

FREE PRACTICAL CHECKLIST

INTERNAL AUDIT RESOURCE LIBRARY

THIRD-PARTY RISK

Third-Party & SLA Audit Checklist

A practical checklist for contracts, service levels, data, compliance, resilience and vendor oversight.









How to use this checklist

This checklist is designed as a practical fieldwork aid for third-party & sla audit. 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

Onboarding and contract

- ☐ **01** Business owner and procurement role are clear.
- ☐ **02** Due diligence reflects financial, legal, cyber and operational risk.
- ☐ **03** Contract defines scope, pricing, responsibilities and termination rights.
- ☐ **04** Confidentiality, data protection and audit rights are addressed.
- ☐ **05** Subcontracting requirements are defined where relevant.

AUDITOR NOTES / EVIDENCE

SLA performance

- ☐ 06 Service levels have measurable definitions and data sources.
- ☐ 07 Performance reports are independently validated where material.
- ☐ 08 Credits/penalties are applied when contractual conditions are met.
- ☐ 09 Recurring service failures have root-cause actions.
- ☐ 10 Changes to scope or pricing are formally approved.

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

Continuity and oversight

- ☐ **11** Business continuity and incident escalation are tested.
- ☐ **12** Critical third parties have exit/transition plans.
- ☐ **13** Access to company systems/data is periodically reviewed.
- ☐ **14** Compliance certificates and insurance are kept current.
- ☐ **15** Management reviews concentration and dependency risk.

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:
