

FREE PRACTICAL CHECKLIST

INTERNAL AUDIT RESOURCE LIBRARY

ACCESS & SOD

Segregation of Duties Review Checklist

A practical checklist for identifying incompatible roles, compensating controls and toxic access combinations.

☒	_____
☒	_____
☒	_____
☒	_____

How to use this checklist

This checklist is designed as a practical fieldwork aid for segregation of duties review. Use it to prepare interviews, structure testing and document areas requiring deeper evidence. A checked box should mean the point was considered and supported - not simply that a question was asked.

SIMPLE STATUS KEY

- ☐ **Done** Evidence supports the point
- ☐ **Review** More evidence or clarification needed
- ☐ **N/A** Not applicable - document why

Design

- ☐ **01** Critical end-to-end processes and sensitive activities are mapped.
- ☐ **02** Incompatible combinations are defined using business risk, not generic labels only.
- ☐ **03** Privileged/system administration access is included.
- ☐ **04** Emergency access has explicit approval and expiry.
- ☐ **05** Small-team constraints and compensating controls are documented.

AUDITOR NOTES / EVIDENCE

User review

- ☐ 06 Access is matched to current job responsibilities.
- ☐ 07 Joiners, movers and leavers are tested.
- ☐ 08 Dormant and shared accounts are identified.
- ☐ 09 Users with multiple conflicting roles are investigated.
- ☐ 10 Temporary/project access has an expiry date.

Risk prompts

- What could fail even if the documented procedure looks adequate?
- Where can one person initiate, change and approve the same outcome?
- Which exceptions are common enough to have become normal practice?
- What data pattern would indicate control bypass or management override?

TESTING NOTES / EXCEPTIONS

Monitoring

- ☐ 11 Role changes are logged and independently approved.
- ☐ 12 Compensating controls are tested for actual effectiveness.
- ☐ 13 High-risk combinations receive periodic transaction monitoring.
- ☐ 14 SoD exceptions have accountable owners and review dates.
- ☐ 15 Remediation is prioritized by business impact and exploitability.

Evidence to retain

- ☐ 01 Relevant system reports or extracts with source and period visible.
- ☐ 02 Approval/workflow evidence for selected high-risk items.
- ☐ 03 Screenshots or logs supporting key control steps and exceptions.
- ☐ 04 Reconciliations or reperformance showing how the conclusion was reached.
- ☐ 05 Management explanation only where corroborated or clearly identified as explanation.

Use data to challenge the checklist

Where transaction data is available, do not rely only on samples. Run targeted tests that identify unusual behavior, control bypass and concentrations. Adapt the tests below to the process and available fields.

- ☐ **01** Trend exceptions by user, approver, location, vendor/customer or month.
- ☐ **02** Identify transactions just below approval or policy thresholds.
- ☐ **03** Search for duplicates, repeated round values and unusual timing.
- ☐ **04** Compare master-data changes with subsequent transactions or payments.
- ☐ **05** Review override, manual-entry and emergency/urgent indicators.
- ☐ **06** Investigate outliers that combine multiple risk indicators.

RED-FLAG RULE

A red flag is not proof of wrongdoing. Treat it as a reason to obtain more evidence. Combine pattern, business context, approval history and supporting records before reaching a conclusion.

Completion and conclusion

Before you close the checklist

- ☐ **01** All material exceptions have an evidence reference.
- ☐ **02** Open questions have an owner and due date.
- ☐ **03** Control design issues are separated from isolated execution errors.
- ☐ **04** Recurring exceptions have been considered for root cause and systemic impact.
- ☐ **05** The conclusion is proportionate to evidence and business risk.
- ☐ **06** Any issue requiring escalation has been communicated promptly.

FINAL CONCLUSION

Overall assessment / key message:

Owner / follow-up date:
