

Best Practices- Internal Controls for Financial Operations

Our insurance serves you so you can serve God.

Serve God



1. Our Current Environment: Perfect Mix

- Operate physically and virtually
- Social Pressure
- Economic Downturn
- Political Uncertainty/Unrest



2. Goal of Internal Controls

- Goal to use Internal Controls to protect the assets of your ministry from misappropriation and fraud
- Stewardship/Fiduciary Duty
- Stability
- Integrity



3.

Session Objectives

- Review of best practices for accounting/operational controls
 - Cash cycles
 - Receipts/Expenses
- Cybersecurity best practices



4. Protect Assets

- Policies and Procedures to protect your ministry's assets:
 - Contributions
 - Property
 - People- Employees and Volunteers
 - Reputation



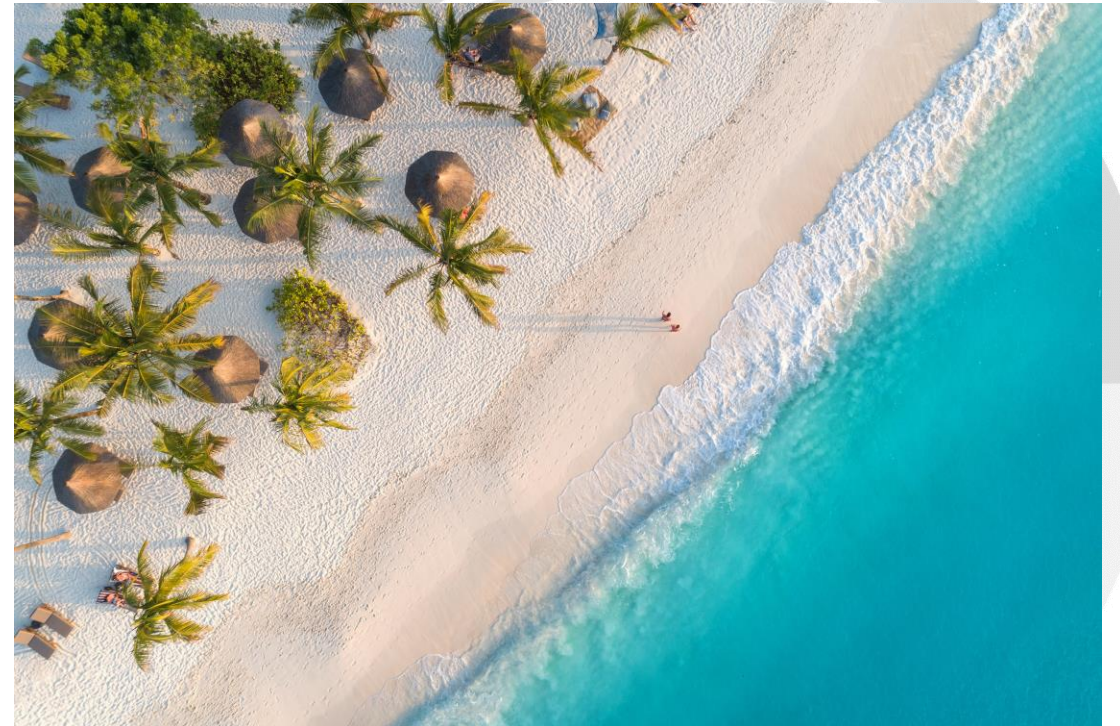
5. Key Players

- Bookkeeper/Accountant
- Accounting Manager/IT dept.
- Treasurer
- Finance Committee/Audit Committee
- Board of Trustees
- Pastor



6. Why Internal Controls Matter

- No accountant/financial manager/volunteer is an island
- Oversight and Review are essential
- Internal Controls are important for congregations no matter the size



7. Crime/Fidelity Claims

Claim Lessons Learned

- Church part-time treasurer stole money from church account.
- Theft occurred over a long period of time.
- Treasurer ran fraud operation and was convicted of embezzling millions from his employer.
- Had prior conviction for filing false tax returns.



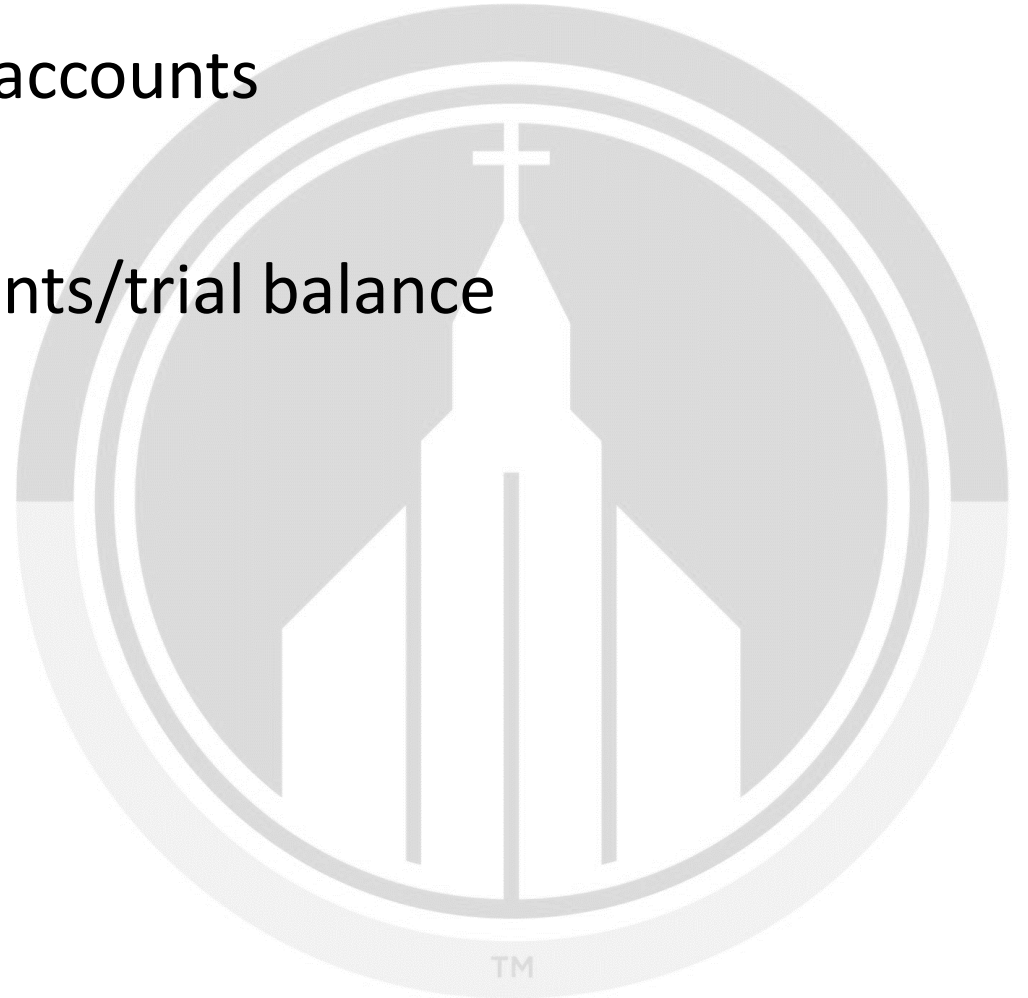
8. Preventative Controls

- Approve transactions
- Segregation of Duties- each task to complete a function is performed by a different person
- Access Controls- checks, systems, donor lists
- Standard Documentation- accounting/operational manual



9. Review Controls

- Reconciliations – bank statements and accounts
- Varying levels of Authority
- Timely preparation of financial statements/trial balance
- Audits/Reviews- external and internal



10. Cash Counting Internal Controls

- Cash Counting procedures
 - Restrictively endorse checks
 - No related count teams
 - Money counted immediately after services
 - Deposit made day of receipt



11. Cash Receipts Procedures-NOT USED

- Gifts are always in dual control- preventative control
 - Counters collect, escort and process contributions
- Standardized form and process- preventative and review
 - Photocopy checks
 - Restrictively endorse checks
 - Clear separation of duties between counters



12. Online Giving

- PCI compliance for on-line giving
- Contributions received electronically
 - Givelify
 - Zelle
 - Venmo



13. Gift Acknowledgement

- Send quarterly statements of giving
- Add a personal note from the pastor
- Let the giver know of church news
- Tax statement that no goods or services were received in exchange for the contribution



14.

Expense Cycle

- Match Vendor Invoices with Supporting Documents
- Check runs on specified dates with appropriate approval
- Review automated bills including credit card charges
- New vendors reviewed and approved



15. Expense Cycle

- Checks run by one individual and signed by someone else
- Unused checks should be locked at all times
- Review automated bills including credit card charges
- Travel and expense policy should be adhered to



16. Credit Card Expense Transactions

- All expenses including regularly occurring charges should be reviewed
- Use of credit card should be limited
- Monthly statements and transactions approved before payment



17.

Banking Transactions

- If paying by ACH or wire instructions (payments or investments) should be entered by one individual and approved by another
- Vendor data should be reviewed prior to submission and approval



18.

Internal Review

- Group of 3 -5 volunteers
- Reviews two months of activity
 - Deposits
 - Checks
 - Bank statements



19. Internal Review

- Summarize results
- Share Findings
 - Errors and corrections
 - Adherence to policies and procedures
- Makes Recommendations



20.

External Audits and Reviews

- Audits transactions throughout the period under examination
- Tests internal controls that the ministry has in place
- Provides donors with confidence
- May recommend additional policies or procedures
- Audit includes an opinion; review does not



21. Cybersecurity Controls

- Connected Devices- over 50 billion
- Lots of data to mine and exploit
- Each piece is an opportunity for fraud



22. Cybersecurity Threats

- Ransomware- malicious software designed to block access to a computer system until a sum of money is paid; files are encrypted so users are denied access
- Phishing- a form of social engineering where attempts are made to acquire sensitive data through a fraudulent email
- Spear-Phishing- a form of phishing in which the email appears to be from a trusted source

23. Cybersecurity Investments

- Employee Training
- Back-up procedures- multiple
- Firewalls
- Network/Software updates



24. Cybersecurity Investments

- Establish IT policies and recovery plans
- Back-up procedures- in the cloud/physical
- Use complex passwords and consider use of a password keeper such as Last Pass, Dash Lane or Keeper
- Separate wifi for church operations and congregants
- Firewalls
- Network/Software updates



25. Internal Controls to the Rescue

- Church secretary received an email from Sr. Pastor requesting bank info updated for new direct deposit. Email contained a form to input the bank information.
- Email appeared to be legitimate = looked like Sr. Pastor work email.
- Church secretary completed the form & forwarded it to the church payroll company.
- Church I.T. double-checked IP address & found the email came from Nigeria.

Counting Duties- this can be part of the presentation around slide 10

- Counts cash
- Photocopies checks
- Runs tape from copies
- Compares tapes
- Prepares deposit slip
- Signs forms
- Deposit is made in a locked bag

- Opens and verifies information in envelopes
- Run tape of checks
- Counts cash
- Compares tapes
- Prepare counter form
- Signs Form
- Receipt is given to Treasurer