Internal Controls

1. Introduction

"For we are taking pains to do what is right, not only in the eyes of the Lord but also in the eyes of men" (2 Corinthians 8:21, NIV).

When Paul wrote those words, he was talking about how he was managing the money raised by the early churches in Greece and Macedonia that was to be taken to Jerusalem and distributed there amongst the believers suffering from a great famine. He wanted the money to be administered properly and transparently.

2. Why set up internal controls?

Internal controls can be used to set out clear lines of authority for incurring expenditures. In addition, they are useful for the prevention of fraud.

It is a sad fact that fraud in Christian organisations is not unknown. This has been the case ever since the earliest of times (see Joshua 7: 19-21), and modern times are no different. Most Christian organisations have a "high trust" culture due to the nature of the people serving in them. Indeed, there is generally a reluctance to give an impression that a Christian worker or volunteer could be distrusted. However, internal controls are not actually about trust – they are about accountability. "High trust" without "high accountability" is a recipe for disaster. The undeniable fact is that *every fraud is committed by a trusted person*.

Fraud will occur when 3 factors coincide:

- *A need*. A person has either internal or external motivation to acquire additional resources. This could include medical needs, a divorce, or even just trying to impress someone.
- *An opportunity*. A person is presented with an opportunity to acquire funds or assets and they convince themselves that they will not get caught.
- *A rationalisation*. A person finds a way to rationalise what they are doing, so they are comfortable committing the fraud. This could be a perception of being unappreciated, underpaid, or even thinking their actions will only result in a short-term loan.

The purpose of setting up internal controls is to attempt to minimise the "opportunity" factor.

3. Setting the balance

Paul referred to "taking pains" to do what is right. Everyone who has been involved in an organisation where internal controls have required two people to be involved in a process, or the need to obtain a signature from another person, or the completion of a form and submission of evidence (ie, just about all of us!), will have muttered under their breath about how painful "taking pains" can be in practice. And it's true that having too many rules, or rules that are too complex, will cause an organisation to grind to a halt.

So, it's a matter of setting the right balance for your organisation, depending amongst other things, on your staff numbers, turnover, mission field and risk profile.

4. Culture of compliance

Just as important as setting internal controls in place is following them in practice. An organisation can have the best set of controls in the world, but if nobody takes any notice of them, or if they are not consistently applied, they are worthless.

It is *absolutely critical* that the senior management of the organisation sets the example for following internal controls. Staff take their cues from the behaviour of their leaders. If the leaders flout the rules themselves, override them in all too frequent "emergencies" or consistently gripe about them, then the controls may as well not exist.

Where the leadership believes, teaches and models that faithful administration is a biblical mandate, a major fraud is unlikely to occur.

5. General Principles – duality and change

The general principle of internal controls is to involve more than one person in any situation where your organisation's assets could be diverted to someone else's use. As a further refinement, and to prevent collusion, it is important to change the duties of particular individuals around from time to time. This usually happens naturally as staff and volunteers come and go, or as position descriptions change, but if one person holds the same trusted position for a long time, the risk increases.

6. Sample controls

Every organisation is different, so the controls for your organisation will be different from another organisation. However, there are some general principles which apply to all organisations and some risk areas which are common to most.

Authorities for expenditures

It is common practice to have clear thresholds for authorising expenditures. These will always vary depending on the size of the organisation, but for the sake of an example, they could be as follows:

> Department/Program Head – expenditures up to $1,000 (if already allocated in budget)
>
> Finance Director/Treasurer – expenditures up to $5,000 (if already allocated in budget)
>
> CEO/Senior Pastor – expenditures up to $5,000 (if not already allocated in budget) and unlimited (if already allocated in budget)
>
> Board – all other expenditures

Revenue collection

If cash is being received (eg church offerings, or donations at a function), then split up the duties. At minimum, the following duties should be separated to prevent theft:

- Collecting cash
- Preparing bank deposits
- Reconciling bank statements
- Posting receipts to the general ledger/contribution system

More specific sample controls for cash follow, depending on your own organisation:

- Collect cash in sealed containers, and/or have two people collecting and providing receipts.
- Organise the specific counting place, so that incoming offerings/donations are opened in a visible area, free of blind spots.
- Whenever possible, place two employees or volunteers in charge of the counting.
- Consider installing a video camera in the counting place.
- Do not allow offering counters to keep purses, briefcases, or other similar items in the area where counting occurs.
- Consider carrying out a background police check of all people who may be involved in handling cash.

If money is being received electronically, understand the three processes included in all e-giving setups, and the safeguards that go along with them:

- Giving Process. Typically, the organisation collects credit card information and, possibly, bank account information through an online giving platform, such as GivingKiosk, PushPay, and SecureGive. Data security on the giving platform is essential.
- Payment Processor. This is the entity which provides a platform to the giver to allow the giver to make the payment (also called the merchant account provider, eg Visa or Amex). It processes the gift and delivers it to the organisation's financial institution.
- Giver Management System. While some payment processors and their platforms have the option of processing and providing gift records, most organisations manage their own gift records on their own IT systems.

The following steps will help establish internal controls vital to security in digital giving:

- Build a strong, multi-person relationship between your organisation and the Payment Processor. In particular, have multiple approvals necessary for any change in the payment process (eg, change of bank account destinations).
- Limit access to your organisation’s Giver Management System.
- Have a different person from the person(s) having the relationship with the Payment Processor be responsible for providing receipts or payment confirmations to the givers.
- Regularly reconcile digital gift accounts. This includes reconciling bank accounts to payment processor transaction reports, gift records to payment processor transactions reports, and gift records to bank accounts.

Expenditures

(a) Normal payments

At a minimum the following duties should be segregated:

- Authorisation of expenditures (see above)
- Writing cheques

- Signing cheques/approving electronic transfers

In addition, it is appropriate to require all cheques/electronic transfers to require dual signatories/electronic authorisations.

(b) Credit Cards/Expenses

For general expense reimbursement, credit cards in the name of the organisation, or reimbursement of personal credit cards:

- Require substantiation within a set period (eg 14 or 30 days)
- Substantiation to include original receipts and documentation of the time, place, amount, and purpose of expenditure (and if other people are involved, the names of the other people)
- Approval of reimbursement to be by a supervisor. If necessary, the CEO's expenses could be approved by the Chair.

Other

(a) Payroll

Intermittently review payroll records, to ensure there are no "phantom employees" or unauthorised bonuses being paid.

(b) International payments

If you regularly send money overseas:

- Confirm banking details of recipients of payments, and double check with a different person any change of banking details.
- Require receipts of funds received.
- Require reporting back on the use of funds.
- For significant and long-term recipients of funds, it may be appropriate to carry out due diligence before the first payment and over time make periodic site visits.
- If appropriate ask for recipient's accounts to be audited annually.
- Check Australian and international Counter Terrorist and Anti Money Laundering lists.

(c) Asset usage

If your organisation's assets are used off-site (by staff or on loan), have a policy on such usage, eg:

- All equipment loans (except as specified) to be approved by supervisor.
- Keep a register of borrowed equipment, including name and contact details of borrower, description of equipment, date of loan and anticipated return date and actual return date.
- Carry out periodic stocktakes (eg monthly, quarterly or annually as appropriate).

7. Reporting Financial Wrongdoing

Should employees and volunteers be encouraged to raise concerns about financial wrongdoing in a Christian organisation? Australian culture is averse to "dobbing in", but the answer should be a resounding "Yes" for at least three reasons:

- It helps create a culture of transparency, empowering employees and volunteers to "see something, say something."
- It gives the organisation the opportunity to address minor issues before they become serious problems.
- Most instances of fraud are detected by reports of wrongdoing from employees and others.

Standard 8.7 of the CMA Standards Council Principles and Standards of Responsible Stewardship requires your organisation to:

> "maintain and publicise a mechanism for members, donors, staff, volunteers and other interested parties to submit feedback or register a complaint with the organisation, and respond in a timely and appropriate manner."

A well-constructed process would include whistle blower protections for staff/volunteers who seek to raise questions around financial issues. We refer you to our Resource Paper on Complaints Policies for further assistance in this regard.

8. Annual Review

Standard 6.6 of the CMA Standards Council Principles and Standards of Responsible Stewardship reads as follows:

> "At least once every three years the governing body or a committee of the governing body containing at least one governing body member must review the appropriateness of the organisation's policies and procedures relating to internal controls, segregation of duties and expenditure approval policies, taking into consideration the size and capacity of the organisation."

The reason we require reviews of your internal controls is that organisations change over time, so that the controls which were appropriate at one time may no longer be appropriate at another time. We require reviews to take place at least every 3 years, but there may be reasons why it could be appropriate for you to do so more often (eg, a change in the law, a new program, a major change in funding or staffing). While it will be the job of management to implement the internal controls, it is the job of the governing body of the organisation to ensure that those controls are and remain appropriate. We suggest that the members of the reviewing group (whether that is the whole governing body or an appropriate committee of the governing body) should take time to read over the existing policies and controls to ensure that they are still relevant and appropriate. If so, that can be noted in the minutes. If not, the CEO or the CFO (as appropriate) should be asked to draft amendments to the policies and controls for approval by your governing body.