

FREE PRACTICAL GUIDE

INTERNAL AUDIT RESOURCE LIBRARY

SEGREGATION OF DUTIES

How to Review Segregation of Duties

A practical guide to identifying incompatible access and evaluating compensating controls

This guide is designed for internal auditors who need a concise, practical way to apply review segregation of duties in real engagements. It focuses on decisions, evidence and common failure points rather than theory.

THE OUTCOME YOU WANT

A practical guide to identifying incompatible access and evaluating compensating controls.

The six-step approach

- 1 Define critical end-to-end activities and decision rights.
- 2 Identify combinations that allow one person to initiate and complete a risky transaction.
- 3 Extract actual user access, not only role descriptions.
- 4 Prioritize combinations by financial or fraud impact.
- 5 Test whether compensating controls operate independently and with evidence.
- 6 Track exceptions, temporary access and remediation ownership.

Steps 1-3: Build the foundation

How to Review Segregation of Duties

1

Define critical end-to-end activities and decision rights.

Define the decision, risk or process question before collecting evidence. Write down what a good outcome would look like.

2

Identify combinations that allow one person to initiate and complete a risky transaction.

Use actual transactions, system evidence, data and accountable owners to confirm how the process operates in practice.

3

Extract actual user access, not only role descriptions.

Record assumptions, exceptions and boundaries early so later testing remains focused and reproducible.

AUDITOR PROMPT

Ask: "What evidence would convince another experienced auditor that this conclusion is reasonable?" If the answer is unclear, strengthen the planned work before moving on.

Steps 4-6: Turn work into assurance

How to Review Segregation of Duties

4

Prioritize combinations by financial or fraud impact.

Match the depth of work to the severity of the risk. High-risk conclusions need stronger evidence and clearer documentation.

5

Test whether compensating controls operate independently and with evidence.

Challenge exceptions for frequency, impact, root cause and management awareness before deciding what they mean.

6

Track exceptions, temporary access and remediation ownership.

Finish with an explicit conclusion and next action: no issue, improvement opportunity, finding, escalation or follow-up.

QUALITY CHECK

Before you finalize, ask whether the work directly answers the original audit question, whether evidence is sufficient, and whether a reader can understand the reasoning without being in the audit team.

CONFLICT

Create vendor + release payment.

RISK

A user could establish a fraudulent vendor and pay it.

COMPENSATION

Independent post-payment review is weaker than preventing the combination; if accepted, it must be timely, documented and complete.

What makes the example useful?

- It starts from a specific risk or audit question.
- It connects evidence and testing to a conclusion.
- It avoids treating process description as proof of control effectiveness.
- It leaves a clear path for management action or follow-up.

Quick reference - use this on your next audit

How to Review Segregation of Duties

Five practical reminders

- Not every access conflict is equally risky; prioritize combinations that enable concealment or unauthorized value transfer.
- Compensating controls must be independent and actually performed.
- Temporary or emergency access should have expiry and review.

Mini self-check

- ☐ Have I linked the work to a clear audit objective or business risk?
- ☐ Is the evidence strong enough for the importance of the conclusion?
- ☐ Have I distinguished facts, explanations and assumptions?
- ☐ Have I considered root cause and recurrence, not only the immediate exception?
- ☐ Can management understand what decision or action is required?

RESOURCE NOTE

This is a practical learning resource, not formal professional guidance. Adapt the approach to your organization, applicable standards, regulation and audit methodology.