Far North District Council
Te Kaunihera o Tai Tokerau ki te Raki

HE ARA TĀMATA
CREATING GREAT PLACES
Supporting our people

ARF010 Data Governance Risk

Risk Status Progress Report December 2021

Prepared: 27/10/2021

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 Data may be inappropriately used Data breach may negatively impact Council reputation We are non-compliant with relevant legislation	Slow, ineffective decision making Lack of confidence in data and decisions made on the data Increased organisational risk Mistakes/errors Ineffective and poor processes Inefficient customer service Legal liability and sanction Reputational damage to Council and Councillors

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

- Assure 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

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

1. The Enterprise data warehouse programme.
2. Program Darwin: this is now recognized as a strategic organisational risk on the top risk dashboard as ARF014 Programme Darwin
3. The Business Intelligence strategy.

High level treatment plan and progress up-date:

High level treatment plan:	Progress update:
Data governance policies	Underway: ICT Operations and Delivery team are implementing an online IT Policy System in collaboration with Kaon Security Ltd to move to a more effective IT policy environment and to provide better governance around IT use and security. This IT Policy System is an enhanced cloud-based solution that has been developed to assist organisations create, deliver, and maintain a comprehensive suite of IT policies. This system streamlines the engagement between the users and the

High level treatment plan:	Progress update:
	content, whilst providing a rich source of guidance on how they should interact with organisational IT systems and data. With security attacks against organisations like ours increasing we must ensure our systems are protected against these threats. One of the foundational steps in achieving this is to document the rules and guidelines around system management, operation, and use. By complying with these rules and guidelines we are protecting our systems. Information security is all about keeping corporate information safe. The policies address the need to protect confidential and sensitive information from disclosure, unauthorised access, loss, corruption, and interference, and are relevant to information in both electronic and physical formats. Information security can be defined in three areas: • **Confidentiality** - Information must not be made available or disclosed to unauthorised individuals, entities, or processes • **Integrity** - Data must not be altered or destroyed in an unauthorised manner, and accuracy and consistency must be preserved regardless of changes • **Availability** - Information must be accessible and useable on demand by authorised entities. Ongoing the policy system will be updated with relevant changes to legislation, standards, and guidelines.
ALGIM (Association of Local Government Information Management) local government ICT security framework.	In place and ongoing: ICT Operations and Delivery team have implemented several ICT security improvements such as device encryption, network security and setting a BIOS password. The Manager – ICT Operations & Delivery provides the Assurance, Risk and Finance Committee regular Cyber Security reports.
FNDC needs to implement the requirements of the internal policy “PC033 Privacy Policy”, adopted August 2019, such as agree designated Privacy Officers.	Implemented. The Privacy Officers are appointed by role. These roles are the Manager – Legal Services and the Legal Services Officer.

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

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