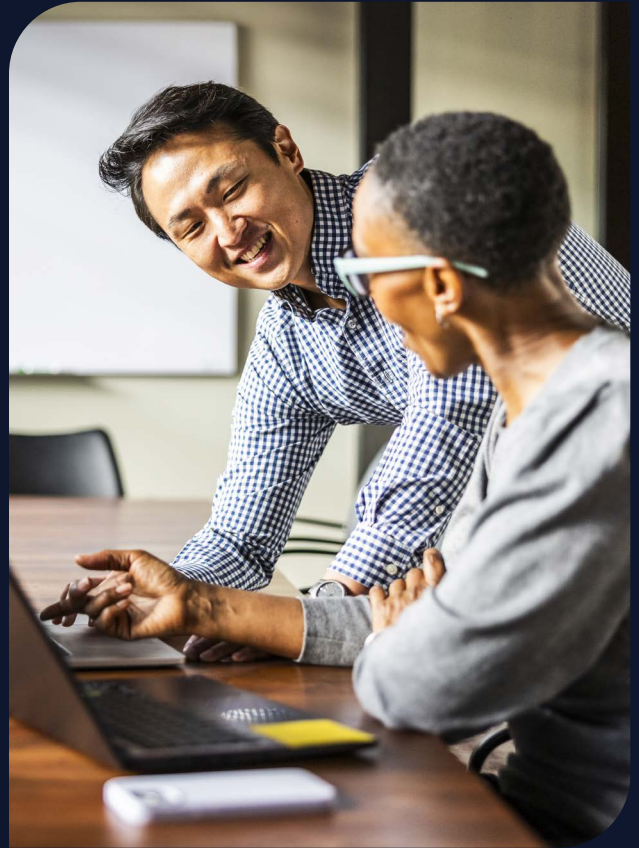




# Fraud Detection Checklist: Limited Segregation of Duties



## 1. General Fraud Risk Mitigation

An organization can mitigate its fraud risk through its fraud risk mitigation culture, perception of detection, and providing an opportunity for others to report their suspicions.

Focus On:	Ask These Questions:	Yes	No
Tone at the Top	Does management discuss what fraud is and how the organization mitigates its fraud risk with employees on a periodic basis?		
Financial Statement Audit	Is the organization subject to a financial statement audit on an annual basis?		
Anonymous Reporting System	Does the organization have an anonymous reporting system in place for employees, customers, and vendors to report financial concerns?		

## 2. Monthly Independent Review of Bank Records

A business owner, employee, board member, or third party without the authorization to initiate or execute bank transactions should conduct this review.

Focus On:	Ask These Questions:	Yes	No
<b>Transfers</b> Compare transfers reported on bank statements to transfers recorded in the accounting records.	Are there transfers to unknown accounts?		
	Are there any larger, even dollar amounts (e.g., \$8,000.00)?		
	Are there transfers to accounts that are different than accounts recorded in the accounting record?		
	Are there any omitted transfers from the accounting records?		
<b>ACH Transactions</b> Compare automated clearing house transactions (ACHs) reported on bank statements to ACHs recorded in the accounting records.	Are there any ACHs to unknown vendors/payees?		
	Are there any larger, even dollar amounts (e.g., \$8,000.00)?		
	Are there ACHs to vendors/payees that are different than the vendors/payees recorded in the accounting records?		
	Are there any omitted ACHs from the accounting records?		
<b>Withdrawals</b> Compare withdrawals reported on bank statements to withdrawals recorded in the accounting records. Review should include withdrawals by ATMs and withdrawals made at the bank.	Are there any withdrawals omitted from the accounting records?		
	Are there any withdrawals made without supporting documentation, such as invoices or receipts?		
<b>Other Debits</b> Compare miscellaneous/other debits reported on bank statements to transactions recorded in the accounting records.	Are there any debits omitted from the accounting records?		
	Are there debits that lack supporting documentation, such as invoices or receipts?		
<b>Check Numbers</b> Compare check numbers clearing the bank account to the check register.	Are there check numbers clearing the bank account not reflected within the check register?		
	Are there check numbers clearing the bank account that are voided within the accounting?		

### 3. Monthly Independent Review of Credit Card Statements

By carefully examining each monthly corporate credit card statement, you can identify any unauthorized transactions, errors, or suspicious activities.

Focus On:	Ask These Questions:	Yes	No
Credit Card Policy	Is there a corporate credit card policy in place defining what the credit card can be used for? Is the policy being followed?		
Reconciling Bank Credit Card Payments	Do all bank credit card payments reconcile to corporate credit payments reflected on each monthly statement?		
Itemized Receipts	Are there itemized receipts to support each charge?		
Charges	Are there unusual charges such as small, recurring charges or non-descript charges? Do the locations of charges make sense for the organization?		

### 4. Monthly Independent Review of Cash Receipts

A business owner, employee, board member, or third party without access to the physical cash receipts or Point-Of-Sales (POS) System, should perform the review. Compare cash receipts and deposits to sales invoices and POS reports. Review deposited items (i.e., checks deposited into the bank account) to customer payments posted within the accounting software.

Focus On:	Ask These Questions:	Yes	No
Cash Flow Decline	Is there a suspicious decline in cash flow?		
Deposit Item Types	Review for unusual trend in deposit transaction type, such as lower than expected cash deposits.		
Aging Receivables	Review for unusual outstanding receivables such as customers that have a history of paying timely.		
Receivables	Are there any discrepancies between the dollar amount of cash and checks received, according to the sales report, to the actual cash and checks deposited per the bank deposit ticket?		
Payor Discrepancies	Do the checks from payors appear to be different than the customer accounts in which the payments were posted?		
POS Reports	If a POS system is used, do the POS reports show frequent or large no-sales, voids, or discounts?		

## 5. Inventory Management

A business owner, employee, board member, or third party without access to purchasing, maintaining, or recording of inventory should perform these functions. A physical count of inventory should be performed with a comparison of purchase orders, receiving slips, and POS reports to the accounting records for any discrepancies.

Focus On:	Ask These Questions:	Yes	No
Security	Is inventory accessible to anyone and are there cameras over the receiving, shipping, and storerooms?		
Adjustments	Are there adjustments made to inventory items. If so, who is making them, how often, and for what purpose?		
Maintaining Inventory	Is inventory maintained by someone independent of the purchasing, receiving, and recording functions?		

## 6. Payroll Processing

A business owner, employee, board member, or third party without access to payroll functions should perform this review. A review of employee's compensation and benefits should be conducted and compared to records listing authorized compensation and benefits.

Focus On:	Ask These Questions:	Yes	No
Employee Listing	Are there any employees listed on payroll that no longer work at the organization, or are the name is not familiar?		
Overtime Hours	Are there any employees that are receiving overtime hours and if so, is the overtime warranted and authorized?		
Compensation	Does each employee's gross pay amount coordinate with the amount authorized in their contract or other payroll documentation?		
Benefits	What benefits are employees receiving and do they reconcile with what has been authorized by management?		
Leave Time	Are there any employees with large leave balances and/or who consistently use large amounts of leave each year?		

This checklist along with the following framework can help organizations assess and strengthen their anti-fraud posture across governance, ownership, assessment, policy, controls, and detection.

## Fraud Risk Management

### 1 Governance & Oversight

- Fraud Risk Oversight: Establish a formal process for the board or audit committee to proactively manage fraud risks. This process should be fully implemented, tested annually, and proven effective.
- Fraud Risk Ownership: Assign a senior management member as the designated fraud risk owner. Clearly communicate responsibilities to all relevant managers across the organization.

### 2 Risk Assessment & Policy

- Fraud Risk Assessment: Implement a periodic and ongoing fraud risk assessment process. Ensure it is tested annually and reflects current organizational risks.
- Risk Tolerance & Management Policy: Define and obtain board approval for the organization's tolerance levels for different types of fraud risks.
- Develop and approve a fraud risk management policy that outlines:
  - Risk ownership
  - Risk rejection strategies (e.g., declining certain business opportunities)
  - Risk transfer mechanisms (e.g., insurance, contracts)
  - Mitigation steps for retained risks

### 3 Controls & Re-engineering

- Process-Level Controls:
  - Re-engineer processes to eliminate or minimize significant fraud risks.
  - Implement and test controls such as segregation of duties and transaction monitoring.
- Environment-Level Controls:
  - Promote ethical behavior and two-way communication.
  - Maintain a tested and effective process to deter wrongdoing and encourage transparency.

### 4 Proactive Detection

- Establish a system to detect, investigate, and resolve fraud-related red flags.
- Embed controls in information systems to flag suspicious transactions for review before processing.