Are you protecting your church or agency against fraud?

One of the most serious threats to the success of any organisation is fraud. Misplaced trust, inadequate hiring and supervision policies and a failure to implement strong internal controls can lead to an environment that is ripe for internal theft and fraud.

Fraud is more common in the church than most believe and can have various impacts on the church and seriously affect its reputation. It is about opportunity. If there are no measures in place to limit the opportunity for fraud, temptation is easily created, which exposes the church to a greater chance of fraud.

For every fraudulent activity, there is a breakdown of internal controls.

The following strategies will help protect the ministry activities of your church or agency (Please forward this to your Church Treasurer):

Never leave blank cheques with one signature already completed

All Uniting Church entities require two signatures to authorise a payment. This is to ensure that each purchase has been appropriately approved, accounted for and to encourage security of funds. With one signature already complete, if your cheque book is stolen the offender is already half way to gaining unauthorised access to your funds. **Therefore under no circumstances should a cheque signatory sign a blank cheque without the payee details included.**

Segregation of duties

It is important to segregate duties among different people to reduce the risk of error or inappropriate action. Normally, responsibility for authorising transactions, recording transactions (accounting) and handling the related asset (custody) eg banking of cash, are divided.

Having two cheque signatories is one way to achieve segregation of duties, however with this responsibility cheque signatories should always sight supporting

documentation and initial the invoice as evidence of their approval before they sign the cheque.

Never write down or share your internet banking passwords

Payments from church accounts can be made through internet banking if two signatories enter their passwords. The authoriser should sight properly approved supporting documentation prior to approving the payment. The second authoriser should print off the payment confirmation as evidence of proper approval.

Don't write down or share your password as it compromises the accountability and security of church funds, as well as breaching the Terms and Conditions of your internet banking contract with the bank.

Perform regular accounting reconciliations

Regular, appropriately performed reconciliations (such as bank reconciliations, UCA Fund account reconciliations and analyses between budget and actual figures), can make fraud concealment very difficult. Therefore bank reconciliations and other financial reconciliations should be completed on a monthly basis and should be approved by Church Council or other Church oversight body.

Perform regular activity monitoring

Regular spot checks in key risk areas, such as outgoing invoices, EFT and other cash payments and cash receipts will help uncover discrepancies, as well as show employees and volunteers that church activities are subject to regular review by internal audit, external audit and Church Leaders.

If you haven't done all you can to protect your church against fraud, you're putting ministry resources at risk.

If you have any questions about this please contact:

Chris Kirwan

Internal Audit Manager
Administration & Finance
130 Little Collins St Melbourne 3000
t (03) 9251 5258 | f (03) 9654 4179 |
e Chris.Kirwan@victas.uca.org.au
w victas.uca.org.au

Uniting Church in Australia
SYNOD OF VICTORIA AND TASMANIA