New Treasurer or Bookkeeper Takeover:

A Crime-Prevention Checklist for Churches and Ministries

A 90-day guide for church treasurers, bookkeepers, financial secretaries, church administrators and finance committees

HOW TO USE THIS CHECKLIST

Use this checklist in your first 90 days as the new treasurer, bookkeeper, financial secretary or church administrator. It helps you confirm that offerings, payments and system access have good safeguards, and that your church's crime coverage fits how money actually moves. Check off each item as you finish it and jot down what you find.

These steps aren't about suspicion. Good controls protect the faithful staff and volunteers who handle the church's money, because no one is ever left alone with it or open to question.

In this checklist, "leadership" means whoever oversees finances in your setting: the finance committee, deacons, elders, trustees, church council, session or vestry, or a school or ministry board. Christian schools and ministries can read "tuition" or "donations" wherever you see "offerings."

Four insurance terms to know

- **Employee theft (sometimes called fidelity).** Loss of money, securities or other property stolen by an employee, even if you can't tell which employee did it. Standard crime forms don't automatically count volunteers as employees; many church policies add them by endorsement, so check how yours reads.
- **Deductible.** The amount the church pays before the policy pays. Some policies call it a retention. Losses smaller than the deductible aren't paid.
- **Discovery or loss sustained.** Crime policies are written one of two ways. A discovery form covers losses first discovered while the policy is in force, even if the theft started earlier. A loss-sustained form covers losses that happen during the policy period and are discovered within a set time afterward. Either way, report promptly.
- **One occurrence.** A series of thefts by the same person, or by people working together, is usually treated as one occurrence, with one limit and one deductible, even if it went on for years.

FIRST DAYS: TAKE OVER AUTHORITY AND ACCESS

Start by learning who can move money and who can see the books, then close any access that no longer fits.

- ☐ Hold a documented handoff with the outgoing treasurer, bookkeeper or financial secretary: open items, unusual transactions and known problems. A gracious handoff makes everything that follows easier.
- ☐ Meet with the pastor and the finance committee chair (or the chair of the deacons, elders or trustees) to confirm what leadership expects you to report and how often.
- ☐ List every bank account, credit card, and online giving or payment platform, and who can use each. Include ministry accounts (youth, missions, women's and men's ministries, the benevolence fund, a preschool or school) and any account opened under the church's name or tax ID.
- ☐ Confirm who can sign checks, approve wires and release ACH payments. Remove anyone who has left or changed roles, and update bank signature cards to match leadership's current authorization.
- ☐ Confirm that no one person handles counting, depositing, recording and reconciling. Plan to separate those duties.
- ☐ Change shared passwords and remove former staff and volunteers from the accounting software, bank portals, payroll, church management and giving software, and church email.
- ☐ Write down approval limits: who can approve which amounts, and when the finance committee, board or congregation must approve under your bylaws or policies.
- ☐ Save a baseline as of your start date: bank balances, fund balances (general, designated and restricted) and a trial balance.
- ☐ Review the last 12 months of bank reconciliations for gaps or old unresolved items.
- ☐ Ask the finance committee chair whether any losses or concerns about dishonesty are already known. If so, make sure your insurance agent is told promptly. Coverage may not apply to someone whose dishonesty leadership already knew about.

OFFERINGS, TITHES, BANK AND CASH

Reconcile everything once yourself so the starting point is clean, and make sure offerings are never handled by one person alone.

- ☐ Reconcile every bank account to its statement for the most recent month. Look into anything unresolved for more than 30 days.
- ☐ Ask each bank for a list of all accounts under the church's EIN (tax ID), and compare it to your list.

- ☐ Confirm offerings are counted by at least two unrelated people (not spouses or close relatives), ideally on rotating teams, and that both sign the count sheet.
- ☐ Confirm offering plates or bags go straight from the service to the counting room under the control of two people and are never left unattended.
- ☐ Confirm counted cash and checks go into a sealed, tamper-evident bag and are deposited promptly, ideally the same or next business day. Compare count sheets to bank deposits.
- ☐ Confirm the person who reconciles the bank statement doesn't also count, deposit or sign checks. Where duties can't be fully separated, have a finance committee member who doesn't handle money review the statement and reconciliation each month.
- ☐ Count petty cash and cash on hand. Confirm there is one custodian, a set limit, and a receipt for every withdrawal.
- ☐ Confirm designated and restricted gifts (building fund, missions, benevolence, memorials, grants) are tracked separately and spent only for their stated purpose.
- ☐ Review transfers between accounts and any payments to staff, leaders or their relatives.
- ☐ Check who has keys, combinations or codes to the safe, church office and cash boxes, and whether they were changed after staff or volunteer turnover.
- ☐ Confirm how deposits get to the bank (a volunteer, staff member, night drop or armored service) and that the process is written down.
- ☐ Store blank check stock securely and account for voided checks in number order.

PAYMENTS: VENDORS, CHECKS, WIRES AND ACH

Fake or altered payment requests are a common way money goes missing, so verify before any money moves and review what has already moved.

- ☐ Pull the vendor list. Look for duplicates, missing W-9s or tax IDs, PO-box-only addresses, and vendors that share an address or bank account with staff, leaders or their relatives.
- ☐ Keep vendor bank account and routing numbers in one secure, access-limited vendor file, so there's a known-good record to check against.
- ☐ Review every change to vendor bank details in the last 12 months. Confirm each was verified with a call-back to the vendor's independently verified number.
- ☐ Before releasing any payment, compare the account and routing numbers on the invoice or payment request with the vendor file. If they don't match, stop and verify before paying.
- ☐ Require two people for wires and ACH: one initiates and one approves. Check the bank portal's dual-control settings and daily limits.
- ☐ Match a sample of paid checks to invoices and approvals. Review check images for changed payees or amounts.

- ☐ Ask the bank about positive pay or payee-match services for checks.
- ☐ Confirm payments to the pastor, church administrator or other senior leaders (including reimbursements and stipends) are approved by someone other than that person, such as the treasurer or finance committee chair.
- ☐ Review benevolence fund payments for a documented need, approval by more than one person, and named recipients. For help to staff members or their families, ask your CPA how the payment should be handled.
- ☐ Scan payments for duplicate invoice numbers, round amounts, and amounts just under an approval limit.
- ☐ Set a call-back rule: no one changes payment details based on an email, letter or call alone. When a "we've changed our bank" notice arrives, call the vendor to confirm the new account and routing numbers before updating anything.
- ☐ Make that call from a church landline or your own cell phone, using a number you look up yourself, such as the vendor's official website or a web search. Don't use the number in the email or invoice, and don't rely on a vendor-file number that may have been changed by the same scam.
- ☐ Write down who you spoke with, the date, and what they confirmed, and have a second person approve the change in the vendor file.
- ☐ Brief everyone who handles money on warning signs: lookalike email addresses or texts that appear to come from the pastor ("I'm in a meeting, can you buy gift cards for me?"), urgent deadlines, new payment details, and requests to keep a payment quiet.

PAYROLL, PASTORAL COMPENSATION, EXPENSES AND CARDS

Check that every paycheck goes to a real, current staff member, that pastoral compensation matches what leadership approved, and that spending is reviewed by someone other than the spender.

- ☐ Compare the payroll register to the current staff list. Look for people with no supervisor, no timesheets, or a shared bank account or address.
- ☐ Confirm the pastor's compensation (salary, housing allowance, benefits) matches what leadership approved. A minister's housing allowance must be officially designated in a definite amount before it is paid, for example in the minutes or the budget. It can't be set after the fact.
- ☐ Confirm ministers are set up correctly in payroll. For ministerial services, the church doesn't withhold Social Security and Medicare (FICA); the minister pays self-employment tax unless the IRS has approved an exemption, and income tax is withheld only under a voluntary agreement. Non-minister staff are generally subject to FICA. Ask your payroll provider or CPA to confirm the setup.

- ☐ Review stipends, honoraria and allowances (guest speakers, musicians, nursery workers) for documented approval, and confirm whether each person is staff (Form W-2) or a nonemployee (Form 1099-NEC). For payments made in 2026, a 1099-NEC is generally required when a nonemployee is paid $2,000 or more for services during the year.
- ☐ Review changes to pay rates and direct deposit details over the last 12 months, and confirm each had an approval.
- ☐ Confirm staff who have left were removed from payroll and from system access.
- ☐ Confirm who can run payroll, who approves it, and what limits apply to the payroll bank account.
- ☐ Review expense reimbursements for receipts and approval under a written reimbursement policy. No one should approve their own expenses, including the pastor.
- ☐ Have someone other than the cardholder review each church credit card statement every month.
- ☐ Confirm payroll taxes are deposited on time, quarterly Form 941 returns are filed and match payroll records, and year-end W-2s and 1099s were filed.

GIVING, PLEDGES, GRANTS AND FUNDRAISING

Gifts can be taken before they're recorded, or hidden through refunds and edits, so compare giving records to what actually reached the bank.

- ☐ Compare giving records (church management software, online and text giving, envelopes and pledges) to bank deposits for a recent period.
- ☐ Confirm online giving, text giving and kiosk payouts go to the church's own bank account, and review who can change the payout account.
- ☐ Review refunds, adjustments and deleted gifts. Confirm each was approved by someone other than the person who made it.
- ☐ Confirm contribution statements come from records kept or reviewed by someone other than the person who handles cash. A member who questions a statement is a helpful check, so follow up kindly.
- ☐ Confirm contribution statements meet IRS rules. For any single gift of $250 or more, the donor needs a written acknowledgment showing the church's name, the amount (or a description, without a value, of a non-cash gift), and whether any goods or services were given in return, or that only intangible religious benefits were. Many churches send annual statements by January 31.
- ☐ When someone pays more than $75 for something that is partly a gift and partly a purchase (a banquet ticket or auction item, for example), confirm the church gives a written disclosure with a good-faith estimate of the value received.

- ☐ Confirm there is a written policy for designated gifts and benevolence, and that designated gifts are recorded and used as given. Gifts earmarked for a specific person aren't tax-deductible for the donor.
- ☐ For grants, confirm funds are spent as the grant agreement requires and that spending reports are reviewed by a second person.
- ☐ For fundraisers (mission trip fundraisers, bake sales, school events, auctions), confirm cash and tickets are counted by two people, with a signed reconciliation of tickets, sales and deposits.
- ☐ Confirm gifts that arrive by mail are logged when opened, ideally by two people, or go to a bank lockbox.
- ☐ Confirm gift cards the church buys or receives (including benevolence gift cards) are logged, secured and reconciled.
- ☐ For a Christian school or preschool, reconcile tuition and fees to the billing system, and confirm who can grant discounts, scholarships or write-offs.

SYSTEMS AND ACCESS

A former staff member or volunteer who still has a login can cause loss long after leaving, so treat access as part of the books.

- ☐ List every user in the accounting software, church management and giving software, bank portals and payroll. Confirm each person is current and has only the access their role needs.
- ☐ Replace shared logins with individual ones, especially where volunteers have access.
- ☐ Confirm the person who records transactions isn't the same person who approves and reconciles them.
- ☐ Turn on multi-factor authentication for banking, email, accounting and the giving platform.
- ☐ Turn on audit logs or change alerts, and review edits to vendor, donor and bank-detail fields.
- ☐ Confirm who can edit or delete posted gifts and transactions.
- ☐ Confirm data is backed up regularly and that a restore has been tested. If the church has cyber coverage, ask your agent what security steps, such as MFA and backups, the policy expects.

PROPERTY, EQUIPMENT AND INVENTORY

Keep records that show how a shortage happened. An item that's simply missing isn't proof of theft, and standard crime forms don't cover a loss shown only by an inventory count.

- ☐ Review the list of equipment: sound and media gear, instruments, laptops, vehicles and tools. Confirm items are tagged and someone is responsible for each.

- ☐ Confirm who has keys or access to buildings, storerooms and offices, and how often access is reviewed.
- ☐ If the church runs a bookstore, café, thrift ministry, camp or school, compare inventory and sales records and look into shortages.
- ☐ Review how items that leave the building (loans, mission trips, off-site events) are tracked.
- ☐ If staff or volunteers handle money or property that belongs to others (members' trip funds, a partner ministry's property, or a family's belongings during a home visit), list it, along with any contract that requires coverage for it.

RETIREMENT AND BENEFIT PLANS (ERISA)

Most church retirement and health plans are exempt from ERISA as "church plans" unless the church elected to be covered, so most churches don't need an ERISA fidelity bond. A Christian school, camp or ministry that isn't controlled by or associated with a church, or a plan that elected ERISA coverage, may be subject to it. Ask your plan provider or benefits advisor which applies to each plan.

- ☐ List every plan the church or ministry sponsors (403(b), denominational retirement plan, health plan, flexible spending account) and who handles plan money.
- ☐ Ask the plan provider, denominational benefits board or advisor whether each plan is an exempt church plan or is subject to ERISA.
- ☐ Confirm employee contributions are sent to the plan promptly after each payroll. For ERISA plans, the Department of Labor requires deposit as soon as contributions can reasonably be separated from church funds, and no later than the 15th business day of the following month; plans with fewer than 100 participants have a 7-business-day safe harbor.
- ☐ If ERISA applies, confirm each person who handles plan funds is bonded for at least 10% of the funds handled, with a $1,000 minimum and, generally, a $500,000 maximum per plan ($1,000,000 if the plan holds employer securities). The bond can't have a deductible, must name the plan, and should be re-checked each plan year.
- ☐ Confirm plan money is kept separate from operating funds.

CRIME INSURANCE REVIEW: QUESTIONS FOR YOUR AGENT

Find out whether your crime coverage is a stand-alone policy or part of your church package policy, then ask these questions about limits and terms.

Question to ask	Why it matters
Is our crime coverage a stand-alone policy or part of our church package policy? What are the policy dates?	Crime coverage built into a package policy sometimes carries a lower limit than a stand-alone policy, so check that the limit fits.

Question to ask	Why it matters
What is the employee theft limit, and could one loss exceed it?	A series of thefts by the same person is usually one occurrence with one limit, and long-running thefts add up.
What is the deductible for each coverage?	Deductibles can differ by coverage, and a smaller loss may fall below the deductible.
Are volunteers, unpaid officers, and deacons, elders or trustees serving on committees counted as employees?	Many churches rely on volunteers to count and deposit offerings. Standard forms add volunteers by endorsement, and definitions vary by carrier.
Is the policy written on a discovery or loss-sustained basis? How are thefts that began before this policy handled?	This affects whether a theft that started years ago, or under a prior policy, is covered.
Is money covered while volunteers or staff carry deposits to the bank, and at off-site events?	Inside-the-premises and outside-the-premises coverage each have their own limits and conditions.
Which coverages are included: forgery or alteration, theft of money inside and outside the premises, computer and funds transfer fraud, and social engineering (fraudulent impersonation)?	Computer and funds transfer fraud coverage generally doesn't cover a payment your own team sent after being tricked by a fake email, such as one that appears to come from the pastor. Many policies exclude these losses unless social engineering coverage is added, which is often optional, may carry a lower sublimit, and may require call-back verification. Terms vary by carrier.
If any plan is subject to ERISA, do we have an ERISA fidelity bond, and does the limit meet the required amount?	Most church plans are exempt. If yours isn't, the bond must cover at least 10% of plan funds handled (within ERISA's minimum and maximum) with no deductible.
Does our denomination, lender, grant agreement or a partner require crime or fidelity coverage at a set limit?	Agreements can set minimum limits that the policy must meet.
Do we need coverage for money or property that belongs to others, such as members' trip funds or a partner ministry's property?	Some agreements require it. It is usually an optional coverage or endorsement, not automatic.
What are the notice and proof-of-loss rules after a loss?	Late notice can put a claim at risk. Standard forms ask for a sworn proof of loss within 120 days of discovery.
Do our limits still fit after growth, a building campaign, a new campus or school, or a merger?	Standard forms cover newly merged or acquired organizations only for a limited time (90 days) unless the insurer is told and agrees.

- ☐ By day 60, schedule a crime coverage review with your agent so it takes place in days 61 to 90.
- ☐ Give your agent a short summary of what you found with this checklist.

RED FLAGS AND WHAT TO DO IF SOMETHING LOOKS WRONG

A red flag is a reason to look closer, not proof that anyone has done wrong. If you find one, write it down and tell the finance committee chair, or another leader who isn't involved, before taking any other step. The one exception: if a suspicious payment is still in progress, call the bank first to try to stop it.

Common red flags

- Reconciling items that stay unresolved or keep being re-explained
- Missing count sheets, deposit slips, receipts or statements
- One person who controls counting, depositing and recording
- Changes to vendor or staff bank details with no clear approval
- Urgent payment or gift card requests that skip normal approvals
- Someone who won't take time off, share duties or accept review
- Designated funds spent for another purpose, or members questioning their giving statements

If something looks wrong

1. Stop and write down what you saw. Don't change or delete records, and don't confront anyone.
2. Tell the finance committee chair or another leader who isn't involved, right away. If the concern involves the chair, the pastor or the church administrator, go to another elder, deacon, trustee or finance committee member, or to your denomination's leadership if that fits your polity.
3. If a payment is still in progress, call the bank immediately. Some transfers can be stopped or recalled if the bank hears quickly.
4. Tell your insurance agent promptly. Crime policies generally require prompt notice, cooperation and a sworn proof of loss (within 120 days of discovery on standard forms).
5. Ask leadership to consider reporting to law enforcement. Some policies require it.
6. Under leadership's direction, limit the person's access to accounts and systems. Standard crime forms end coverage for a person as soon as leadership learns of a theft or dishonest act by them, so that person shouldn't keep handling money, signing checks or approving payments while the matter is reviewed.
7. Talk with legal counsel before any employment or volunteer action, and check whether your denomination, lender or grantors expect notice. Handle the matter with care and confidentiality for everyone involved.

30-60-90 DAY PLAN AND SIGN-OFF

Work through the checklist in three passes, starting with access and cash and ending with the insurance review.

Timeframe	Focus	Sections to complete

Days 1 to 30	Control access, offerings and cash	First days; Offerings, tithes, bank and cash; Systems and access
Days 31 to 60	Review payments, payroll and giving	Payments; Payroll and pastoral compensation; Giving and fundraising; Property
Days 61 to 90	Close gaps and review insurance	Retirement and benefit plans; Crime insurance review; Red flags

Sign-off

☐ Checklist completed by: _____ Date: _____

☐ Reviewed by (finance committee, deacon, elder or trustee chair): _____ Date: _____

☐ Findings shared with our insurance agent by: _____ Date: _____

Prepared by MinistrySure Insurance

If you'd like a second set of eyes on how your crime coverage fits the way your church handles money, we're glad to talk it through. Call (770) 716-0180 or visit ministrysure.com.

This checklist is general risk-management guidance, not legal, tax, accounting or insurance advice. Coverage depends on the terms of the policy actually issued, which vary by carrier. Talk with your CPA, attorney and insurance agent about your situation. Tax and ERISA figures are current as of November 2026.