Lithgow CITY COUNCIL

DRAFT

9. GOVERNANCE

Policy 9.2

FRAUD AND CORRUPTION CONTROL PLAN

Version 1

1. PLAN

The plan gives guidance and direction to Council officers and stakeholders on the processes for:

- preventing fraud and corruption;
- detecting fraud and corruption in Council; and
- responding to fraud and corruption in Council.
-

The plan aims to:

- reduce the potential for fraud and corruption within and against Council;
- build a culture which seeks to prevent fraud and corruption;
- explain how Council deals with suspected fraud and corruption through risk management practices; and
- provide guidance on how any suspected instances of fraud or corruption are dealt with by Council.

This plan is comprised of three stages: prevention, detection and response. Distributed across these three stages are the ten attributes taken from the Audit Office of NSW's Fraud Control Improvement Kit (February 2015).

The plan also references the NSW Auditor-General's Report on Fraud Control in Local Councils (June 2018).

1.1 Fraud Control Checklist

Attribute 1: Leadership

1. CEO and senior management commitment to fraud control:
    - CEO visibly endorses fraud control activities;
    - senior managers demonstrate their commitment to mitigate fraud risks.

2. Clearly defined CEO and senior management accountability and responsibility:
    - senior management assigned responsibility for implementing the fraud control framework;
    - senior managers' individual performance agreements contain performance measures and indicators relating to successful fraud control;

Attribute 2: Ethical framework

3. Clear policies setting out acceptable standards of ethical behaviour:
    - staff have easy access to ethical behaviour policies (Code of Conduct);
    - ethical behaviour policies are included in the induction process.

4. Demonstrated compliance with the ethical framework:
    - staff annually evidence their commitment to acceptable standards of behaviour.

5. Employees can articulate obligations to ethical behaviour and the organisation's position on fraud:
    - staff understand fraud is not tolerated and the consequences of committing fraud.

Attribute 3: Responsibility structures

6. Management and all staff have clearly defined responsibilities for managing fraud:
    - staff are aware of the responsibility structure in the organisation;
    - responsibilities for fraud control are contained in role descriptions, where appropriate.

7. Fraud management is integrated with core business:
    - managing fraud risks included in business unit plans.

8. Resources are allocated to managing fraud:
    - Fraud Prevention Manager duties allocated to a Director role.

9. Clearly defined roles for audit and risk committee and auditors:
    - proactive and influential audit and risk committee;
    - internal audit work covers controls over high risk fraud areas.

10. Staff with responsibility for fraud control and staff in high risk fraud areas are provided with training:
    - refresher and knowledge update training are provided on an ongoing basis;
    - external training program is integrated within a wider education and awareness campaign.

Attribute 4: Fraud and corruption control policy

11. Risk-based policies appropriate to the organisation:
    - fraud and corruption control policy addresses the level and nature of internal and external fraud risks;
    - fraud and corruption control plan addresses the ten attributes of fraud control.

12. Holistic and integrated:
    - fraud and corruption control policy does not operate in isolation and has strong links to other ethical behaviour policies (Code of Conduct).

13. Regularly reviewed, current and implemented:
    - fraud and corruption control policy is responsive to changes in the operating environment and reviewed at least every two years.

Attribute 5: Prevention systems

14. Proactive and integrated fraud risk assessment:
    - fraud risk assessment is part of organisation's enterprise risk management process;
    - risk assessment reviewed after substantial change and at least every two years.

15. Planning, follow up and accountability:
    - fraud control plan in place and outcomes reported to the Executive Management Team and audit and risk committee;

16. Analysis of and reporting on suspected and actual frauds:
    - fraud database established containing all reports of fraud, action taken and outcomes;
    - database kept up to date and published on website.

17. Ethical workforce:
    - pre-employment screening.

18. IT security strategy:
    - specific IT security strategy aligned with the organisation's business strategies;
    - cybercrime included as a risk on the risk register.

Attribute 6: Fraud awareness

19. Comprehensive staff education and awareness program:
    - ongoing ethical behaviour and fraud education and awareness program;
    - fraud control message repeated and reinforced using a variety of communication channels;
    - fraud control expectations included in the induction process;
    - staff have a good understanding of what fraud is;
    - guidance material deals with real life situations, conflicts and fraud risks staff face in their work area.

20. Staff awareness of fraud control responsibilities:
    - staff have a good appreciation and understanding of their responsibilities for preventing, detecting and reporting fraud.

21. Customer and community awareness:
    - publicity campaigns developed where appropriate;
    - customers and the community encouraged to report suspicions of fraud and provided with easy to use channels to make reports;
    - customers and the community have confidence in the integrity of the organisation;
    - statement of business ethics setting expectations and mutual obligations.

Attribute 7: Third party management systems

22. Targeted training and education for key staff:
    - targeted training and education programs for staff with responsibilities for dealing with third parties.

23. Third party due diligence and clear contractual obligations and accountabilities:
    - structured risk-based due diligence before engaging contractors or third parties;
    - contracts and service level agreements include clear accountabilities for managing the risk of fraud;
    - position descriptions for staff with responsibilities for managing third parties include accountabilities for managing fraud risks.

24. Effective third party internal controls:
    - specific internal controls relating to third parties in place;
    - checks and reviews carried out on dealings with third parties.

25. Third party awareness and reporting:
    - contractors and suppliers understand Council will not tolerate corruption including fraudulent dealings;
    - statement of business ethics setting expectations and mutual obligations;
    - reporting mechanisms established for reporting suspected fraud;
    - contractors and suppliers encouraged to provide information if they suspect fraud is occurring.

26. Staff disclosure of conflicts of interest and secondary employment:
    - staff regularly required to disclosure conflicts of interest and secondary employment;
    - records of conflicts of interest and secondary employment reviewed and kept up-to-date.

Attribute 8: Notification systems

27. Culture that supports staff reporting fraud and management acting on those reports:
    - well-publicised options for staff to report fraud;
    - staff feel confident they will be protected from reprisal action;
    - demonstrated action taken in response to reports of fraud.

28. Polices, systems and procedures that support reporting:
    - reporting system appropriate to organisation;
    - different channels available to report fraud;
    - feedback and follow-up with internal reporters.

29. Processes to support upward reporting:
    - actual and suspected frauds reported to General Manager and audit and risk committee;
    - fraud database published on organisation's website.

30. External reporting:
    - staff are clear on policy and procedures for external reporting;
    - external reporting in accordance with legislation and policy;
    - clear and consistent approach to external reporting.

Attribute 9: Detection systems

31. Robust internal controls:
    - well documented risk-based internal controls;
    - routine checks of activities, processes controls and transactions;
    - range of internal controls that 'prevent, detect and correct'.

32. Monitoring and review:
    - available data monitored and reviewed to ensure irregularities and warning signals are picked up early;
    - early warning signs acted on quickly and red flag behaviour recognised.

33. Risk-based internal audit program:
    - internal audit program evaluates the potential for fraud and how fraud risk is managed;
    - internal audit recommendations assigned to individuals with timeframes for response.

Attribute 10: Investigations systems

34. Clear documented investigation procedures:
    - reports of fraud investigated promptly and to the highest standards;
    - investigations are independent;
    - sufficient resources allocated, including budget.

35. Investigations conducted by qualified and experienced staff:
    - investigations conducted by appropriately qualified personnel with recognised qualifications and appropriate experience.

36. Decision-making protocols:
    - documented decision-making processes;
    - proportionate responses to incidents of fraud.

37. Disciplinary systems:
    - staff understand fraud will not be tolerated and the perpetrators will face disciplinary action;
    - commitment to taking action against the perpetrators of fraud;
    - consistent application of sanctions.

38. Insurance:
    - obtain a fidelity guarantee insurance policy to protect against the financial consequences of fraud.

1.2 Risk Assessment

This risk assessment methodology gives an overview of the fraud risk assessment process and contains examples of the type of fraud risks and internal controls. Different organisations and different areas within your business may have different fraud risks and the examples are not an exhaustive checklist. The risk assessment deliberately does not include actual ratings for the effectiveness of internal controls, the results of the risk analysis, the options for the residual fraud risk or further treatment plans. Each organisation needs to undertake its own risk analysis and determine its own risk appetite.

1.2.1. Type of fraud risk

This column should include the potential fraud risks your organisation may face. Please specify any additional risks in the relevant section.

1.2.2. Existing controls

Once the potential fraud risks are identified, identify what controls currently exist to reduce each fraud risk.

1.2.3. Effectiveness of the existing controls

Assess how well controls are operating and if they are mitigating fraud risks as intended. Only one rating should be made for each fraud risk taking into consideration all controls existing for that risk. A scale of 1 to 5 is used.

1	There is a very high exposure to fraud (almost certain)
2	There is a high opportunity for fraudulent activity (likely)
3	There is a moderate opportunity for fraudulent activity (possible)
4	There is a low opportunity for fraudulent activity (unlikely)
5	There is no apparent opportunity for fraudulent activity (rare)

1.2.4. Fraud risk analysis

After considering how effective the controls are in step 1.2.3 above, the consequence and likelihood of each risk is assessed. By progressing in this order, this framework intends to assess the identified fraud risks on a residual basis, that is, after existing controls.

Impact / Probability	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	Medium	Medium	High	Extreme	Extreme
Likely	Low	Medium	High	Extreme	Extreme
Possible	Low	Low	Medium	High	Extreme
Unlikely	Low	Low	Low	Medium	High
Rare	Low	Low	Low	Low	High

1.2.5. Option for residual fraud risk

After considering the internal controls, determine if the residual fraud risk is at an acceptable level. If the residual fraud risk is acceptable, then there is no need for further action.

However if either:

(a) properly designed controls are not in place to address certain fraud risks, or

(b) controls identified are not operating effectively to sufficiently reduce the residual risk to an acceptable level

then action must be taken.

1.2.6. Further treatment/action necessary to address residual fraud risk

Where further action must be taken, the response should be to change or enhance existing controls or to implement additional controls.

2. REVIEW

The General Manager will review the plan every 2 years.

Maintained by Department:	Governance	**Approved by:**	Council		
Reference:	Council Plan	**Policy No:**		**Effective Date:**	
Min No:	EMT endorsed Jan 2019	**Version No:**	1	**Reviewed Date:**	
Attachments:	Nil.				