and gathers the proof.
3	**System administrator**	Confirms any system limit and shows how it is set.

What this step does not do. It looks at the proof you collect. It does not prove a safeguard works for every period or every transaction.
You are done with this step when you have: proof that a safeguard ran, or a note that it is missing.

Get more free resources: www.sodcheck.com

The five steps of the CHECK Method



SOD Check
Segregation of Duties
www.sodcheck.com

Step 5 of 5: Keep a Record of Decisions

The question: what did management decide, and why?

What to do

1. Write one entry for each item: item ID, system and process, the potential conflict, what was checked, the decision and reason, the owner and due date, and the status.
2. Write a clear reason. Not "Reviewed, OK." Say what the team checked and why the decision makes sense.
3. Use simple statuses: More review needed, Evidence pending, Change approved, Closed with support.
4. Do not close an item because someone sent an email. Save the proof and the date.
5. Test the record: could someone who missed the meeting say what was flagged, what was checked, what was decided, why, and what happened next?

Who owns what

#	Person	Their part
1	**Controller**	Decides the business risk and writes down the reason.
2	**System administrator**	Carries out an approved access change, or confirms it was made.
3	**System owner**	Approves any change to the system.

What this step does not do. A record does not fix an access problem, replace the Controller's decision, or prove a safeguard works. Keep real records in approved, secure storage.

You are done with this step when you have: a log with an owner and a due date for every open item.

Internal controls and SOX simplified. | A2Q2 SOD Check | © 2026 A2Q2. All Rights Reserved. | LM-004 v3
More free resources: www.sodcheck.com