# ARF010 Data Governance Risk

## Risk Status Progress Report December 2020

Prepared: 30/10/20

### Description of risk and impact

| Because of | There is a chance that... | leading to... |
|---|---|---|
| Lack of formal data governance | Data quality may be negatively impacted<br><br>Data may be inappropriately used<br><br>Data breach may negatively impact Council reputation<br><br>We are non-compliant with relevant legislation | Slow, ineffective decision making<br><br>Lack of confidence in data and decisions made on the data<br><br>Increased organisational risk<br><br>Mistakes/errors<br><br>Ineffective and poor processes<br><br>Inefficient customer service<br><br>Legal liability and sanction<br><br>Reputational damage to Council and Councillors |

Data is an asset. Good data, used and analysed appropriately, enables faster, transparent, decision making, reducing organizational risk.

Data governance is the overarching framework that outlines the creation, maintenance, disposal and protection of data. The objectives of data governance are:

- Assure of data security and data quality
- Maximise the benefit generation of information
- Designate accountability for data quality
- Enable evidence-based policy development
- Increase consistency and confidence in decision making
- Consistent reporting
- Enable evidence-based business cases and strategies

### Existing Treatments

A number of improvement initiatives, such as Resource Consents Vision 20/20 process improvement project and BCA improvements, have positively impacted data governance with both data and processing progress within these functions now visible.

Three active programmes of work will also result in improved data governance. These are:

1. Enterprise data warehouse programme
2. Program Darwin
3. Business Intelligence strategy.

## High level treatment plan and progress up-date:

| High level treatment plan: | Progress update: |
|---|---|
| Data governance policies:<br><br>a.  Data Governance Policy designed to manage the creation, transformation, and usage of data and related information owned by or in the care of Far North District Council<br>b.  A Data Protection Policy has also been drafted. Its purpose is to describe how personal data must be collected, handled, and stored and retrieved, in order to meet the Far North District Council's data protection standards, comply with the law, and respect individual rights.  This policy address data - collection, storage, use, accuracy, retention and protection.<br><br>To address governance the following internal policies and procedures are required:<br><br> o Policy for Data (Security, Privacy, Ethics, Retention, Sourcing)<br> o Procedures for monitoring performance<br> o Procedures for reporting on raw data (meta-data)<br> o Procedures for ensuring legislative and Audit compliance including Internal data audit<br> o Procedure for actions in event a data breach | Underway:<br><br>Several policies have been drafted and the need for additional policies identified e.g. IT Security Policy. |
| Implementation of the ALGIM (Association of Local Government Information Management) local government ICT security framework. | Underway:<br><br>ALGIM completed an audit and benchmarking exercise in October 2020 which measured the compliance status of FNDC against the ALGIM local government ICT security framework. The framework then provides a number of recommendations to improve ICT security compliance status. This is subject of separate report on the Assurance Risk and Finance December 2020 Committee Agenda. |
| FNDC needs to implement the requirements of the internal policy "PC033 Privacy Policy", adopted August 2019, such as agree designated Privacy Officers. | To start. |

## Where are the gaps? / what more could we be doing?

| Inherent Risk: | Trend | Residual Risk: | Accountable: | CEO | Date raised: | 29/11/18 | Report frequency: |
|---|---|---|---|---|---|---|---|
|  | ⬇ |  | Responsible: | Chief Digital Officer | Date accepted: | 30/05/19 | Six monthly |