

Risk Management

Sample Parish Fraud Prevention Checklist

The following checklist is intended to provide general information to assist parishes to assess and reduce the risk of fraud. Please note that this is not an exhaustive checklist of all possible procedures or controls you might use to prevent fraud.

Understanding the risks that your parish is exposed to will assist you to put in place measures that reduce the incidence of fraud.

The parish fraud prevention policy should be consistent with best practice prevention programs and standards. The parish may need to seek professional advice for specific fraud prevention measures.

Where the parish answers the question with a "no", further investigation of the risk and possible control measures should be identified and implemented.

I. Parish Management Commitment and Approach to Fraud Prevention

- | | | |
|-------|---|--|
| I.1 | Do parish management communicate and make available the Fraud Prevention Policy and Procedures for parish staff and parishioners that assist with parish assets? | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| I.2 | Do staff and volunteers receive training in Fraud Prevention Procedures and their responsibility to report any suspected fraud? (eg. is this included in the induction programs for new staff?) | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| I.3 | Do parish management ensure that the Fraud Prevention Policy and Procedures are followed by all parish staff by providing supervision and review of processes and financial statements? | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| I.4 | Are there clearly defined reporting procedures in place for employees or parishioners to report cases of suspected fraud to parish management? | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| I.4.1 | Are there procedures in place to protect whistleblowers who report fraudulent activities? | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| I.5 | Is the parish's commitment to pursuing and taking legal action against the person(s) responsible for any fraudulent activity communicated to employees and parishioners? | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| I.6 | Is there adequate Fidelity Guarantee Insurance held for the parish businesses and operations? (This can be determined by contacting your Account Executive at Catholic Church Insurances on 1 300 655 001.) | <input type="checkbox"/> Yes <input type="checkbox"/> No |

2. Parish employee and volunteer practices

- 2.1 Are pre-employment checks of employees and volunteers carried out including: verification of identity, criminal record checks, referee checks, and verification of qualifications? Yes No
- 2.2 Is there a parish organisational structure? Yes No
- 2.3 Do staff role descriptions include:
- 2.3.1 Authorisation levels where necessary, Yes No
- 2.3.2 The duty to report financial discrepancies or suspected fraud to management, Yes No
- 2.3.3 The duty not to disclose any private financial information to a third party and Yes No
- 2.3.4 The expected code of conduct? Yes No
- 2.4 Are service level agreements in place for contractors at the parish including code of conduct, work performance and defined tasks? Yes No
- 2.5 Are staff regularly educated on Fraud Prevention Procedures? Yes No
- 2.6 Is there a policy for leave accumulation? Yes No
- 2.7 Are staff duties rotated on a roster? Yes No
- 2.8 Are money collections banked within 48 hours? Yes No
- 2.8.1 Is there a defined limit for the maximum amount of cash that can be held at the parish at one time? Yes No
- 2.9 Is access to the room containing the parish safe and financial documents restricted to nominated parish management by the use of a restricted key system? Yes No
- 2.10 Are parish keys stored out of sight in a locked cabinet or safe? Yes No
- 2.10.1 Is the key to the safe restricted to nominated parish managers? Yes No
- 2.11 Is there a parish Asset Register listing all physical and financial assets owned by the parish? Yes No
- 2.11.1 Are regular stocktakes conducted to keep the asset register current? Yes No
- 2.12 Are parish budgets forecasted for regular business operations? Yes No
- 2.12.1 Are the budgets and actual financial performance compared for discrepancies and reported? Yes No
- 2.13 Are all high risk areas for fraud identified within the parish operations and business including but not limited to: cash, access to bank accounts and assets that could easily be removed? Yes No
- 2.14 From the high risks identified, is the likelihood and consequences of the risk of the fraud assessed? Yes No
- 2.15 Are appropriate procedures and risk controls put into action to prevent these risks occurring? Yes No
- 2.16 Are regular parish meetings conducted to discuss financial reports and budgets? Yes No
- 2.16.1 Are the minutes of the meetings recorded? Yes No
- 2.17 Are there written procedures for the evaluation and selection of investment funds and assets to achieve the best outcomes for the parish? Yes No
- 2.18 Are procedures written for the financial authorisation limits for all staff including: cheques, credit cards, investments, purchases, petty cash etc? Yes No
- 2.19 Are controls for these limits in place? (eg. maximum limits of cheque accounts and credit cards are confirmed in writing with the bank) Yes No
- 2.20 Are written procedures kept for all financial areas including money collection, money counting, banking, cheques, credit cards, contractor payments, reconciliation, and audits etc? Yes No
- 2.21 Do cheques have two signatories with the appropriate authority levels? Yes No

- 2.22 Is petty cash kept to a nominated limit? Yes No
- 2.23 Are cash counting and banking signed off by at least two people and supervised by a senior parish member at all times? Yes No
- 2.24 Are financial transactions recorded regularly so that unauthorised transactions are immediately identified? Yes No
- 2.25 Are reconciliations conducted for all cheques, credit cards, investments and bank accounts with discrepancies reported? Yes No
- 2.26 Are there written procedures for fraud reporting, investigation and disciplinary actions Yes No
- 2.26.1 Are staff aware of their responsibilities and accountable for their actions?
- 2.27 Do parish management ensure that all staff are complying with the fraud prevention procedures through supervision and review of financial records? Yes No

3. Segregation of duties

- 3.1 Are the duties of accounting reconciliation review and the accounting functions segregated? Yes No
- 3.2 Are bank statements, investments credit and cashbooks reconciled by a separate person in a timely manner to detect discrepancies? Yes No
- 3.3 Are the duties of money collecting/payments segregated to the duties of the person providing the accounting function? Yes No
- 3.4 Is the administration of parish funds supervised by a parish manager? Yes No
- 3.5 Is the internal and external audit of parish finances conducted by a person separate to the parish fund administrator? Yes No

4. Parish Data Protection Procedures

- 4.1 Are files containing financial or personal information stored in lockable two hour fire rated cabinets in a secure storage room? Yes No
- 4.2 Is a key register/security card register maintained to control key access? Yes No
- 4.2.1 Is the register reviewed when personnel changes occur? Yes No
- 4.3 Are filing cabinet keys for cabinets containing financial and/or personal information kept in a lockable key safe and signed out and in after use? Yes No
- 4.4 Are all computers protected by passwords and locked whilst not in use with a timed password security process to protect computers if staff are away from their desk? Yes No
- 4.5 Is all computer equipment installed with Firewalls and Anti-virus software and regularly updated? Yes No
- 4.6 Is all parish financial or personal information contained in-house? Yes No
- 4.6.1 Is the use of portable back-up devices such as data sticks and portable hard drives prohibited, unless expressly required for business continuity purposes? Yes No
- 4.7 If financial and/or personal records are to be stored off-site for business continuity purposes, is the information backed up by a senior member of staff and stored in a secure data storage facility? Yes No
- 4.8 Are paper documents and electronic records shredded when required to dispose of information, by either of the following ways: Yes No
- Shredded via a data shredder?
 - Degaussed (de-magnetising magnetic media for example hard drives)?
 - Physically destroyed (eg. incineration or pulverisation etc?) **(this should be undertaken by a suitably qualified individual in accordance with EPA guidelines)**
- 4.9 Are data protection procedures reviewed for effectiveness and amended if deemed necessary by a member of management or Parish Priest? Yes No

5. Review process

- 5.1 Is there a parish Fraud Prevention and Control Review checklist completed at least annually? Yes No
- 5.2 Are regular internal audits conducted for the following control areas? Yes No
- Account balances and accounting records
 - Parish and Personnel practices
 - Duty segregation practices
 - Data and data protection practices
- 5.3 Is an independent party engaged to conduct external audits of the parish finances annually? Yes No
- 5.4 Are the internal and external financial audit reports reviewed by parish management and the findings investigated? Yes No
- 5.5 Where current controls are deemed ineffective or out-dated, are revised risk controls implemented? Yes No

How to Contact Us

CCI's Risk Management Help Desk
Telephone 1300 660 827