

FREE PRACTICAL CHECKLIST

INTERNAL AUDIT RESOURCE LIBRARY

FRAUD RISK

Fraud Risk Assessment Checklist

A practical checklist for identifying fraud scenarios, opportunities, override and response readiness.

- ☒ _____
- ☒ _____
- ☒ _____
- ☒ _____

How to use this checklist

This checklist is designed as a practical fieldwork aid for fraud risk assessment. 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

Fraud scenarios

- ☐ **01** Relevant fraud schemes are identified by process and asset.
- ☐ **02** Management override scenarios are explicitly considered.
- ☐ **03** Third-party and collusion risks are considered.
- ☐ **04** Digital/payment fraud scenarios reflect current systems and channels.
- ☐ **05** Prior incidents, whistleblowing and near misses are incorporated.

AUDITOR NOTES / EVIDENCE

Drivers and controls

- ☐ 06 Pressure/incentive factors are discussed where relevant.
- ☐ 07 Opportunities created by weak segregation or access are identified.
- ☐ 08 High-judgment estimates and manual journals are considered.
- ☐ 09 Preventive and detective controls are mapped to each major scenario.
- ☐ 10 Control owners understand fraud-specific responsibilities.

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 and response

- ☐ 11 Red-flag analytics are defined for high-risk schemes.
- ☐ 12 Whistleblowing channels are accessible and protected.
- ☐ 13 Investigation roles and escalation protocols are defined.
- ☐ 14 Evidence preservation requirements are known.
- ☐ 15 Lessons from incidents are converted into control improvements.

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:
