MĀWHERA
GREY
DISTRICT COUNCIL

105 Tainui St | Greymouth 7805
PO Box 382 | Greymouth 7840
Tel 03 769 8600
Fax 03 769 8603
info@greydc.govt.nz
www.greydc.govt.nz

A Meeting of the Risk and Assurance Sub-Committee Meeting will be held as follows:

Date: **Monday 19 February 2024**

Time: **3:30pm**

Venue: **Council Chambers, 105 Tainui Street, Greymouth**

Paul Morris
Chief Executive

AGENDA

Members:

Chair:	Mr Rob Caldwell
Deputy Chair:	Mayor Tania Gibson
Members:	Councillor Robert Mallinson
	Councillor Rex MacDonald
	Councillor Jack O'Connor

(Quorum 3 members)

Contact Telephone: 03 7698600
Email: trish.jellyman@greydc.govt.nz
Website: https://www.greydc.govt.nz/our-council/agendas-and-minutes/Pages/default.aspx

The information in this document is provided to facilitate good competent decisions by Council and does in no way reflect the views of Council. Reports and recommendations contained in this agenda are not to be considered as Council policy until adopted.

TERMS OF REFERENCE

Type of Committee	Council Subcommittee
Subordinate to:	Finance, Regulatory and Business Support
Subordinate Committee	None
Legislative Basis	Subcommittee reconstituted by Council as per Schedule 7, Section 30 (1) (A) Local Government Act 2002. Subcommittee delegated by powers by the Council as per Schedule 7 (Section 32) of the Local Government Act)
Membership	Independent Chair: Mr Rob Caldwell Deputy Chair: Mayor Gibson Member: Cr Robert Mallinson Member: Cr Rex MacDonald Member: Cr Jack O'Connor
Quorum	Three members
Meeting frequency	February, April, June, August and October.
Terms of Reference	The purpose of the Risk and Assurance Committee is to assist the Council in discharging its responsibilities in relation to: • The robustness of the internal control framework and financial management practices. • The integrity and appropriateness of external reporting and accountability arrangements. • The robustness of risk management system, processes, and practices. • Compliance with applicable laws and regulations. • Standards and best practice guidelines, and • The establishment and maintenance of controls to safeguard the Council's financial and non-financial assets. Areas that broadly fall under the umbrella of this committee are: • Risk management framework • Financial risk management • Health and safety risk management • Compliance with legislation

	• External audit or review of any Council activities, including but not limited to NZTA, Building Controls, Audits.
Power to Act Assurance	For Council's Annual Report, Consultation Document and Long Term Plan Audits, The Risk and Assurance Committee will: • Approve the annual external audit proposal for the Annual Report and the audit of the Long Term Plan. • Agree the appropriateness of the Council's existing accounting policies and principles and any proposed changes. • Enquire of external auditors for any information that affects the quality and clarity of the Council's financial statements of service performance, and assess whether appropriate action has been taken by management in response to the above. • Satisfy itself that the financial statements of service and performance are supported by appropriate management signoff on the statements and on the adequacy of the systems of internal control (i.e. letters of representation) and recommend to Council the signing of the financial statements by the Chief Executive / Mayor and adoption of the Annual Report. • Identify and recommend to the Council the external auditor's remuneration and the terms of their engagement. • Confirm consulting services and related fees provided by the external auditors. • Consider and review any serious difficulties or disputes which management encountered during the audit. • Consider and review any other matters related to the conduct of the audit. • Consider and review any significant findings during the audit process and managements responses.

	• Consider and review any matters considered appropriate, without the Chief Executive or other Council staff present in the meeting. • Consider and review any difficulties encountered during the audit including any restrictions on the scope of work. • Consider and review any changes required in the planned scope of the audit plan. • Consider and review the audit management letter prior to presentation to the Council. • Meet with the external Auditors at any time with or without management present as deemed appropriate by the Chairman of the committee.
Risk	Council is responsible for setting the tolerance to risk and risk culture at the Grey District Council. The Chief Executive is charged with implementing appropriate risk management systems within Grey District Council. While the responsibility for risk lies with Council, oversight of the processes to manage risk within GDC is delegated to the Risk and Assurance Committee. The Council will receive periodic reporting on those areas of risk identified by the Committee. The Risk and Assurance Committee will: • Review and approve Council's risk management framework. • Review corporate risk assessment and internal work management practices. • Receive and review Health and Safety reports. • Oversight of the processes used to manage project risks. • Review insurance arrangement annually. • Overseeing Council's systems, processes, and practices for risk management: a) Ensure that management has in place a current and comprehensive risk management framework and associated procedures for effective identification and management of the Council's

Assurance – other	significant risks (including financial and non-financial risks). b) Consider whether appropriate action is being taken by management in its treatment of risk to either accept or mitigate Council's significant risks. • Monitoring insurance claims. It is anticipated that the Council will from time to time be required by third parties to undertake an audit process. They may include by not be limited to Waka Kotahi, Building Control, MBIE. The Risk and Assurance Committee will: • Approve (if required) any other external audit proposal. • Liaising with the relevant external auditor: a) At the start of each audit, confirm the terms of engagement with the external auditor including the nature and scope of the audit, timetable and fees. b) Approve the external audit engagement letter and letter of undertaking and any additional services to be provided by the external auditor. c) Receive the external audit report (s) and review action to be taken by management on significant issues and audit recommendations raised within. d) Conduct a member only session (i.e. without any management present) with external audit to discuss any matters that the auditors wish to bring to the committee's attention and / or any issues of independence.
Conflicts of Interest	Once per year, Committee members will provide written declarations to the Mayor, stating they do not have any conflicts of interest that would preclude them from being members of the Committee.

Delegations	The Committee will in general make recommendations to Council on certain matters. Where the Committee is delegated to approve a matter this is considered a decision by the Committee.
Limits to Delegations	Matters that cannot be delegated by the Council include: • The power to make a rate. • The power to make a bylaw. • The power to borrow money, or purchase or dispose of assets, other than in accordance with the long term plan. • The power to adopt a long term plan, annual plan, annual report or strategic plan. • The power to appoint a Chief Executive. • The power to adopt policies required to be adopted and consulted on under this Act in association with the long term plan or developed for the purpose of the local governance statement. • The power to adopt a remuneration and employment policy.
Reporting Procedures	• After each meeting the Chair will report the committee's recommendations and findings to the Council. • The minutes of all meetings of the Committee will be presented to Council and to such other persons as the Council directs. • The Chair will present an annual report to the Council summarising the Committees activities during the year and any significant results and findings.
Power to Act.	Generally recommending powers only, but certain decisions can be taken by the committee.
Referral to Council	The minutes of the subcommittee serve before Council as a recommendation.
Management responsibility	Chief Executive

SUB-COMMITTEE IN OPEN MEETING

GENERAL BUSINESS AND TABLED ITEMS

Items not on the agenda for the meeting require a resolution under section 46A of the Local Government Official Information and Meetings Act 1987 stating the reasons why the item was not on the agenda and why it cannot be dealt with at a subsequent meeting on the basis of a full agenda item. It is important to note that late items can only be dealt with when special circumstances exist and not as a means of avoiding or frustrating the requirements in the Act relating to notice, agendas, agenda format and content.

LOCAL AUTHORITIES (MEMBERS' INTERESTS) ACT 1968

Sub-Committee members are reminded that if he/she has a direct or indirect interest in any item on the agenda be it pecuniary or on grounds of bias and predetermination, then he/she must declare this interest and refrain from discussing or voting on this item.

Table of Contents

1 APOLOGIES AND DECLARATIONS OF INTEREST

1.1 APOLOGIES

Nil

1.2 UPDATES TO THE INTERESTS REGISTER

Sub-Committee members to please advise if there are any changes to be made to the current Interests Register.

1.3 IDENTIFY ANY CONFLICTS OF INTERESTS IN THE AGENDA

Notification from committee members of:

1.3.1 Any interests that may create a conflict with their role as a committee member relating to the items of business for this meeting (prior to taking part in the deliberation of a particular item); and

1.3.2 Any interests in items in which they have a direct or indirect pecuniary interest as provided for in the Local Authorities (Members' Interests) Act 1968.

1.4 NOTIFICATION OF LATE ITEMS

Where an item if not on the agenda for a meeting, that item may be dealt with at that meeting if:

1.4.1 The Committee by resolution so decides; and

1.4.2 The Chairperson explains at the meeting at a time when it is open to the public the reason why the item is not on the agenda, and the reason why the discussion of the item cannot be delayed until a subsequent meeting.

2 CONFIRMATION OF MINUTES OF PREVIOUS MEETINGS

2.1 CONFIRMATION OF THE RISK AND ASSURANCE SUB-COMMITTEE MEETING HELD ON 24 OCTOBER 2023

SUGGESTED RECOMMENDATION

That the minutes of the Risk and Assurance Sub-Committee Meeting held on 24 October 2023 be confirmed as true and correct.

MINUTES OF THE RISK AND ASSURANCE SUB-COMMITTEE MEETING OF THE GREY DISTRICT COUNCIL

Held in Council Chambers, 105 Tainui Street, Greymouth

on Tuesday 24 October 2023 commencing at 3.30pm

PRESENT: Mr Rob Caldwell (Chair)

Mayor Tania Gibson (Deputy Chair), Councillor Robert Mallinson, Councillor Rex MacDonald, Councillor Jack O'Connor

IN ATTENDANCE: Paul Morris (Chief Executive), Gerhard Roux (Group Manager Support), Trish Jellyman (Democracy Advisor), Tracy Fitzgerald (Finance Manager) left meeting at 4.37pm, Colleen McGeady (Health & Safety Officer), Megan Bourke (Communications Manager)

1 APOLOGIES AND DECLARATIONS OF INTEREST

1.1 APOLOGIES

There were no apologies.

1.2 UPDATES TO THE INTERESTS REGISTER

There were no updates to the Interest Register.

1.3 IDENTIFY ANY CONFLICTS OF INTERESTS IN THE AGENDA

There were no declarations of interest.

1.4 NOTIFICATION OF LATE ITEMS

There were no late items.

2 CONFIRMATION OF MINUTES OF PREVIOUS MEETINGS

2.1 CONFIRMATION OF THE RISK AND ASSURANCE SUB-COMMITTEE MEETING HELD ON 28 AUGUST 2023

COMMITTEE RESOLUTION RA 23/10/005

Moved: Cr Robert Mallinson
Seconded: Mayor Tania Gibson

That the minutes of the Risk and Assurance Sub-Committee Meeting held on 28 August 2023 be confirmed as true and correct.

Carried Unanimously

3 AGENDA ITEMS

3.1 TREASURY UPDATE 31 AUGUST 2023/30 SEPTEMBER 2023

Refer page 16 of the agenda. The GMS spoke to this report and advised that all compliance measures from Year 1 – 10 are still valid. He welcomed any questions.

COMMITTEE RESOLUTION RA 23/10/006

Moved: Mayor Tania Gibson
Seconded: Cr Jack O'Connor

1. That the Risk and Assurance Sub-Committee Meeting receives the report.

Carried Unanimously

3.2 REPORT ON AUDIT RECOMMENDATIONS FROM MANAGEMENT LETTER

Refer page 22 of the agenda.

The Chairman advised that this report includes both the previous management letter and the latest management letter. The GMS took the report as read and advised this will be updated for next week's full meeting of Council. The GMS clarified colour coding in the report.

COMMITTEE RESOLUTION RA 23/10/007

Moved: Cr Robert Mallinson
Seconded: Cr Jack O'Connor

That the Risk and Assurance Sub-Committee Meeting receive the report.

Carried Unanimously

4 IN COMMITTEE ITEMS

COMMITTEE RESOLUTION RA 23/10/008

Moved: Cr Robert Mallinson
Seconded: Mayor Tania Gibson

That the Risk and Assurance Sub-Committee Meeting the Risk and Assurance Sub-Committee Meeting resolves to exclude the public on the grounds contained in Section 48(1) of the Local Government Official Information and Meetings Act:

General subject of each matter to be considered	Reason for passing this resolution in relation to each matter	Ground(s) under section 48 for the passing of this resolution
4.1 - CONFIRMATION OF IN COMMITTEE MINUTES OF RISK AND ASSURANCE SUB-COMMITTEE MEETING HELD ON 28 AUGUST 2023	**s7(2)(a) - the withholding of the information is necessary to protect the privacy of natural persons, including that of deceased natural persons** **s7(2)(b)(ii) - the withholding of the information is necessary to**	**s48(1)(a)(i) - the public conduct of the relevant part of the proceedings of the meeting would be likely to result in the disclosure of information for which good reason for**

	protect information where the making available of the information would be likely unreasonably to prejudice the commercial position of the person who supplied or who is the subject of the information **s7(2)(d) - the withholding of the information is necessary to avoid prejudice to measures protecting the health or safety of members of the public**	**withholding would exist under section 6 or section 7**
4.2 - LONG TERM PLAN 2024-2034 RISK REGISTER	**s7(2)(f)(i) - free and frank expression of opinions by or between or to members or officers or employees of any local authority**	**s48(1)(a)(i) - the public conduct of the relevant part of the proceedings of the meeting would be likely to result in the disclosure of information for which good reason for withholding would exist under section 6 or section 7**
4.3 - EY 2023 MANAGEMENT LETTER POINTS	**s7(2)(f)(i) - free and frank expression of opinions by or between or to members or officers or employees of any local authority**	**s48(1)(a)(i) - the public conduct of the relevant part of the proceedings of the meeting would be likely to result in the disclosure of information for which good reason for withholding would exist under section 6 or section 7**
4.4 - HEALTH AND SAFETY REPORT	**s7(2)(b)(ii) - the withholding of the information is necessary to protect information where the making available of the information would be likely unreasonably to prejudice the commercial position of the person who supplied or who is the subject of the information** **s7(2)(f)(i) - free and frank expression of opinions by or between or to members or officers or employees of any local authority**	**s48(1)(a)(i) - the public conduct of the relevant part of the proceedings of the meeting would be likely to result in the disclosure of information for which good reason for withholding would exist under section 6 or section 7**
4.5 - ICT AND CYBERSECURITY IMPLEMENTATION PLAN ON AUDITS PERFORMED	**s7(2)(b)(ii) - the withholding of the information is necessary to protect information where the making available of the information would be likely unreasonably to prejudice the commercial position of the**	**s48(1)(a)(i) - the public conduct of the relevant part of the proceedings of the meeting would be likely to result in the disclosure of information for which good reason for withholding would exist under section 6 or section 7**

	person who supplied or who is the subject of the information **s7(2)(g) - the withholding of the information is necessary to maintain legal professional privilege** **s7(2)(h) - the withholding of the information is necessary to enable Council to carry out, without prejudice or disadvantage, commercial activities**	

Carried Unanimously

5 SUB-COMMITTEE RESUME IN OPEN MEETING

CLOSURE OR RATIFICATION OF DECISIONS IN OPEN MEETING.

The meeting concluded at 5.12 pm.

Confirmed

_____ _____/_____/_____

R Caldwell **Date**

Chairperson

3 AGENDA ITEMS

3.1 TREASURY UPDATE 31 DECEMBER 2023

File Number:

Report Author: Group Manager Support

Report Authoriser: Chief Executive

Appendices: 1. December Treasury dashboard

1. REPORT PURPOSE

1.1. The purpose of this report is to provide the Committee with an update of Council's treasury position as of 31 December 2023.

2. OFFICER RECOMMENDATION

That the Risk and Assurance Sub-Committee Meeting:

1. Receives the report and notes the contents.

3. BACKGROUND

3.1. Council manages its treasury functions in accordance the treasury policies adopted.

3.2. Bancorp Treasury Services Limited are engaged by Council to provide Treasury related services to Council and ensure Council complies with its adopted treasury policies.

3.3. Bancorp provide a quarterly update which is attached in Appendix 1.

3.4. Council is compliant with it the policy bands set out in the treasury policy.

4. NEXT STEPS

4.1. That the Risk and Assurance Sub-Committee Meeting receives the report.

Confirmation of Statutory Compliance

Compliance with Statutory Decision-making Requirements (ss 76 - 81 Local Government Act 2002).

(a) This report contains:

(i) sufficient information about all reasonably practicable options identified and assessed in terms of their advantages and disadvantages; and

(ii) adequate consideration of the views and preferences of affected and interested persons bearing in mind any proposed or previous community engagement.

(b) The information reflects the level of significance of the matters covered by the report, as determined in accordance with the Council's significance and engagement policy.

MĀWHERA GREY DISTRICT COUNCIL

Quarterly Treasury Dashboard

31 December 2023

STRICTLY PRIVATE AND CONFIDENTIAL

BANCORP

BANCORP TREASURY SERVICES LIMITED

Economic Commentary

Global (for the December 2023 quarter)

The December quarter saw what has been described as epic moves in the benchmark US 10-year Treasury bond. The markets started the quarter with expectations of one further rate increase as the Fed reiterated its commitment to fighting inflation, concerns about the ability of the market to attract sufficient buyers to purchase US bonds as a result of the ever-increasing US deficits and continuing fallout from Fitch's downgrade of the US credit rating in early August. These factors saw the 10-year yield hit 17-year highs, peaking at 5.02% on the 20th of October, however since then the fall in US bond yields has been startling, with the market moving from 'higher-for-longer' outlook, to one of 'we have seen the top and then to pricing in six rate cuts at one point', the US 10-year bond closed the year at 3.76%, which represented a remarkable 1.26% fall in 72 days.

The Fed released a dovish statement on the 13th of December, where it appeared to pivot from the prospect of raising rates in earlier statements to talk of three rate cuts in 2024, the market then seized on this statement and as indicated above moved to price into six rate cuts at one point. However, many commentators make a good argument that economic data has not yet validated these significant market moves, and it is premature given that the battle against inflation is far from won and that the concerns around government bond issuance and the possibility of further US credit rating downgrades continue.

Despite the above, from a global perspective, the US still stands out as one of the few bright lights as we enter 2024. China continues to struggle to recover from the lifting of its Covid-19 restrictions, with China consumer prices declining for a third month in December, highlighting persistent deflationary pressures. These factors remain a concern for global growth given China's standing as the world's second-largest economy.

European inflation has fallen significantly from the 10.6% highs seen in late 2022, November inflation had fallen to 2.4% (on an annual basis) but increased back to 2.9% in December after seven straight monthly declines as food prices rose and support for high energy bills ended in some countries. The rise in price levels fueled debate over how soon interest rate cuts could be expected from the European Central Bank.

Across the Tasman, the Reserve Bank of Australia continued to increase its cash rate to 4.35% in November. However, at its December meeting, it kept rates unchanged, stating that any further moves would be data-dependent, however, its tone was seen as relatively hawkish. There is a widely held perception that it sits six to twelve months behind the rest of the world in its inflation settings. Like New Zealand though it has high levels of immigration which has increased aggregate demand which may see inflation higher than it would be otherwise.

Geopolitical issues also weigh on the global economy with the Ukraine and Russian war dragging on and with the tragic events in Palestine spilling over into tensions in the Red Sea. The impact on the global economy is strained supply lines and higher shipping costs.

BANCORP

GREY DISTRICT COUNCIL

Economic Commentary

New Zealand (for the December 2023 quarter)

	OCR	90 day	2 years	3 years	5 years	7 years	10 years
30 Sep 2023	5.50%	5.74%	5.72%	5.48%	5.22%	5.17%	5.18%
31 Dec 2023	5.50%	5.63%	4.64%	4.32%	4.09%	4.07%	4.14%
Change	+0%	-0.11%	-1.08.%	-1.16%	-1.23%	1.10%	-1.04%

December was a significant quarter, with the shape of the new government being known, a continuing hawkish Reserve Bank of New Zealand ("RBNZ"), a market which is challenging the RBNZ's stance by pricing in multiple rate cuts, poor economic data and a divergence in views amongst economists.

The new coalition government's first piece of legislation was to change the RBNZ's mandate back to a single mandate, requiring the RBNZ's Monetary Policy Committee to target inflation, not price stability and "maximum sustainable employment". The change is not expected to materially impact the RBNZ's monetary policy settings.

On 29th November, the RBNZ's *Monetary Policy Statement* stated that *"The Committee is confident that the current level of the OCR is restricting demand. However, ongoing excess demand and inflationary pressures are of concern, given the elevated level of core inflation. If inflationary pressures were to be stronger than anticipated, the OCR would likely need to increase (rates) further"*.

However, this statement was effectively ignored by the market, as it instead focussed on the sharp fall in US Treasury bonds and then the higher-than-expected local unemployment data (September quarter unemployment up from 3.60% to 3.90%). This was followed by the release in December of the shocking third quarter GDP data which saw GDP contract by 0.3% versus expectations of a 0.3% increase. Even worse Q2 GDP was revised downwards from 0.9% to 0.5%, occurring in a backdrop of soaring migration (at levels not seen since 1947) and the downward revision to the Q1 data once again put the country into recession for the six months ending 31st March 2023. The market then moved to a stance where it was pricing in 4-5 rate cuts in 2024.

In looking at the bank's economists' views, we have a clear divergence in views, with some banks picking multiple rate cuts in 2024, with others such as Westpac and ANZ being much more cautious on the inflation outlook, particularly the sticky nature of non-tradeable inflation. By the end of December, the markets were pricing in the first OCR cut in May 2024 and for it to fall to 4.0% by May 2025.

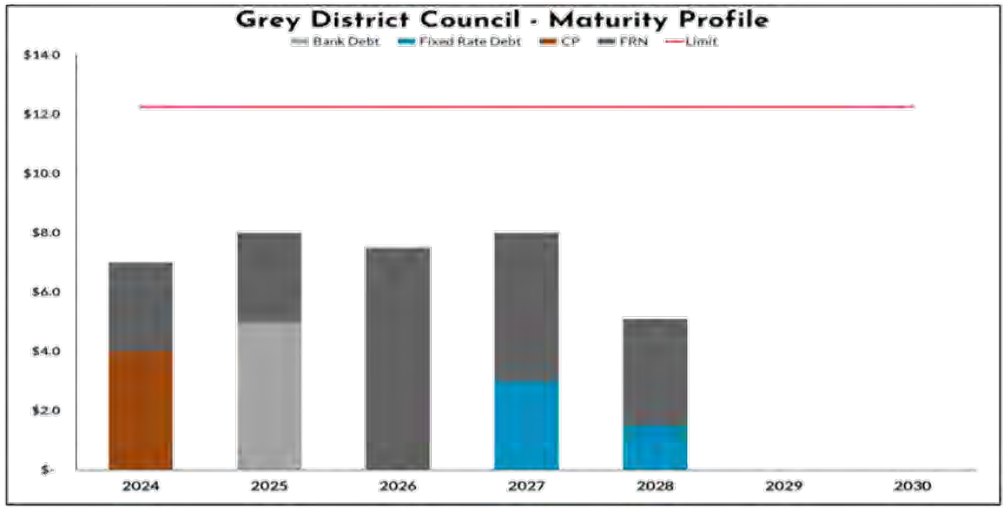
Swap rates saw significant levels of volatility, with the reference 5-year swap rate peaking at 5.40% in early October and falling to a low of 4.06% in late December (in very thing trading). The downward momentum was initiated by falling US Treasury bond yields, a change to the Fed's dot plots (which inferred 3 rate cuts in 2024 and then by the shocking NZ Q3 GDP data).

The new government's policy agenda will be of interest with tax cuts potentially providing support to the economy which may see inflation remain higher for longer.

BANCORP

GREY DISTRICT COUNCIL

Liquidity and Funding



Policy Compliance	Compliant
Have all transactions been transacted in compliance with policy?	Yes
Is fixed interest rate cover within policy control limits?	Yes
Is the funding maturity profile within policy control limits?	Yes
Is liquidity within policy control limits?	Yes
Are Term Deposit counterparty exposures within policy control limits?	Yes

Debt
$30.6m
External Council Drawn Debt

LGFA
$30.6m
Funds Drawn from LGFA

Liquidity = undrawn bank facility + term deposits + cash in bank
$12.26m

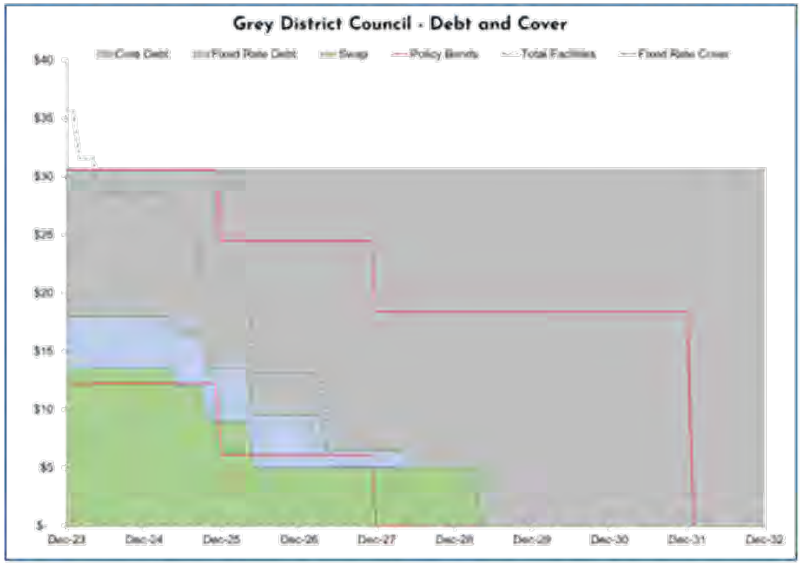
Liquidity Ratio
140.07%
Definition: (Cash Reserves + Lines of Credit + Drawn Debt)/Drawn Debt

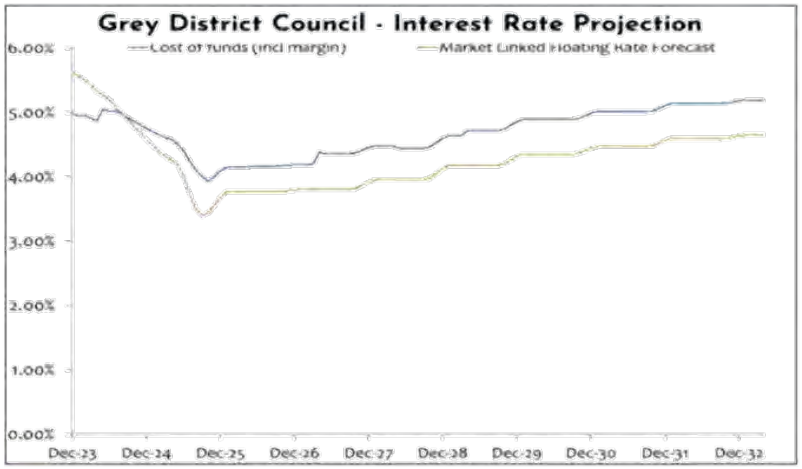
Cost of Funds as at 31 December
4.98%

BANCORP

GREY DISTRICT COUNCIL

Interest Rate Risk Management





Current % of Debt Fixed	58.8%
Current % of Debt Floating	41.2%
Value of Fixed Rate (m)	$18.0
Weighted Average Cost of Fixed Rate Instruments	3.26%
Weighted Average Cost of Fixed Rate Instruments (incl margin)	3.73%
Value of Forward Starting Cover	$5.0
Weighted Average Cost of Forward Starting Cover	3.57%
Value of Floating Rate (m)	$12.6
Current Floating Rate	5.63%
Current Floating Rate (incl margin)	6.26%
All Up Weighted Average Cost of Funds Including Margin	4.98%
Total Facilities In Place	$35.6

Policy Bands

	Minimum	*Maximum*	*Policy*
0 - 2 years	40%	100%	Compliant
2 - 4 years	20%	80%	Compliant
4 - 8 years	0%	60%	Compliant

BANCORP

Grey DC - Funding

As of 31st December 2023, Grey DC had $30.6 million of core debt, all of which is sourced from the LGFA using Commercial Paper ("CP"), Floating Rate Notes ("FRN's") and Fixed Rate Bonds ("FRB's"). Details of the debt as of 31 December are as follows.

Instrument	Maturity	Yield	Margin	Amount
LGFA CP	16-Feb-24	5.93%	N/A	$4,000,000
LGFA FRN	15-May-24	6.15%	0.51%	$3,000,000
LGFA FRN	15-May-25	6.21%	0.57%	$3,000,000
LGFA FRN	15-May-26	6.26%	0.62%	$4,000,000
LGFA FRN	15-May-26	6.30%	0.66%	$3,500,000
LGFA FRB	15-Apr-27	1.95%	N/A	$3,000,000
LGFA FRN	15-May-27	6.35%	0.71%	$5,000,000
LGFA FRN	15-May-28	6.32%	0.68%	$3,600,000
LGFA FRB	15-May-28	5.11%	N/A	$1,500,000

BANCORP

GREY DISTRICT COUNCIL

LGFA Borrowing Rates

Listed below are the credit spreads and applicable interest rates as at the end of December for Commercial Paper ("CP"), Floating Rate Notes ("FRN") and Fixed Rate Bonds ("FRB"), at which Grey District Council could source debt from the Local Government Funding Agency ("LGFA").

Maturity	Margin	FRN (or CP Rate)	FRB
3-month CP	0.20%	5.83%	N/A
6-month CP	0.20%	5.91%	N/A
April 2024	0.49%	6.12%	6.18%
April 2025	0.55%	6.18%	5.98%
April 2026	0.61%	6.24%	5.68%
April 2027	0.71%	6.34%	5.58%
May 2028	0.86%	6.49%	5.59%
April 2029	0.93%	6.56%	5.57%
May 2030	0.97%	6.60%	5.59%
May 2031	1.09%	6.72%	5.71%
April 2033	1.13%	6.76%	5.81%
May 2035	1.22%	6.85%	5.95%
April 2037	1.24%	6.87%	6.06%

BANCORP

GREY DISTRICT COUNCIL

Disclaimer

IMPORTANT NOTICE

Statements and opinions contained in this report are given in good faith, but in its presentation, Bancorp has relied on primary sources for the information's accuracy and completeness. Bancorp does not imply, and it should not be construed, that it warrants the validity of the information. Moreover, our investigations have not been designed to verify the accuracy or reliability of any information supplied to us.
It should be clearly understood that any financial projections given are illustrative only. The projections should not be taken as a promise or guarantee on the part of Bancorp.
Bancorp accepts no liability for any actions taken or not taken on the basis of this information and it is not intended to provide the sole basis of any financial and/or business evaluation. Recipients of the information are required to rely on their own knowledge, investigations and judgements in any assessment of this information. Neither the whole nor any part of this information, nor any reference thereto, may be included in, with or attached to any document, circular, resolution, letter or statement without the prior written consent of Bancorp as to the form and content in which it appears.

CONFIDENTIALITY

The information provided herein is provided for your private use and on the condition that the contents remain confidential and will not be disclosed to any third party without the consent in writing of Bancorp first being obtained.

GET IN TOUCH

Bancorp Treasury New Zealand Ltd
Head Office, Level 3, 30 Customs Street, Auckland
09 912 7600

www.bancorp.co.nz

3.2 ICT STRATEGY 2023-2028

File Number:

Report Author: Group Manager Support

Report Authoriser: Chief Executive

Appendices: 1. ICT Strategy 2023-2028

1. REPORT PURPOSE

1.1. For Council to adopt the Grey District ICT Strategy 2023-2028.

2. EXECUTIVE SUMMARY

2.1. During 2022 and 2023 Council completed both an ICT and Cybersecurity audit. An action plan has been produced from the recommendations and implementation has commenced to address the outstanding matters.

2.2. A significant part of that process is the design, implementation, and adoption of an ICT Strategy (the Strategy) for Council.

2.3. This ICT strategy has been finalised, and the next step is for this committee to review, and to recommend to Council to adopt this ICT Strategy.

3. OFFICER RECOMMENDATION

That the Risk and Assurance Sub-Committee:

1. Receives the 2023-2028 ICT Strategy report and accompanying Appendix.
2. Recommend to Council that Council adopts the ICT Strategy 2023-2028.

4. BACKGROUND

4.1. An ICT strategy has been drafter for implementation and adoption by Council to set the strategic direction of Council regarding Information and Communication Technology and its use and protection against cybersecurity.

4.2. The ICT Strategy has been recommended by the Executive Leadership Team at the meeting held on 18 November 2023.

4.3. The next step is for Council to adopt the strategy and use this when making strategic decisions over the next five years relating to ICT and cybersecurity.

5. OPTIONS

5.1. That Council adopts the ICT Strategy 2023-2028.

Or

That Council declines the adoption of the ICT Strategy 2023-2028.

6. CONSIDERATIONS

6.1. Legal and Legislative Implications

6.1.1. N/A

6.2. Financial

6.2.1. The committee recognises that there will be future funding required by Council and while this is out of scope for this committee it recommends that Council adopts the Strategy.

6.3. Existing Policy and Strategy Implications

6.3.1. N/A

6.4. Fit with Purpose of Local Government Statement

6.4.1. N/A

6.5. Effects on Manawhenua

6.5.1. N/A

6.6. Significance and Engagement

Issue	Level of Significance	Explanation of Assessment
Is there a high level of public interest, or is decision likely to be controversial?	N/A	N/A
Is there a significant impact arising from duration of the effects from the decision?	N/A	N/A
Does the decision relate to a strategic asset? (refer Significance and Engagement Policy for list of strategic assets)	N/A	N/A
Does the decision create a substantial change in the level of service provided by Council?	N/A	N/A
Does the proposal, activity or decision substantially affect debt, rates or Council finances in any one year or more of the LTP?	N/A	N/A
Does the decision involve the sale of a substantial proportion or controlling interest in a CCO or CCTO?	N/A	N/A
Does the proposal or decision involve entry into a private sector partnership or contract to carry out the deliver on any Council group of activities?	N/A	N/A
Does the proposal or decision involve Council exiting from or entering into a group of activities?	N/A	N/A

6.7. Community Wellbeings and Outcomes

6.7.1. N/A

6.8. Other

6.8.1. N/A

7. NEXT STEPS

7.1. The Strategy along with the committee's recommendation is reported to Council for their consideration and adoption.

Confirmation of Statutory Compliance

Compliance with Statutory Decision-making Requirements (ss 76 - 81 Local Government Act 2002).

(a) This report contains:

(i) sufficient information about all reasonably practicable options identified and assessed in terms of their advantages and disadvantages; and

(ii) adequate consideration of the views and preferences of affected and interested persons bearing in mind any proposed or previous community engagement.

(b) The information reflects the level of significance of the matters covered by the report, as determined in accordance with the Council's significance and engagement policy.

Grey District Council

INFORMATION TECHNOLOGY STRATEGIC PLAN

FY 2023 - 2028

Document Control

Review cycle

This document should be reviewed when there have been further changes to the solution architecture, and the updated changes referenced in this document.

Version control

Version	Date	Description of Changes	Author
1.0	11/10/2023	Initial draft	Russel Maliwat

Document reviewers

Name	Role	Date	Signature
Gerhard Roux	Group Manager – Support	12/10/2023	Recommended to ELT

Document Acceptance/Approval

This document has been approved and accepted by:

Name	Role	Date	Signature
Paul Morris	CEO	07/11/2023	Approved at ELT meeting

Document contributors

This document has been contributed to by the following resources:

Name	Role	On behalf of
Russel Maliwat	ICT Manager	Grey District Council
Stephen Wilcox	Consultant	Focus Technology Group (FTG)
Dave Loschiavo	Consultant	SSS – IT Security Specialists (SSS)

Table of Contents

1. Executive Summary

In today's rapidly evolving business landscape, the success of any company heavily relies on the alignment of its IT initiatives with its overall business goals. Building a business-aligned IT strategy is crucial for ensuring IT excellence and driving technology innovation. This is particularly true for Grey District Council (GDC), as the company aims to leverage technology to gain a competitive edge and achieve its business objectives. By developing a comprehensive IT strategy that is closely integrated with the company's overall vision and objectives, GDC can maximize the value of its IT investments, enhance operational efficiency, and effectively respond to the ever-changing market demands.

Grey District Council (GDC) is undergoing significant change and development, prompting the need to establish Strategic and Business Plans to achieve short-, medium-, and long-term objectives. In this digital age, Information Technology (IT) plays a crucial role in how GDC operates and delivers services, enabling more efficient and effective interactions with the community and stakeholders. This IT Strategic Plan outlines the necessary steps to enhance service delivery, empower staff, and leverage emerging technologies. By focusing on key priorities, collaborating with partners, and strengthening the technical infrastructure, GDC aims to drive efficiency, transformation, and digital innovation from 2023 to 2028.

IT is a fundamental component of the business, driving significant changes and advancements. However, its role is primarily that of an enabler rather than an end in itself. To support the business strategies effectively, various levels of technology are required, including the foundational IT infrastructure (such as computers, servers, networks, and hardware), the utilization of corporate and line-of-business software solutions, and the implementation of robust information governance management and security measures.

The IT Strategic Plan sets a clear path for the future development and delivery of IT services for Grey District Council. It outlines the actions required to enhance service delivery, improve customer experience, ensure regulatory compliance, and leverage new and emerging technologies effectively.

1.1 Alignment with the Corporate Business Plan

This IT strategy has been developed to ensure alignment with the GDC's Strategic Business Plan objectives.

The IT strategy is also aligned to the current Grey District Council 2021 - 2031Long-Term Plan (LTP)[1].

1.2 The Challenges

Grey District Council (GDC) is a small district council catering to a population of less than 10,000 residents. In order to achieve its corporate vision and meet the evolving needs and expectations of residents, Information Technology (IT) will play a crucial role.

As the demand for public services continues to grow, citizens and businesses expect the same level of access and personalization that they experience with large private sector organizations online. They anticipate the ability to access services from various locations and devices, at their convenience.

To meet these expectations and drive efficiency in service delivery, GDC must prioritize providing choice in how people access their services. This will ensure maximum flexibility for citizens while streamlining operations.

Furthermore, the risk of cybercrime is on the rise, with organizations holding personal data being the primary targets. Common cyber-attacks include fraudulent emails, viruses, and malware. It is imperative for GDC to implement robust cybersecurity measures to protect against such threats.

[1] A revised Long-Term Plan for 2024 to 2034 is currently being developed.

1.2.1 IT Infrastructure Sustainability and Modernization

As the volume of information and data continues to expand, it becomes increasingly important to effectively manage, access, and share these assets. Upgrading the aging and critical IT infrastructure is essential for ensuring long-term access to valuable business information and maintaining high-quality services for both the Council and our customers. By implementing modern IT solutions, we can address these challenges and ensure the continued availability of reliable and efficient services.

1.2.2 Meeting Citizens' Expectations

Citizens have high expectations for their council, desiring access to programs and services that prioritize their needs and provide a seamless and user-friendly experience. This means that:

- Services should be easily accessible and user-centric, with a focus on simplicity and convenience.
- Data should be shared and reused when appropriate, ensuring consistency in interactions with the government.

To meet these expectations, services should be digitally enabled and seamlessly integrated.

1.2.3 Workplace and Workforce Evolution

Council employees have a growing expectation for modern and efficient tools that are interconnected, user-friendly, and accessible at all times and locations. They also require updated business processes that streamline their day-to-day work and enhance their contributions. In a contemporary work environment, employees need digital tools that foster collaboration, facilitate information sharing, and boost productivity. Moreover, these tools should be inclusive and accessible to individuals with disabilities.

1.2.4 Privacy and Security

Cybersecurity is a dynamic component of every IT strategy and plan. While system consolidation offers valuable opportunities, it also expands the potential "attack surface," necessitating stronger security measures to mitigate risks. Inadequate management of council networks and inconsistent security profiles of council end-point devices further heighten the vulnerability to cyberattacks.

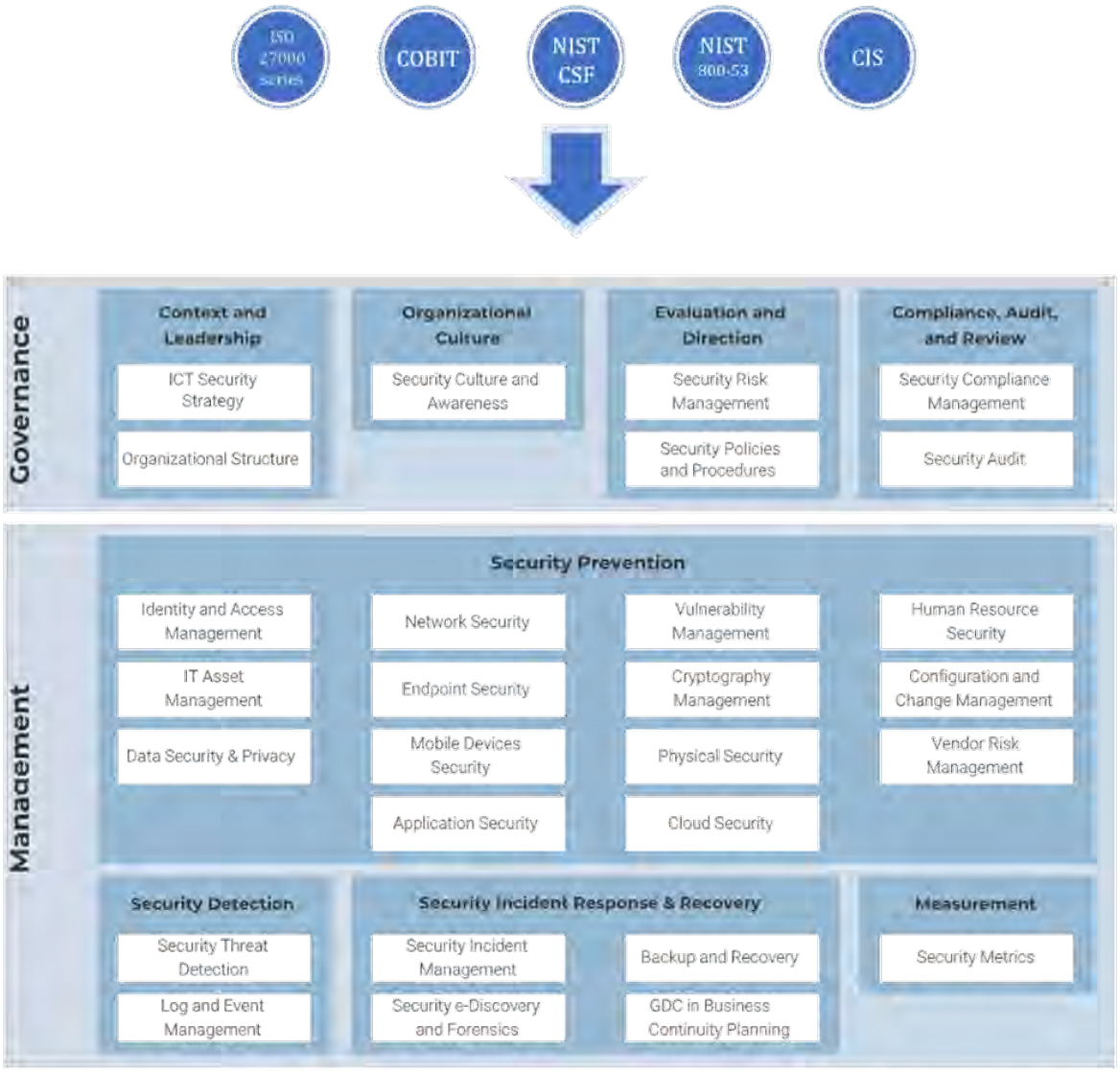
1.3 GDC Security Strategy Model

An Information Security Strategy model that is:

- **Business-Aligned.** Determines business context and cascades enterprise goals into security alignment goals.
- **Risk-Aware.** Understands the security risks of the business and how they intersect with the overall organizational risk tolerance.
- **Holistic.** Leverages a best-of-breed information security framework to provide comprehensive awareness of GDC's security capabilities.

1.4 Cyber Security Framework

In today's interconnected and threat-filled digital world, having a robust cybersecurity framework is essential for protecting digital assets, adhering to regulations, and mitigating risks. It provides the necessary structure to safeguard GDC's operations and maintain its reputation.



GDC has chosen to adopt ISO 27000, NIST, COBIT, and CIS as part of their cybersecurity framework. This decision reflects their commitment to implementing internationally recognized standards and best practices. By incorporating these frameworks, GDC aims to enhance their information security risk management, establish effective governance, and proactively address cyber threats.

2. The Information Technology Vision

2.1 Vision Statement

We are a service-oriented organisation that delivers leading information systems to support Grey District Council's Business Strategy, enhance resilience and support customer experience.

2.2 Vision, Goals, Initiatives, Actions, and Guiding Principles

Strategic Themes are fundamental focus areas that guide the council's strategic direction, shaping specific goals and initiatives in alignment with its mission or vision.

Goals identify the Council's main areas of focus for information technology, and they indicate the results that needs to be achieved.

Initiatives are larger, coordinated efforts or projects that encompass multiple actions.

Actions break down the initiatives into their more specific parts and activities.

Guiding Principles guide decision-making in the continual development of information technology.

2.3 The Strategic IT Vision

An IT Strategic vision has been established for GDC's Information Technology (IT), to provide **innovative**, **reliable**, **effective** (cost & use), and **secure** services both internally to the organisation and externally to the community and stakeholders.

INNOVATIVE	• How GDC can use new technologies to help the community. • How to make the organisation a more effective, enjoyable place to work.
RELIABLE	• Stable business systems and network communications. • Appropriate redundancy to sustain critical functionality.
EFFECTIVE	• Simplified IT experience for all users. • IT experiences the community wants and values. • IT tools and experiences that help GDC staff deliver for the community. • IT that is easily used and understood.
SECURE	• Safe from cyberattacks. • Keeping personal information/data secure.

This Strategic Plan will enable GDC to benefit from IT innovations, increasing capabilities, and delivering efficiencies in support of administrative functions, establishing a framework to:

- drive improved project and service delivery,
- focus on maximizing the value from IT,
- increasing benefits through improving information quality and accessibility, which will enable better decision-making.

The pace of change in IT is accelerating and customer expectations are evolving rapidly, demanding advanced and seamless experiences. It is important to invest in state-of-the-art capabilities like data analytics, cybersecurity, automation, and third-party system integration.

While GDC can't predict technology beyond 2026, they can anticipate transformative changes in the services provided through innovative technology.

The following figure outlines the framework for this Strategic Plan.

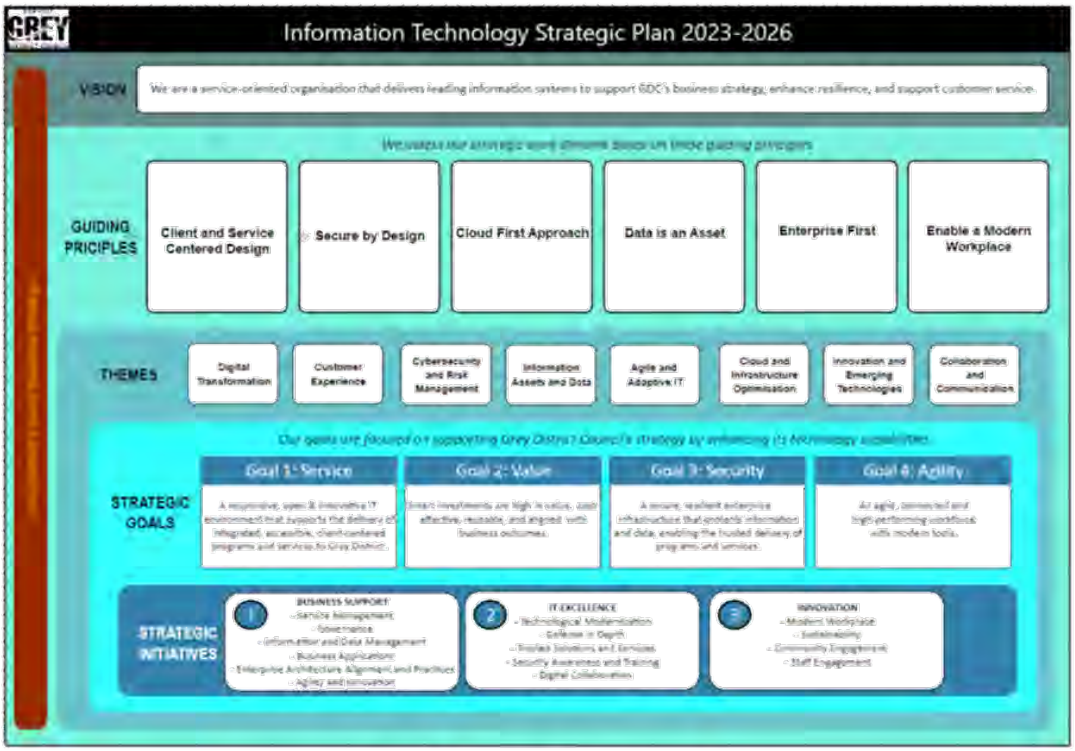


Figure 1. IT Strategic Plan Framework.

Refer to Appendix A for a larger version of figure 1.

2.4 Key Drivers

- **Service Excellence** – Service excellence depends on a customer-centric culture, engaged employees, clear standards, and continuous improvement. These drivers will help GDC to consistently meet customer expectations and build trust and loyalty.
- **Effective Financial and Asset Management** – Effective financial and asset management means smart resource allocation, strategic planning, and efficient asset utilisation, resulting in improved profitability and long-term sustainability.
- **Regulatory Compliance** - Following laws and rules to avoid legal issues and maintain trust and ethics in operations.
- **Motivated, Satisfied Employees and Work Safety** – Motivated, satisfied employees and work safety are essential for a positive workplace culture and productivity.
- **Financial Management and Security** – Financial management and security ensure the responsible handling of money and assets to protect against risks and achieve long-term stability.
- **Technology Modernisation, Security, and Resiliency** – The IT infrastructure, and applications need to be kept current to keep pace with business and technology requirements. The Council faces increasing threats to its systems and data, and continuous modernisation is required to ensure Council systems and data are properly protected.
- **Data Governance** – The process of managing the availability, classification, usability, integrity, and security of the data in enterprise systems ensures that data is consistent, adheres to policy, is trustworthy and doesn't get misused.
- **Usability** – As technology capabilities evolve, applications and services can be enhanced to improve the user experience and complete tasks and services more efficiently.

2.5 GDC Key Customers

Customers are any people who utilise IT Services from Grey District Council, including:

- Citizens
- Ratepayers
- Business
- Elected members
- Internal staff
- Business partners

2.6 Key Legislation and Council Strategies

- Health and Safety in Employment Act 1992
- Employment Relations Act 2000
- Local Government Official Information and Meetings Act 1987
- Public Records Act 2005
- Privacy Act 2020
- Government ICT Strategy and Action Plan (www.digital.govt.nz)

2.7 Guiding Principles

The following guiding principles will guide us in these endeavours.

GP1	**Enable a Modern Workplace** GDC strives to be an innovative organisation that: • provides its employees with modern technology for easy access to information and data, promoting collaboration anytime, anywhere. • provides customisable tools and resources for users. • provides automated, digital processes in support of better services.
GP2	**Cloud First Approach** Where practical, possible, and financially viable, cloud solutions will be used, allowing us to take advantage of greater scalability and resilience options.
GP3	**Client and Service Centred Design** Focus on designing services and systems with a deep understanding of the end-users' requirements, ensuring that the services are not only functional but user-friendly and tailored to meet specific needs: • **User-Centric Approach** - Placing the client or end-user at the center of the design process to understand their goals, preferences, and pain points. • **Accessibility** - Ensuring that services are accessible to a diverse range of users. • **Efficiency** - Improving processes and workflows for greater efficiency. • **Service Integration** - Considering the entire service ecosystem and how different services and systems interact to provide a seamless experience.
GP4	**Data is an Asset** • Data has value to the organisation, and GDC will leverage their data assets to provide improved transparency, analysis, insights, and decision-making. • Eliminate duplication and inefficiency by organising, standardising, and cleaning GDC data. This ensures accurate, clear presentation and seamless system integration.
GP5	**Secure by Design** GDC information is safeguarded for security, privacy, and confidentiality, is monitored to prevent leaks, and is protected for future generations.
GP6	**Enterprise First** The organisation will follow common standards, approaches, and direction, and use existing enterprise assets, such as processes, data, contracts, and solutions, as accelerators where: • information is created once, reused numerous times, and managed GDC-wide as a single-aligned asset that is consistent, standardised, and interoperable. • solutions support the use of open standards, are scalable and can be rapidly deployed. • cost-effective and efficient business solutions facilitate information and data integration, reuse, management, sharing and analytics. • adopt shared solutions at the enterprise level before considering department-specific or legacy systems. This strategy ensures that common business needs are addressed efficiently and consistently across the entire organisation, promoting synergy and cost-effectiveness.

3. Information Technology Strategic Themes

A corporate Information Technology (IT) function must be driven by the needs of the organisation and from the customer's perspective. Yet at the same time an IT function must be a driver to help the organisation exploit new technological advances. This strategy focuses on ensuring that the technology within GDC is aligned with the strategic direction of the Council and its Services.

To support the organisation effectively, the IT strategy is structured around key Information Technology Strategic Themes. These IT strategic themes are concentrated areas of strategic planning within GDC's overall Information Technology strategy. Each theme signifies a specific aspect or priority that shapes GDC's use of technology to attain its objectives. These themes play a crucial role in aligning IT projects with broader business goals, offering a structure for decision-making, and aiding in the allocation of resources within the IT department.

To be able to support the organisation, the IT strategy has been split into eight main themes. Each of these themes has an evolving roadmap of activity supporting it. The themes will not only address organisational pressures but also be driven and updated by wider technology industry demands and trends.

1. **DIGITAL TRANSFORMATION** - Using technology to fundamentally change the way GDC operates, interacts with customers, and delivers value.
2. **CUSTOMER EXPERIENCE** - Leveraging IT to improve customer interactions and satisfaction.
3. **CYBERSECURITY & RISK MANAGEMENT** - Safeguarding GDC's digital assets and sensitive information.
4. **INFORMATION ASSETS & DATA** - Ensuring data quality and utilising data to gain valuable insights that can inform strategic decisions.
5. **AGILE & ADAPTIVE IT** - Emphasizes flexibility and responsiveness in IT operations.
6. **INFRASTRUCTURE RESILIENCE & OPTIMISATION** - Infrastructure is resilient, cost effective, well supported, and recoverable within clearly defined requirements. Optimising GDC's IT infrastructure, with a 'Cloud first' adoption strategy.
7. **ENABLE EMPLOYEES ANYWHERE** - Employees can access, capture, and update the information they need to effectively do their job and support others, wherever they may be working.
8. **COLLABORATION & COMMUNICATION** - Improving internal and external communication and collaboration through IT tools and platforms.

3.1 THEME 1: Digital Transformation

Background	The IT strategic theme for Digital Transformation can be defined as a comprehensive and overarching approach that guides an organisation's Information Technology (IT) initiatives and investments in alignment with its broader digital transformation goals. It involves the strategic use of technology to enable and support the transformation of various aspects of the organisation, including its processes, operations, customer experiences, and overall business model.
Objective	Create a future where technology is not merely a tool but the driving force behind the organisation's evolution. To enable a digitally transformed organisation that seamlessly integrates cutting-edge technology into every facet of its operations.
Principles	Key elements and characteristics of the Digital Transformation theme include: 1. **Alignment with Business Objectives -** It is closely tied to GDC's overall business strategy and objectives, ensuring that technology initiatives are directly contributing to achieving the desired transformation outcomes. 2. **Long-term Vision -** It encompasses a long-term vision for how technology will be leveraged to create a more agile, innovative, and competitive organisation. 3. **Holistic Approach -** Consider all facets of IT, including infrastructure, applications, data, security, & talent, to ensure that the entire IT ecosystem supports the transformation efforts. 4. **Customer-Centric Focus -** Improvement of customer experiences and engagement through digital channels, recognising the importance of meeting customer needs and expectations. 5. **Data-Driven Decision-Making -** It emphasizes the collection, analysis, and utilisation of data to inform strategic decisions and drive continuous improvement. 6. **Agility and Innovation -** It encourages experimentation and the adoption of emerging technologies to stay ahead in a rapidly changing digital landscape. 7. **Change Management -** It includes plans and strategies for managing organisational change, as digital transformation often requires shifts in culture, processes, and employee skillsets. 8. **Cybersecurity and Risk Management -** It addresses the cybersecurity and risk considerations associated with digital transformation to protect the organisation from potential threats and vulnerabilities. 9. **Measurement and Evaluation -** It defines key performance indicators (KPIs) and metrics to assess the progress and success of digital transformation initiatives.

3.2 THEME 2: Customer Experience

Background	Local Government must change customers perceptions of what can be provided and how this will be provided. Many people are already benefitting from the internet, digital TV, and mobile communications. These offer opportunities to access services, save money, keep in touch, pursue personal interests, and help with learning. This theme covers the technology and services that will provide new access channels and true self-service to the Greymouth citizens from any place and on any device.
Objective	Provide a customer-centric digital self-service experience accessible from any platform. A preferred Customer Portal will enable online payments and real-time tracking, reducing the need for direct contact. Alignment across IT, Customer Services, and Digital Transformation is crucial for success.
Principles	The main principles for this theme are: 1. **Customer Understanding -** Understanding customers' needs both internal and external and design services around them and for them. 2. **Seamless Multichannel Experiences -** Offer accessible end-to-end digital services, providing a consistent, personalised experience across all customer touchpoints, including in-person, online, mobile, and social media, enhancing engagement and customer satisfaction. 3. **Effortless Interactions -** Optimise processes to minimise customer effort, ensuring ease and convenience in interactions, inquiries, purchases, and support. Self-service options are encouraged whenever feasible. 4. **Empowered Customer Service -** GDC customer service teams are empowered with the tools, knowledge, and autonomy to resolve customer issues effectively and exceed expectations. 5. **Measurable Impact -** Measure GDC success through key performance indicators (KPIs) such as Net Promoter Score (NPS)[2], Customer Satisfaction (CSAT)[3], and Customer Effort Score (CES)[4] to gauge progress and make continuous improvements.

[2] NPS is a metric that assesses customer loyalty and gauges the likelihood of customers recommending a company's products or services to others.

[3] CSAT measures overall customer satisfaction with a product, service, or interaction. It provides insights into the customer's perception of the quality and effectiveness of what they received.

[4] CES measures the ease with which customers can complete a specific task or interaction with a company, such as resolving an issue, making a purchase, or accessing information.

3.3 THEME 3: Cybersecurity and Risk Management

Background	Cybersecurity and Risk Management is a strategic domain that focuses on safeguarding an organisation's digital assets and sensitive information from cyber threats, vulnerabilities, and breaches. It involves the identification, assessment, and mitigation of risks related to information security, as well as the implementation of measures and protocols to protect against cyberattacks. This theme encompasses the strategic planning and ongoing management of cybersecurity practices to ensure the organisation's resilience to evolving cyber threats.
Objective	Establish a robust and adaptive cybersecurity framework that safeguards GDC digital assets and sensitive information, enabling the organisation to thrive in a secure digital landscape.
Principles	The main principles for this theme are: 1. **Proactive Threat Mitigation** - Proactively identify and assess cyber risks, vulnerabilities, and emerging threats, with risk management practices that enable us to mitigate these threats. 2. **Data Protection** - Sensitive data is protected through encryption, access controls, and stringent data security protocols, prioritising data privacy & compliance with relevant regulations. 3. **Continuous Monitoring** - Maintain continuous vigilance through real-time monitoring and threat detection systems. Any anomalies or suspicious activities are swiftly addressed. 4. **Employee Awareness** - GDC cultivate a cybersecurity-aware workforce through training and awareness programs. GDC employees are the first line of defense against cyber threats. 5. **Incident Response** - GDC have a well-defined incident response plan in place, with the capability respond swiftly to a cybersecurity incident, minimising downtime, and exposure. 6. **Business Continuity** - GDC ensure that critical systems and data are protected to minimise disruption during any events or cyber incidents. 7. **Risk-Informed Decision-Making** - GDC integrate cybersecurity risk into decision-making processes, ensuring that security considerations are part of every strategic initiative. 8. **Compliance Assurance** - GDC maintain strict adherence to cybersecurity regulations and standards, demonstrating commitment to data protection and security best practices. 9. **Resilience and Adaptability** – GDC's cybersecurity framework is designed to evolve with the ever-changing threat landscape, ensuring resilience against new and emerging cyber risks.

3.4 **THEME 4:** Information Assets and Data

Background	GDC data is a powerful and influential organisational asset. GDC must manage data and information securely, efficiently, economically, and effectively whilst at the same time maintaining privacy and protecting customer data. This will help enable delivery of the necessary efficiencies, improve performance, improve customer service, and allow us to be more open. This theme covers what GDC need to do to pass data and information seamlessly between corporate systems, share data externally and how to manage data centrally.
Objective	Provide accurate and consolidated records for Council information. This will enable services to manage and control their own information in an accurate and efficient way. Where required and relevant, data will be shared across the organisation and externally to help design and underpin better public services. GDC will store information in a secure and robust location that will enable services to make best use of management information. This will drive day to day service planning activities.
Principles	The main principles for this theme are: 1. **Data-Centric Decision-Making** - Data drives decision-making processes. GDC utilise data analytics and insights to make informed, data-driven decisions at all levels of the organisation. 2. **Data Quality and Integrity** - Prioritise data quality, accuracy, and integrity to ensure that information assets are reliable, trustworthy, and fit for purpose. GDC implement data governance practices to maintain data consistency and quality. 3. **Data Privacy and Security** - GDC rigorously protect sensitive and personal data, complying with privacy regulations and implementing robust cybersecurity measures to safeguard information assets. 4. **Data Accessibility** - GDC make data securely and easily accessible to those who need it, promoting collaboration and informed decision-making. 5. **Data Lifecycle Management** - GDC manage data throughout its lifecycle, from creation and storage to archiving and disposal, optimising its usage and minimising data redundancy. 6. **Innovation through Data** - GDC leverage data analytics and machine learning to uncover insights, discover new opportunities, and drive innovation across all aspects of the business. 7. **Compliance and Risk Mitigation** - GDC ensure that data practices align with legal and regulatory requirements, reducing the risk of non-compliance and associated penalties.

3.5 **THEME 5**: Agile and Adaptive IT

Background	Agile and Adaptive IT is a strategic approach that emphasises flexibility, responsiveness, and continuous improvement in an organisation's Information Technology systems and practices. It involves the use of Agile methodologies and principles to adapt quickly to changing business needs, customer expectations, and technological advancements. This approach promotes collaboration, iterative development, and a customer-centric mindset, enabling IT to deliver value more rapidly and efficiently.
Objective	Create an Information Technology ecosystem that seamlessly aligns with the organisation's dynamic needs and rapidly changing digital landscape; it's about creating a dynamic IT environment that drives innovation, customer satisfaction, and business growth in an ever-evolving digital landscape.
Principles	The main principles for this theme are: 1. **Strategic Value Delivery** - GDC measure success not only by IT efficiency but by the strategic value IT delivers to the organisation. 2. **Adaptive Infrastructure** - The IT infrastructure is designed for flexibility, supporting cloud-native solutions and architecture that can easily adapt to changing workloads and demands. 3. **Customer-Centric Innovation** - GDC prioritise understanding and meeting the needs of customers. Agile and adaptive practices allow us to co-create solutions with their customers, 4. **Rapid Response to Change** – GDC's IT systems and teams are highly adaptable, enabling us to respond quickly to changing market conditions, customer preferences, and emerging technologies. 5. **Efficiency and Effectiveness** - Optimise IT processes to eliminate bottlenecks, reduce waste, maximising efficiency, resulting in quicker delivery of solutions & improved resource utilisation. 6. **Data-Driven Decision-Making** - Harness data and analytics to inform decisions and continuously improve GDC IT solutions, ensuring they remain aligned with business objectives and customer expectations. 7. **Empowered Teams** – GDC's IT teams are empowered to make decisions and take ownership of their work, fostering a sense of ownership and accountability. 8. **Collaborative Culture** - Foster a culture of collaboration and teamwork, where IT collaborates closely with business units to drive innovation and deliver value-driven solutions.

3.6 **THEME 6:** Infrastructure Resilience & Optimisation

Background	This theme focusses on the underlying core technology infrastructure that supports the IT service providing the foundation and building blocks for all the technology that GDC use. This includes server room technology, telephony infrastructure, IT security, networking, and cloud services. IT plays a crucial role in supporting various organisational services, and it's vital that the IT platform aligns with the business's goals, particularly in improving efficiency through technology adoption. The theme's focus is on aligning IT services with the organisation's needs and ensuring consistent high performance to support overall business objectives.
Objective	Provide a robust, dependable, efficient, and modern infrastructure that aligns with the business requirements. It must be flexible enough to accommodate changing business needs and support the evolving use of technology, allowing remote work and 24/7 online access to services for customers.
Principles	The main principles for this theme are: 1. **Scalability and Flexibility** - GDC infrastructure can adapt and expand smoothly to handle changing workloads and sudden surges in activity, ensuring uninterrupted operations. 2. **Secure by Design** - Security is at the core of GDC infrastructure, with robust access controls, encryption, and threat detection mechanisms to safeguard data & systems against threats. 3. **Automation and Efficiency** - Automation enhances infrastructure efficiency by automating tasks, minimising errors, and expediting provisioning and configuration processes. 4. **Resilience and High Availability** - GDC infrastructure is architected for high availability and fault tolerance. Failures are gracefully handled, ensuring minimal disruption to operations and services. 5. **Cloud First** - GDC embrace a hybrid or multi-cloud strategy to leverage the best of various cloud providers and avoid vendor lock-in. GDC strategy enhances resilience and flexibility. 6. **Compliance** - Keeping infrastructure up to date and in line with industry compliance. 7. **Availability** - Proactive capacity and scalability planning striving for an "always on" IT service. 8. **Strong Vendor Relationships** - Partnership opportunities are fully explored and developed where viable. 9. **Cost Efficiency and Optimisation** - Service offerings are continually assessed to ensure value for money is achieved whilst delivering excellent IT operational activities.

3.7 THEME 7: Enable Employees Anywhere

Background	"Enabling employees anywhere" refers to the ability to provide workers with the necessary tools, technology, and infrastructure to perform their tasks from various locations, whether in the office, at home, or on the go. This approach supports flexibility, collaboration, and productivity, which are increasingly important in today's dynamic work environment.
Objective	Create a seamless and adaptable work environment where employees have the freedom to work from any location, ensuring they are empowered with the right technology, resources, and support. This theme envisions a future where geographic boundaries are irrelevant, and employees can collaborate effectively, maintain work-life balance, and contribute to organisational success no matter where they choose to work. It prioritises flexibility, connectivity, and innovation to drive productivity and job satisfaction, ultimately leading to a more resilient and competitive organisation.
Principles	The main principles for this theme are: 1. **Technology Enablement** - Provide employees with the necessary technology and tools to work efficiently from any location. This includes access to cloud-based applications, secure remote connectivity, and mobile-friendly solutions. 2. **Security and Compliance** - Prioritise data security and compliance with relevant regulations, implementing robust cybersecurity measures to protect sensitive information regardless of where it is accessed or stored. 3. **Adaptability and Scalability**- Build systems and processes that can adapt to changing circumstances and accommodate a growing remote workforce. 4. **Flexible Work Arrangements** - Offer flexible work options, such as remote work or hybrid models, allowing employees to choose where they work based on their preferences and job requirements. 5. **Training and Skill Development** - Provide training and resources to equip employees with the necessary skills and knowledge to thrive in a remote or hybrid work environment. 6. **Health and Safety Considerations** - Provide resources and guidelines to support employee health and safety, whether they are working in the office or from another location.

3.8 THEME 8: Collaboration and Communication

Background	The IT strategic theme for Collaboration and Communication focuses on leveraging technology to enhance how individuals, teams, and departments within an organisation collaborate, communicate, and share information. It aims to create a cohesive and efficient work environment where communication barriers are reduced, knowledge is readily accessible, and teamwork is facilitated. With the integration of digital tools, platforms, and processes, GDC can foster seamless communication, knowledge sharing, and collaboration across the organisation, ultimately enhancing productivity and innovation.
Objective	Create a highly connected, agile, and innovative organisation, fostering a collaborative, knowledge-sharing, and communicative culture that enhances productivity and the overall effectiveness of the organisation. This theme is not just about implementing technology solutions; it's about transforming how GDC work together, breaking down silos, and harnessing the collective knowledge and creativity of the organisation to drive growth and innovation.
Principles	The main principles for this theme are: 1. **Foster Seamless Communication** - GDC will create an environment where communication barriers are minimised, enabling real-time, cross-functional, and cross-border communication through various channels, from traditional email to modern messaging apps. 2. **Promote Knowledge Sharing** - GDC will cultivate a culture of knowledge sharing and learning, where information is easily accessible, and expertise is readily shared across teams and departments. 3. **Enable Remote and Flexible Work** - GDC will provide the necessary tools and infrastructure to support remote and flexible work arrangements, allowing GDC's workforce to be productive from anywhere. 4. **Enhance Team Collaboration** - GDC will empower teams to collaborate efficiently by providing them with collaborative workspaces, document sharing, and project management tools that facilitate seamless teamwork. 5. **Improve Decision-Making** - GDC will ensure that data and information are readily available to inform decision-making processes, resulting in quicker and more informed choices. 6. **Enhance Customer Engagement** - GDC will extend collaborative efforts to engage with customers and partners, providing them with easy access to information and support, fostering stronger relationships.

4. Strategic Goals

The over-arching strategic goals of **service, value, security**, and **agility** provide the guiding framework for the GDC Information Technology Strategic Plan. GDC is committed to:

- offering responsive and innovative IT services that meet business needs, enhance the end-user experience, and enable digital service delivery.
- making smart investments that ensure high-value and cost-effectiveness.
- ensuring a secure, accessible, and resilient enterprise infrastructure that enables the trusted delivery of programs and services.
- providing a connected and high-performing workforce that uses modern tools.

Goal	Description
SERVICE	A responsive, dynamic, and inventive IT ecosystem that facilitates the provision of integrated, easily accessible, client-focused programs and services to GDC clients while: • ensuring that GDC customers receive the highest level of service quality, efficiency, and responsiveness, creating a positive and lasting impact on their experience and satisfaction. • continuing to implement the enterprise-wide approach to delivering IT services. • adopting emerging technology to improve solution and service delivery.
VALUE	Intelligent investments deliver significant value, are cost-efficient, reusable, and in alignment with business objectives, while also: • encouraging collective use of resources, tools, processes, and systems. • developing enterprise-wide solutions to address common business needs. • ensuring sustainability of IT systems and infrastructure. • strengthening data governance and accountabilities. • adopting more agile procurement approaches, where possible.
SECURITY	A secure and resilient enterprise infrastructure protects information and data, enables the trusted delivery of programs and services, and: • enhances security measures to minimise risk. • provides more consistent management of council networks. • protects personal and sensitive information. • broadens awareness of cybersecurity risks.
AGILITY	An agile, connected, and high-performing workforce with modern tools: • attracts and retains highly skilled and diverse IT talent. • provides a technologically advanced workplace that supports mobility. • promotes digital literacy and collaboration. • pilot's new practices, processes and solutions that exploit information as a strategic asset.

5. Strategic Initiatives

The plan's strategic initiatives encompass a variety of actions, ranging from essential operational needs to forward-thinking strategic endeavours, categorised under three pillars: **Business Support**, **IT Excellence,** and **Innovation**.

5.1 **Initiative**: Business Support

This initiative focuses on building and evolving IT foundational elements, including processes, practices, and infrastructure to enable implementation of current capabilities, technologies, and solutions. This approach will ultimately result in improved programs and services for Greymouth citizens and better internal services for council employees by focusing on developing a modern, reliable, interoperable, and accessible IT environment.

The following table summarises the planned strategic **Business Support** action areas.

Category	Actions
1. **Service Management**	• Develop IT service portfolios and catalogues. • Report on key areas of IT system health performance. • Implement enterprise IT service management tools.
2. **Governance**	• Establish enterprise IT governance. • Document roles and responsibilities for IT and IT security. • Introduce stronger project oversight at the concept phase. • Establish data governance.
3. **Information and Data Management**	• Define a data strategy with data governance goals and objectives • Implement an Information Management Solution • Implement an Electronic Records Management System (ERMS) Document Management Platform
4. **Business Applications**	• Microsoft Office Applications Licensing • Review the current CRM Platform • Enhancement of GIS Platform • ELMO
5. **Enterprise Architecture Alignment and Practices**	• Evolve IT management practices, processes, and tool. • Develop enterprise architectures for business, information, applications, and technology. • Adopt agile approaches to implementing business solutions. • Standardise metadata. • Develop information and data valuation framework. • Develop an information management performance framework.
6. **Agility and Innovation**	• Establish a Digital Advisory Board • Lead Innovation • Embrace Agile Practices • Collaboration with External Partners

5.1.1 Service Management

Ref	Action	Description
BS.1a	**Develop IT service portfolios and catalogues**	An IT service portfolio describes services in terms of business value, including: • a list of services. • a description of how they are bundled or packaged. • a description of the benefits they deliver. An IT service catalogue is a list of available technology resources and offerings within GDC. It is a tactical, operational tool that is intended to make it easier for clients to request IT services on a day-to-day basis. GDC will develop an IT service portfolio and service catalogue that clearly articulate enterprise service expectations for the services they provide.
BS.1b	**Report on key areas of IT system health performance**	Key performance indicators that focus on operational excellence and delivery are critical tools in managing the delivery of IT services. The IT department will put in place metrics for monitoring client satisfaction and key areas of IT system performance (security, availability, reliability, and capacity).
BS.1c	**Implement enterprise IT service management tools**	IT service management (ITSM) refers to an organisation's planning, delivery, operations, and control of IT services offered to clients. GDC will put in place enterprise ITSM tools and make them available to all departments. Doing so will bring consistency to the practice of ITSM and, more importantly, reduce the cost and delays of fulfilling service requests. This will include the implementation of a suitable Help Desk solution for logging and management of service requests etc.

5.1.2 Governance

The importance of IT governance lies in its ability to ensure that GDC's information technology (IT) resources and activities are aligned with its strategic goals and objectives.

- **Alignment with Business Goals:** IT governance aligns IT investments with GDC's overall business strategy to drive its success.
- **Risk Management:** IT governance helps spot and manage IT risks like cyber threats, data breaches, and compliance issues through risk assessment and management processes.
- **Resource Optimisation:** Ensures efficient and effective use of IT resources, including hardware, software, and personnel, leading to cost savings and improved resource allocation.
- **Accountability:** IT governance defines roles and responsibilities for IT decision-makers and stakeholders, clarifying who is accountable for IT-related decisions and outcomes.
- **Compliance and Legal Requirements:** IT governance will help GDC adhere to regulatory requirements related to data privacy, security, and compliance, reducing the risk of legal issues and penalties.
- **Enhanced Decision-Making:** Clear governance enables GDC to make informed IT decisions about investments, project priorities, and technology adoption.
- **Transparency:** IT governance fosters transparency by providing visibility into IT activities and expenditures, which helps to build trust among stakeholders.
- **Resource Prioritisation:** Prioritises GDC IT projects based on their impact on business objectives, ensuring critical projects get needed attention and resources.

- **Continuous Improvement:** IT governance fosters continuous improvement through standards, best practices, and performance metrics at GDC, enabling learning from past experiences and adapting to tech changes.

Ref	Action	Description
BS.2a	**Establish Enterprise IT Governance**	Establish an Enterprise IT Governance Framework with the necessary structures, policies, and procedures to ensure that IT resources are used effectively and aligned with the organisation's strategic objectives. This involves defining roles and responsibilities, setting up accountability mechanisms, establishing IT-related policies, and creating a framework for monitoring and managing IT activities to ensure they support the overall goals of the organisation.
BS.2b	**Document roles and responsibilities for IT and IT security**	Provide clear direction to departments on IT security roles and responsibilities, including security-control objectives and other security-related requirements.
BS.2c	**Introduce stronger project oversight at the concept phase**	GDC will enhance and strengthen the oversight function for IT-enabled projects (defining the solution or the project to implement the solution, allowing for early engagement and setting of direction) by introducing earlier reviews of investment concept cases. For high-risk project investments, GDC will monitor and report on performance and governance throughout the life of the project. Better management of project investments, coupled with an agile approach to development and delivery, maximises value and reduces service delivery costs, enabling the government to respond more rapidly to emerging issues.
BS.2d	**Establish Data Governance**	GDC are committed to making better use of data to inform decision making. To do so, GDC must ensure that the maximum value possible can be extracted from the data that the council collects in support of providing their individual programs and services. Currently, data is fragmented and stored in departmental or program silos, with no coherent council-wide approach to managing data and minimal infrastructure in place to support sharing among stakeholders and to effectively manage the data across its lifetime. To ensure informed decision making based on enterprise-wide data, the council needs to take steps to ensure the sound governance of data and its integrity and quality.

5.1.3 Information and Data Management

Ref	Action	Description
BS.3a	**Define a data strategy with data governance goals and objectives**	Identify the business objectives and desired results for GDC's data strategy. A data strategy identifies, prioritises, and aligns business objectives across the organisation and its various lines of business. A good data strategy will: • Make Data Available. • Maintains Data Consistency. • Maintain Data Accuracy. • Support Data Security.

BS.3b	**Implement an Information Management Solution**	The current lack of adequate information management across the council poses an operational inefficiency, security, and privacy risk. To address this council, need to implement an effective means to catalogue, sort and secure the various sources of information. Looking at current needs and future goals, GDC need to ensure that any system chosen to fulfil this role needs to be flexible.

BS.3c	**Implement an Electronic Records Management System (ERMS) Document Management Platform**	GDC need to implement an electronic records management system to efficiently manage records and meet legal obligations under LGOIMA[5]. The benefits of an ERMS include:
		• Ability to meet legal obligations (LGOIMA)
		• Better control of Document access (Security)
		• Ability to improve workflows (Improved Process)
		  ○ information more accessible to staff.
		  ○ Improved workflows for public interactions
		  ○ Automation of simple tasks
		
		Possible solutions for review, include:
		• LaserFiche
		• Micro Focus Content Manager
		(formerly HP Content Manager, HP Records Manager, HP TRIM)
		• SharePoint
		• SharePoint based solution
		• Egnyte
		• M-File

5.1.4 Business Applications

Ref	Action	Description
BS.4a	**Microsoft Office Applications Licensing**	GDC currently have predominately Microsoft 365 E3 licenses in use. To gain access to a range of features and capabilities that would be beneficial to the operation and security of GDC's environment, GDC should standardise all Microsoft 365 licensing to Business Premium licenses, this would provide the best value for GDC (purchased through All of Government pricing model).
BS.4b	**Review the current CRM Platform**	Review the current CRM solution and the use of workflows.

[5] LGOIMA - Local Government Official Information and Meetings Act
Local Government Official Information and Meetings Act 1987 No 174 (as at 23 August 2023), Public Act Contents – New Zealand Legislation

BS.4c	**Enhancement of GIS Platform**	The current GIS platform is changing with the retirement of IntraMAPS (functionality now being provided by ArcGIS). GDC now enhance the GIS user experience by implementing Smart Maps. Smart Maps are a suite of user-friendly maps designed to provide fast access to information. Maps are easy to print and can be viewed on smartphones or tablets as well as laptops and PCs. Available in ArcGIS Online and ArcGIS Server, smart mapping appears when working with your hosted data. Refer to GIS Mapping Software, Location Intelligence & Spatial Analytics | Esri for further information. Review AssetFinda's out-of-the-box functionality for GIS interfaces to ArcGIS, Mapinfo, and QGIS.
BS.4d	**Implement HR Management solution**	The Human Resources Management solution ELMO is currently in the process of implementation. Once implemented, ensure that all on-boarding and off-boarding processes are setup and automated using this platform.

5.1.5 Enterprise Architecture Alignment and Practices

Sound IT management starts with consistent planning based on documented descriptions of the enterprise. With an understanding of what is in play, management can adopt solutions that best address their business needs.

Ref	Action	Description
BS.5a	**Evolve IT management practices, processes, and tools**	IT plans should be executed so that they align with the GDC's Strategic Plan for IT and overall enterprise modernisation priorities. Important tools to support management include: • investment plans • architectural reviews • application portfolio management • expenditure and performance reporting Better IT investments for business results drive improvements in IT management processes & tools. • Manage IT consistently and with greater maturity. • better understand IT at the enterprise level. • evolve digital service delivery. • monitor and track progress against council priorities. • set future priorities.

BS.5b	**Develop enterprise architectures for business, information, application, and technology**	Developing enterprise architectures is vital for organisations looking to improve IT investments, align with business goals, and make smart decisions in a fast-changing IT landscape. It offers a structured way to handle complexity and change in IT environments. This process involves four key architectural domains: **Business Architecture:** Focuses on understanding and modelling the organisation's business strategy, processes, goals, and structure. It helps ensure that IT solutions are closely aligned with the business's needs and objectives. **Information Architecture:** Involves defining how data is organised, stored, and used within the organisation. It addresses data governance, data quality, data flow, and data integration to ensure that information is available, reliable, and supports decision-making. **Application Architecture:** Defines the structure and relationships of software applications used within the organisation. It includes considerations like application integration, development standards, and the selection of technologies and platforms to support business processes. **Technology Architecture:** Technology architecture focuses on the hardware, software, networking, and infrastructure components that underpin the organisation's IT environment. It includes decisions regarding hardware platforms, network design, security measures, and technology standards.
BS.5c	**Adopt agile approaches to implementing business solutions**	The adoption of a flexible and iterative methodology for designing, developing, and deploying solutions that address business needs and challenges. Agile methodologies are characterised by their collaborative, adaptive, and customer-centric nature. By adopting agile practices, organisations can better align their solutions with changing business needs, improve customer satisfaction, and increase their overall responsiveness in a rapidly changing business environment.
BS.5d	**Standardise metadata**	Metadata is the backbone of digital automated processes, information retrieval, and the use and sharing of information and data. Metadata defines and describes the structure and meaning of information and data and of the context and systems in which they exist. Metadata supports efficient and effective management of information and data resources over time, which facilitates decision making, accountability and the efficient delivery of council programs and services. Standardised metadata supports: • interoperability within and across systems • reuse of information resources within, across and outside the GDC

BS.5e	**Develop an information and data valuation framework**	Organisations that are information-centred and information-savvy recognise information and data as valuable assets. Accounting for information and data as strategic assets, similar to human and financial assets, allows organisations and its partners to maximise the full potential of all information and data. Developing an information and data valuation framework means creating a structured way to figure out how valuable the information and data in the organisation is. It helps us understand which data is really important and how it can be used to make better decisions and achieve its goals. This framework involves coming up with rules and methods to assess and rate the value of different pieces of data based on classification. It helps the organisation manage its data more effectively and make better use of it.
BS.5f	**Develop an information management performance framework**	Developing an information management performance framework means creating a structured way to measure and evaluate how well an organisation is managing its information. This framework helps the organisation understand its strengths and weaknesses in information management, allowing it to make improvements and ensure that information is well-organised, secure, and serves its purposes effectively. By leveraging the right performance metrics, the council can better understand the impact of information and data management on its business. Designing metrics that are forward-looking and closely linked to business outcomes can help establish and better communicate the value of information and data. Furthermore, by shifting the focus of measurement away from compliance toward outcomes, desired behaviour changes can be fostered, including increased information sharing and reuse and improved data quality.

5.1.6 Agility and Innovation

GDC is transforming its IT to better serve Council customers, with innovation being key to delivering on this agenda. Successful innovation combines creativity with process to transform novel ideas into business enablers that deliver tangible results. It embraces experimentation and intelligent risk taking, bringing new approaches that address existing problems and leverage future opportunities.

Innovation calls for collaboration, both with new and traditional partners, to identify and break down any barriers that prevent us from achieving maximum results.

Ref	Action	Description
BS.6a	**Establish a Digital Advisory Board**	To benefit from a broader range of expertise and experience, GDC will establish a Digital Advisory Board to provide advice to the GDC ELT on IT activities related to strategic direction, service delivery and investment priorities.
BS.6b	**Lead Innovation**	Leading innovation in information technology solutions for the organisation involves actively seeking out opportunities to leverage technology for competitive advantage, foster a culture of innovation, and drive meaningful change within the organisation.
BS.6c	**Embrace Agile Practices**	Implement agile methodologies like Scrum or Kanban to enhance project management and development processes, allowing teams to respond quickly to changing requirements and market conditions.
BS.6d	**Collaboration with External Partners**	Collaborate with external partners, such as technology vendors, startups, and industry experts, to access new ideas, expertise, and emerging technologies.

5.2 Initiative: IT Excellence

This initiative addresses the management and governance of Information Technology across the council in a way that ensures that IT investments:

- take advantage of economies of scale.
- demonstrate value.
- are sustainable.

The following table summarises the planned strategic **IT Excellence** Action areas.

Category	Actions
1. **Technology Modernisation**	• Cloud-First Adoption Strategy • Core Network Infrastructure Upgrade • Structured Cabling Upgrade • Wide Area Network (WAN) • WAN Redundancy • Provide extended Wi-Fi Access • Server & Storage Infrastructure • Backup & Recovery Capabilities • Disaster Recovery • End-Point Device Management • IT Asset Management (ITAM) • Monitoring and Logging • Building Security
2. **Defence in Depth**	• Implement an enterprise approach to vulnerability and patch management. • Manage and control administrative privileges.
3. **Trusted Solutions and Services**	• Protect web transactions to and from external-facing websites. • Implement a secure communication service for classified information. • Implement enterprise data loss prevention.
4. **Security Awareness and Training**	• Enhance awareness of enterprise cybersecurity threat and risk environment
5. **Modern Workplace**	• Modernise workplace technology devices. • Support a mobile workforce. • Improve IT accessibility.
6. **Digital Collaboration**	• Advance digital collaboration.

5.2.1 Technology Modernization

Ref	Action	Description

EX.1a	**Cloud First Strategy**	When looking at new solutions, GDC will adopt a "cloud-first approach" where preference is given to using cloud computing services and solutions for its technology needs over traditional on-premises. This is not a cloud only policy, in this approach, cloud services are the default choice for deploying new applications, managing data, and running IT operations, however, some solutions are still more cost-effective, and functional as an on-premises or hybrid solution.
EX.1b	**Core Network Infrastructure Upgrade**	The core network is currently running on a 10/100 platform which presents a significant bottleneck in optimising operations across all ICT platforms. Industry-standard has been 10/100/1000 for over a decade. The core network infrastructure should be upgraded to support a minimum of 1Gbps network connections. In head office this will also be dependent on the current structured cabling installed (refer to SA2c).
EX.1c	**Structured Cabling Upgrade**	The structured cabling (Unshielded Twisted Pair (UTP) cable) currently installed in the head office building is predominantly of type category 5. This severely restricts network speeds on the network to a maximum of 100MBps. A plan should be devised to upgrade/replace the current UTP cabling to category 6 or 7 in head office. This has already been identified in current proposals to refurbish the head office building.
EX.1d	**Wide Area Network (WAN) upgrade**	The current WAN system is a fully managed solution and has all the remote sites connected to head office, with a single break-out point to the web services. This is traditionally the standard design for multi-site networks to ensure secure communications outside of the GDC LAN (Local Network). The fully managed WAN solution is not a cost-effective service for the council and does not offer many of the benefits now available in UFB (Ultrafast broadband) networks. The few benefits it does allow for (Inter-site connectivity and Reliability) can be achieved via more cost-effective and robust solutions. GDC should migrate from the current WAN solution to a new platform based on SDWAN connections with UFB, and extended site failover with 4G and Starlink. Inter-site communication should be achieved using SDWAN on firewall-controlled connections at each site with ZTNA (Zero trust network access) solutions; these would allow us to route traffic using any connectivity solution via software/cloud-based mechanisms. This also enables the council to secure external connections for council devices operating off-site (work from home) while removing the need for a traditional dial-in VPN.
EX.1e	**WAN Redundancy**	With the implementation of a new wide area network, redundant connectivity should be included to provide redundancy in all WAN connections using 4G and/or Starlink connections. Adding redundant satellite connectivity for the Main office and WRC is a priority to ensure connectivity during a significant event. As both UFB and Cell infrastructure share some critical points of failure, having a completely independent form of communication is advisable.

EX.1f	**Wi-Fi upgrade and extend coverage.**	The current wireless network is aging and limited in coverage and capabilities. Access to wireless data networks is critical for employee productivity. GDC will ensure that there is widespread, secure, and inclusive availability of Wi-Fi (wireless internet) coverage across all council buildings and locations, that will allow users to connect to council services. It will ensure that users have reliable and extensive access to Wi-Fi services for their devices, such as laptops, smartphones, tablets, and other wireless-capable devices. This is important for enabling seamless connectivity and productivity to transact council business.
EX.1g	**Server & Storage Infrastructure replacement.**	The council currently runs a mixed-aged server infrastructure. Some hardware is severely aged, while other components are still in their supported life, approaching replacement. As part of the "Cloud-First' adoption strategy, current applications and workloads should be assessed to determine where they are best suited to be hosted (Cloud, On-premises, or Hybrid). A prime example of this is email, currently run in a hybrid environment with Exchange on-premises and Microsoft 365 Exchange Online (this is an on-going project to fully migrate email fully to Exchange Online). The final goal is to move as much of the workload into the cloud as viable. Some core systems will most likely remain on-premises, and require a suitable, appropriately resourced, and resilient server/storage infrastructure to host them.
EX.1h	**Backup & Recovery Capabilities**	With workload hosting locations changing (on-premises and cloud), along with changes to the wide area network, consideration needs to be given to how GDC backup data and systems on-premises and in the cloud. This also includes provision of 'Air-Gapped' backups which form an essential component of GDC's disaster recovery plan (see SA2i). GDC should fully identify all backup requirements for the ICT environment and implement an appropriate backup/recovery solution.
EX.1i	**Disaster Recovery Plan**	GDC currently do not have any complete, tested disaster recovery capabilities for the IT infrastructure, which poses a high risk to the business. Appropriate backup/recovery capabilities should be identified and implemented (SA2h), and appropriate processes and testing schedules implemented to provide an end-to-end disaster recovery capability. All network and server infrastructure upgrades should incorporate resiliency and redundancy in their capabilities. Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for the business need to be identified and documented.

EX.1j	**End-Point Device Management**	Endpoint device management is vital for security, efficiency, and compliance. It ensures devices are secure, up-to-date, and optimised, reducing risks, enhancing productivity, and helping GDC adapt to evolving technology trends. GDC need to identify and implement a suitable End-Point Management solution to provides a set of tools and features that help GDC manage and secure computers, mobile devices, and applications. It will allow IT teams to control and protect these devices, ensuring they work correctly and stay safe from security threats. A good example of this is Microsoft's End Point Manager (InTunes), which is provided as part of the Microsoft 365 Business Premium license.
EX.1k	**IT Asset Management (ITAM)**	IT Asset Management is essential for organisations of all sizes as it helps optimise IT spending, reduce risks, improve security, and ensure that IT resources are aligned with business objectives. It is a critical component of effective IT governance and will help GDC make informed decisions about technology investments. GDC should identify and implement a suitable ITAM solution.
EX.1l	**Centralized Monitoring and Logging**	Monitoring and logging are crucial for maintaining the health, security, and performance of computer systems. Monitoring helps catch issues in real-time, ensuring smooth operations, while logging provides a record for troubleshooting, security analysis, and compliance, helping organisations understand and improve their IT environments. GDC should implement a centralised SIEM (Security and Information Event Management) solution to manage all logging within the ICT environment. Implement a monitoring and Alert management solution for complete 24/7 monitoring of GDC's ICT infrastructure. This includes environmental monitoring of the computer room which is currently not in place.
EX.1m	**Building Security and Monitoring**	The current Security System is controlled via a Win 7 machine (this poses a security risk to the business). The current building security cards use a proprietary encryption method which is no longer supported, so the cards will not work with other systems (GDC are also struggling to get additional cards as this encryption standard has been discontinued some time ago for brand agnostic encryption). GDC currently have very minimal CCTV capabilities. A new IP based CCTV platform should be implemented that provides extensive coverage across all council facilities which sufficient storage to enable playback if required for forensic purposes. There have been some proposals for CCTV options already presented to council. A new fully integrated building security system across all council facilities should be identified and implemented.

5.2.2 Defense in Depth

Ref	Action	Description
EX.2a	**Asset Inventory**	Create a full inventory of all GDC assets, including hardware, software, data, and personnel, using an automated platform with auto-update capabilities. This helps you understand what needs protection.

EX.2b	**Network Segmentation**	Segment the GDC network infratsructure using VLANs, physical isolation and firewalls, to isolate sensitive systems and data from less critical resources. This limits the lateral movement of attackers within the network. This should isolate Operational Technology (OT) such as SCADA etc, from IT network infrastructure.
EX.2c	**Perimeter Security**	Implement perimeter security measures, such as firewalls, intrusion detection systems, and intrusion prevention systems, to protect the network from external threats. This should isolate Operational Technology (OT) such as SCADA etc, from IT network infrastructure.
EX.2d	**Access Control**	Implement strong access controls, including user authentication and authorisation mechanisms, to ensure that only authorised personnel have access to critical systems and data.
EX.2e	**Security Awareness Training / Program**	Security Awareness Training is an ongoing process that helps create a security-conscious workforce and reduces the risk of security incidents caused by human error. It is a critical element of a holistic cybersecurity strategy. Human error is a common cause of security breaches. Phishing simulation is a specific and valuable component of Security Awareness Training designed to educate employees and users about the dangers of phishing attacks and improve their ability to recognise and respond to phishing attempts effectively.
EX.2f	**Document Security Policies and Procedures**	Develop and document security policies and procedures that align with GDC's goals and compliance requirements. These policies should cover areas such as access control, data protection, and incident response.
EX.2g	**Enforce Data Encryption**	Data encryption is a critical measure to protect sensitive information from unauthorised access, and it is an essential component of a comprehensive cybersecurity strategy. It helps safeguard data both at rest and in transit, ensuring the confidentiality and integrity of valuable information. Encrypt sensitive data both at rest and in transit to protect it from unauthorised access.
EX.2h	**Patch Management**	Keep all software and systems up to date with the latest security patches and updates to address known vulnerabilities. Establish a patch management process to keep software and systems secure by regularly applying updates and patches to address known vulnerabilities.
EX.2i	**Incident Response Plan**	Develop and regularly test an incident response plan that outlines how GDC will respond to security incidents. This should include communication plans and procedures for containing and mitigating breaches.
EX.2j	**Monitoring and Logging Tools**	Implement continuous monitoring of the network and systems. Use security information and event management (SIEM) tools to collect and analyze logs for signs of suspicious activity.
EX.2k	**Regulatory Compliance**	Ensure that security practices align with industry standards and regulatory requirements specific to council and local government requirements.
EX.2l	**Third-Party Risk Assessment**	Assessing and managing the security risks posed by third-party vendors and contractors who have access to GDC systems or data is crucial to safeguarding GDC's sensitive information and maintaining overall cybersecurity. Assess and manage the security risks posed by third-party vendors and contractors who have access to GDC systems or data.

EX.2m	**Manage and Control Administrative Privileges**	GDC need to manage internal risks to the security of their IT environment. Privileged accounts (such as local or domain administrators and other accounts that have elevated access) are the most powerful accounts in any organisation. They are also the most targeted by malicious parties that wish to compromise council information. GDC will work to minimise the misuse of any account that has elevated privileges, either malicious or accidental. Tools and processes will be implemented to ensure the proper management, control and monitoring of such accounts, including establishing strong authentication mechanisms for all privileged accounts. GDCwill also implement measures to manage and control the life cycle of and access to privileged accounts, including: • audits and reviews to confirm validity of privileges • continuous monitoring to look for uncharacteristic behaviour
EX.2n	**Security Continuous Improvement**	Security is an ongoing process. Continuously monitor, evaluate, and improve GDC security measures to adapt to evolving threats.
EX.2o	**Implement an enterprise approach to vulnerability management**	The council must ensure that vulnerabilities are identified and remediated quickly to minimise the risk of future intrusion and potential loss. GDC will implement an enterprise-wide vulnerability and patch management capability to systematically detect and remediate vulnerabilities.
EX.2p	**Restore test plan**	Regularly back up critical data and test the restoration process to ensure business continuity in case of data loss or a cyberattack.

<table>
<tr>
<td>EX.2q</td>
<td>Implement security profiles on end-point devices.

(Security profiles)</td>
<td>Malicious actors often target vulnerable Internet-facing services and devices to breach IT systems and access sensitive information. Endpoint devices like laptops, tablets, and servers serve as entry points for these threats, potentially leading to data compromise, including personal information.

Default settings in operating systems and applications often contain unnecessary componentsand setting that are easily identified using automated tools. In an enterprise context, addressing system weaknesses and misconfigurations is crucial to prevent attacks on other organisations and ensure a secure environment. Enhancing endpoint device security is a key aspect of achieving this security.

Recognising the risk posed by misconfigured end-point devices, GDC will implement a platform that will effectively manage and secure devices, applications, and data across the organisation, regardless of the platform or device type. Simplifying endpoint management will enhance security, and ensure compliance with organisational policies. Additional security controls, such as host-based intrusion prevention and application whitelisting (a computer administrative practice used to prevent unauthorised programs from running) will be implemented to further ensure the integrity of systems and information.

Microsoft 365 Endpoint Manager, which includes Microsoft Intune, plays a significant role in addressing the risk associated with misconfigured endpoint devices. Here's how it aligns with the goal described by GDC:

<table>
<tr><td>Endpoint Device Profiles:</td><td>Microsoft Intune lets GDC create and manage device profiles for laptops, tablets, and mobile devices, setting security configurations and policies.</td></tr>
<tr><td>Security Best Practices:</td><td>Intune enforces security best practices on endpoints, reducing the risk of misconfigurations with administrator-configured policies.</td></tr>
<tr><td>Regular Validation and Updates:</td><td>Intune enables ongoing monitoring and updates of device profiles, ensuring they align with GDC's security standards and practices.</td></tr>
<tr><td>Application of Security Controls:</td><td>With Intune, GDC can boost endpoint security through added measures like intrusion prevention, encryption, and application control.</td></tr>
<tr><td>Integration with Microsoft 365:</td><td>Microsoft 365 Endpoint Manager integrates with other Microsoft 365 services, offering a comprehensive approach to device management and security, including features like conditional access, data loss prevention, and threat protection.</td></tr>
</table>

Microsoft 365 Endpoint Manager (Intune) supports GDC's goal by providing a complete toolkit to manage and safeguard endpoint devices. It helps create consistent security settings, keep configurations up-to-date, and add extra security measures to prevent issues from wrongly set endpoints</td>
</tr>
<tr>
<td>EX.2r</td>
<td>End-Point Security Tools</td>
<td>Use endpoint security solutions, such as antivirus software, endpoint detection and response (EDR) tools, and mobile device management (MDM) systems, to protect individual devices.</td>
</tr>
</table>

By following these steps and adopting a Defense-in-Depth strategy, GDC can significantly enhance its cybersecurity posture and reduce the risk of security breaches.

5.2.3 Trusted Solutions and Services

Establishing identity is fundamental to most council interactions that involve exchanging information or permitting access to sensitive resources.

Ref	Action	Description
EX.3a	**Protect web transactions to and from external-facing websites**	As more citizen's interface electronically with the GDC, the amount of sensitive information transferred to and from council websites will increase. To maintain maximum trust in these online transactions, the council must protect them. GDC will establish an "HTTPS everywhere" standard that will require the use of HTTPS protocol for all external-facing websites and cloud services. This protocol, along with approved encryption algorithms, will ensure the secure transmission of data online and the delivery of secure web services.
EX.3b	**Implement a trusted digital identity for people accessing internal government networks and systems**	GDC will take an enterprise-wide approach to internal identity, credential and access management to: • reduce costs • promote interoperability • improve end-user experience by reducing the need for multiple user IDs and passwords GDC will implement common internal identity and credential processes and technologies tailored to the level of assurance required for particular business processes. For example, a unique digital identity will be needed to authenticate employees, contractors, trusted guests or any other authorised users who access internal council networks and systems. GDC will migrate applications to this new enterprise service when their applications are upgraded as part of regular life-cycle maintenance of assets.
EX.3c	**Implement enterprise data loss prevention**	With its responsibility for maintaining large amounts of sensitive data, the GDC needs to minimise the risk of unauthorised disclosure. GDC will establish a framework to support an enterprise approach to data loss prevention that will be supported by Information Mannagement solutions. Preventing the unauthorised transfer or release of sensitive information involves first identifying sensitive data. Unauthorised data flows and operations will be monitored, detected and blocked.

5.2.4 Security Awareness and Training

Understanding the assets within an IT environment is essential to knowing what to protect and enables the council to be more proactive and efficient when responding to threats and attacks.

Ref	Action	Description
EX.4a	**Enable comprehensive understanding of end-point devices**	It is critical to be able to proactively and accurately determine: • the status of all end-point devices • what is running on them • who is accessing them End-point devices that pose a risk to the enterprise can be identified, allowing the council to be more effective when responding to threats and attacks. GDC will acquire and implement tools and processes to enable a real-time, enterprise view of the current status and configuration of government end-point devices. Such information includes: • hardware and software versions • operating system versions • patch installations Procedures will be established to mitigate risks to the GDC network should immediate action be required.
EX.4b	**Enhance awareness of enterprise cyberthreat and risk environment**	As the council adopts an enterprise approach, and programs and services become more integrated, it will be imperative that cyber-risks are also managed at the enterprise level. Key to effectively managing enterprise-wide risk is understanding the changing cyberthreat landscape (for example, who is trying to exploit government networks and systems, by what means, and for what purpose). GDC need a proactive approach to cybersecurity in order to keep pace with emerging threats, technologies and trends. GDC will establish a centralised capability to conduct governance, risk and compliance management activities in order to gain a holistic picture of cyber-related business risks at GDC. This capability will pull together data from multiple sources, for example, threat assessments, risk registers, investment plans, audit results and critical asset listings, to feed a consolidated enterprise view of cyber-risks. One of the key data sources will be the GDC Enterprise Threat Assessment. The continuous monitoring of the cyberthreat and risk landscape will inform decision making and influence how corrective actions are prioritised across the enterprise to ensure maximum protection of council assets.

5.2.5 Modern Workplace

Information and technology are key enablers of a modern workplace that support collaboration, innovation, and mobility. Ensuring that smart technology provides a consistent, accessible workplace experience throughout council will improve how all employees work together and provide better services to GDC customers.

Ref	Action	Description
EX.5a	**Modernise Workplace Technology Devices**	Workplace technology devices are essential for a modern workplace and a collaborative, mobile workforce. GDC will establish enterprise standards and processes for life-cycle management and set direction to guide future workplace technology devices standards and secure configurations.
EX.5b	**Support a mobile workforce**	GDC is committed to and encourages an open and collaborative work environment where mobile devices are used. GDC will develop a mobility strategy, focusing initially on smartphones, tablets and laptops.
EX.5c	**Provide desktop videoconferencing to employees**	Increased access to videoconferencing supports the collaborative operations of virtual teams across departments, time zones and regions.
EX.5d	**Improve IT accessibility**	Enhance the ease with which individuals, including those with disabilities, can access and use council information technology (IT) systems, software, and digital content. This improvement aims to make IT resources more inclusive and user-friendly for a broader range of people.

5.2.6 Digital Collaboration

Digital collaboration refers to the skills and mindset needed to work effectively in an open digital environment. Tools that respect council requirements such as accessibility, privacy, security.

Ref	Action	Description
EX.6a	**Create a Digital Collaboration Strategy**	Develop a comprehensive strategy that outlines how digital collaboration will be integrated into GDC business processes.
EX.6b	**Promote digital literacy and collaboration**	Digital literacy means more than just basic computer skills. It's crucial for getting the most out of the technology GDC have and making sure it helps us work better, not worse. GDC will work with partners to create a program that helps all council employees: • Understand data better • Make decisions based on evidence • Be good digital citizens inside and outside the organisation.
EX.6c	**Provide Training and Support**	Offer training sessions to employees to ensure they are proficient in using the chosen collaboration tools. Provide ongoing support and resources to address questions, issues, and updates related to the tools.

5.3 **Initiative**: Innovation

This initiative focuses on safeguarding sensitive council data and ensuring that citizens accessing online services can trust the council with their personal information. As the shift to digital services increases and the sophistication and frequency of cyberattacks grow, GDC's defences must also evolve.

In essence, information technology serves as an enabler, offering the digital infrastructure and tools necessary to foster staff and community engagement. By harnessing IT resources effectively, organisations can strengthen their connections with their communities, improve communication, and drive more inclusive and participatory engagement processes.

The following table summarises the planned strategic **Innovation** action areas.

Category	Actions
1. **Sustainability**	• Ensure IT infrastructure sustainability. • Rationalise investments. • Develop process to balance infrastructure supply and demand.
2. **Community Engagement**	• Better Public Services - Increasing GDC customers' ability to access and interact with digital service channels (Website, social media etc). • Enable on-line events, webinars, and Virtual Town Halls.
3. **Staff Engagement**	• Staff Engagement in IT Projects. • Work Flexibility.

5.3.1 Sustainability

Ensuring that IT investments are sustainable and that they meet business needs, enabling GDC to provide better services to GDC customers.

Ref	Action	Description
IN.1a	**Ensure IT Infrastructure Sustainability**	A sustainable funding model must take into account the regular renewal cycle of IT infrastructure assets and the appropriate level of investment. GDC will explore alternative financial and service delivery models to address IT renewal.
IN.1b	**Rationalise Investments**	In keeping with enterprise IT governance, spending on new or significant changes to certain IT and IT-enabled projects will be subject to consultation and approval by ELT/SLT. Departments will take an enterprise approach to managing their portfolio of applications to: • determine opportunities for common, council-wide solutions. • retire aging and at-risk applications. • applications that remain in use and that support mission-critical business functions are to be kept evergreen until they can be replaced by modern solutions.
IN.1c	**Develop a process to balance infrastructure supply and demand**	In addition to prioritising projects and initiatives, management will develop a framework to allow departments and the council to access alternative service options where appropriate, while maintaining enterprise standards. This approach will reduce capacity pressures while allowing departments to continue progressing with projects, programs and service delivery.

5.3.2 Community Engagement

A vital outcome of the IT strategy is to improve council engagement with the community.

Ref	Action	Description
IN.2a	**Build on Core Community Functions**	Giving the community access to more services and allowing them to carry out more core functions via digital means. This will enable the council to optimise service delivery and better oversite into delivery time frames and service levels.
IN.2b	**Provide Communications Channels**	Information Technology can provide better communication channels for the council to express ideas and project development to the community and give the community more effective channels to express their concerns and ideas to the council. Customer self-service.
IN.2c	**Enable on-line events, webinars, and Virtual Town Halls**	Facilitate online events, webinars, and virtual town halls, allowing staff to engage with the community in real-time, even when physical meetings are not possible.

5.3.3 Staff Engagement

Ref	Action	Description
IN.3a	**Staff Engagement in IT Projects**	Staff should also be engaged from the start of all IT projects as getting early buy-in can improve the delivery process and ensure an optimal outcome. Incorporating staff input into IT projects not only enhances the likelihood of project success but also fosters a culture of collaboration and engagement within the organisation. It's an investment in both the project's outcome and the satisfaction and productivity of employees.
IN.3b	**Work Flexibility**	Due to changes brought on by Covid-19, most organisations have determined that allowing work flexibility generally has a positive outcome on productivity and staff satisfaction. It is now the 2nd highest criterion for job satisfaction. Council should look to adopt a work Anywhere at any time strategy; this would expand the council's ability to support current staff. It also presents a future opportunity for the council to utilise skillsets outside the region, an approach that has been adopted across the globe.

6. IT Strategic Plan Implementation

The implementation of the strategy will be developed annually by the Grey District Council. To achieve the longer-term IT goals, the strategy is executed incrementally through the Programme of Work & Operational Planned Activities (OPAs)

The Grey District Council executive leadership team (ELT), regularly review the progress of the OPAs to ensure alignment to the Strategic Plan Goals and update the Programme of Work. The ELT prioritise the elements of the Strategic Plan to drive actions and investments toward successful mission delivery.

6.1 Programme of Work

The Programme of Work summarises all planned IT Strategic Goals for the defined period, it summaries strategic level information for each goal, identifying estimated costs, priority, status and timeframes.

This is a management tool for the ELT team.

6.2 Operational Planned Activities (OPA)

OPAs will be developed to support the IT Strategic Plan Goals and Objectives and ensure that the goals are met. OPA's are task specific project plans, led and approved by the ELT (who will set the scope, milestones, and metrics to achieve the desired results) but typically created and managed by the IT technical resources in the business.

OPAs are periodically reviewed and refined to adapt to challenges and ensure success in achieving the objectives and larger strategic priorities.

Operational Plan Activities (OPA) detail the specific activities and tasks for the immediate 12-month period and will be updated if the planned work carries over to the next 12-24 month period.

7. Monitoring & Measuring Progress

Without the measurement of progress, a strategic planning endeavour is unlikely to realise its intended outcomes. It's only by steadfastly ensuring accountability for both the delivery and the alignment of progress with the plan that GDC can truly make an impact and meet the established expectations.

7.1 Resourcing the Delivery

Funding for the IT Strategy 2023-2026 will be incorporated within Information Technologies' annual budget and capital programme and drawn down based on costed business cases. Additional resources and investment may also be required if the pace of delivery required by the business is greater than current delivery capacity.

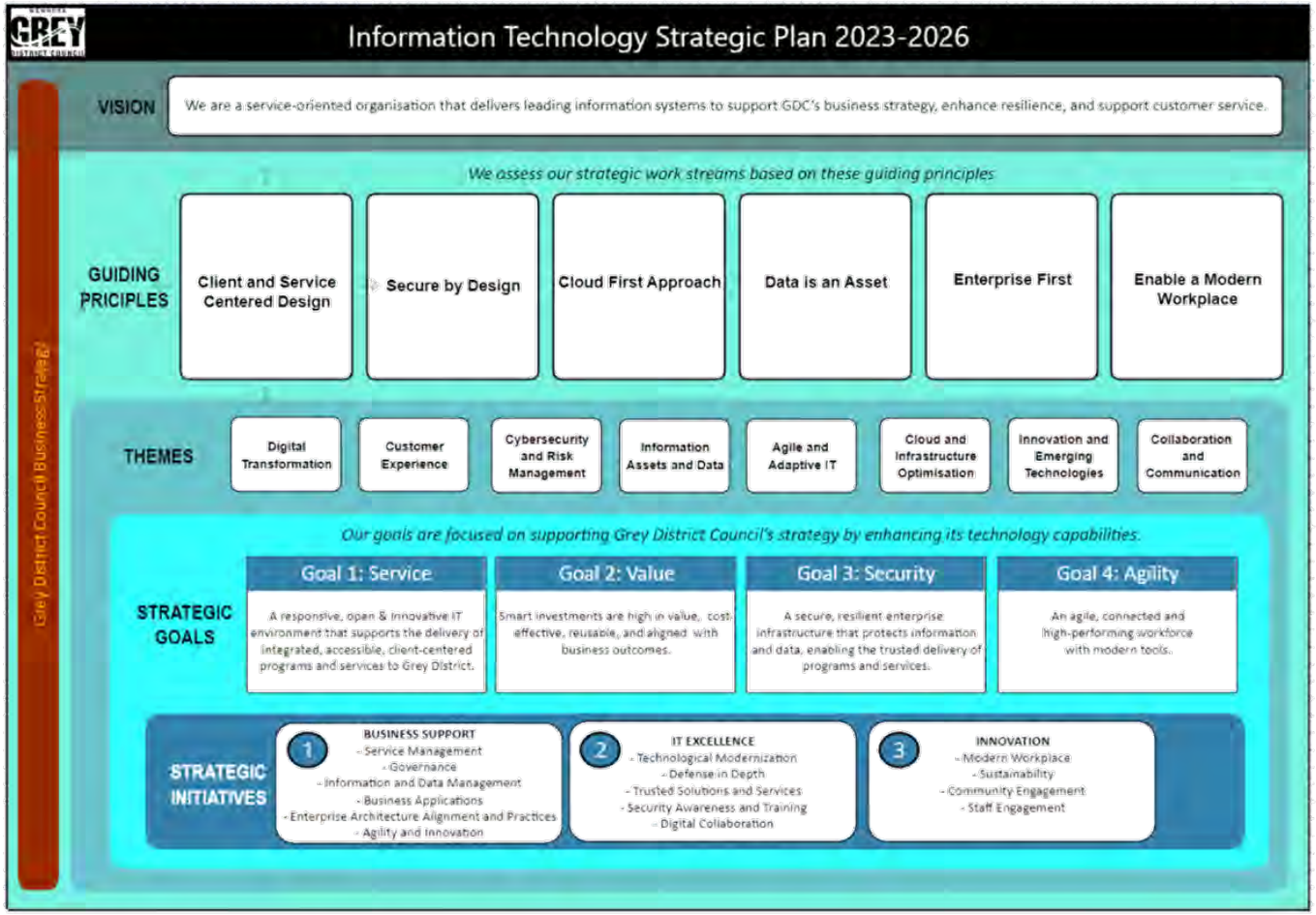
7.2 Monitoring and Reporting Progress

It is essential that GDC monitor progress and ensure that the work GDC are doing is delivering a tangible difference to GDC staff, business, and clients. Ensuring that the OPA's and Programme of Work are actively maintained and updated (which will identify the delivery of priorities and will set out key milestones and achievements), will provide a mechanism for us to actively monitor the implementation of IT Strategic goals.

In addition to measuring progress, it is critical that the strategic plan is reviewed regularly. This is to ensure that GDC account for changes in business direction, new influences, and drivers (internal or external) and to ensure that the steps being taking are delivering the expected results. Progress in implementing the strategy and delivery plan will be reported to the ELT monthly.

The following PDCA diagram depicts the cyclical nature of effective planning:

8. Appendix A


Information Technology Strategic Plan 2023-2026
VISION
We are a service-oriented organisation that delivers leading information systems to support GDC's business strategy, enhance resilience, and support customer service.
Grey District Council Business Strategy
We assess our strategic work streams based on these guiding principles
GUIDING PRICIPLES
Client and Service Centered Design
Secure by Design
Cloud First Approach
Data is an Asset
Enterprise First
Enable a Modern Workplace
THEMES
Digital Transformation
Customer Experience
Cybersecurity and Risk Management
Information Assets and Data
Agile and Adaptive IT
Cloud and Infrastructure Optimisation
Innovation and Emerging Technologies
Collaboration and Communication
Our goals are focused on supporting Grey District Council's strategy by enhancing its technology capabilities.
STRATEGIC GOALS
Goal 1: Service
A responsive, open & innovative IT environment that supports the delivery of integrated, accessible, client-centered programs and services to Grey District.
Goal 2: Value
Smart investments are high in value, cost effective, reusable, and aligned with business outcomes.
Goal 3: Security
A secure, resilient enterprise infrastructure that protects information and data, enabling the trusted delivery of programs and services.
Goal 4: Agility
An agile, connected and high-performing workforce with modern tools.
STRATEGIC INITIATIVES
1
BUSINESS SUPPORT
- Service Management
- Governance
- Information and Data Management
- Business Applications
- Enterprise Architecture Alignment and Practices
- Agility and Innovation
2
IT EXCELLENCE
- Technological Modernization
- Defense in Depth
- Trusted Solutions and Services
- Security Awareness and Training
- Digital Collaboration
3
INNOVATION
- Modern Workplace
- Sustainability
- Community Engagement
- Staff Engagement

9. Appendix B

9.1 Cloud Computing

This appendix explains aspects of cloud computing, including the characteristics, models, and types.

"**Cloud computing** is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

9.1.1 Advantages of Cloud Computing

The following is a list of characteristics of a cloud-computing environment. Not all characteristics may be present in a specific cloud solution.

- **Elasticity and Scalability** - Cloud computing gives you the ability to expand and reduce resources according to your specific service requirement. For example, you may need many server resources for the duration of a specific task. You can then release these server resources after you complete your task.
- **Pay-per-use** - You pay for cloud services only when you use them, either for the short term (for example, for CPU time) or for a longer duration (for example, for cloud-based storage or vault services).
- **On Demand** - Because you invoke cloud services only when you need them, they are not permanent parts of your IT infrastructure—a significant advantage for cloud use as opposed to internal IT services. With cloud services there is no need to have dedicated resources waiting to be used, as is the case with internal services.
- **Resiliency** - The resiliency of a cloud service offering can completely isolate the failure of server and storage resources from cloud users. Work is migrated to a different physical resource in the cloud with or without user awareness and intervention. This characteristic often makes cloud solutions attractive for fault tolerance and business continuity reasons.
- **Multi-tenancy** - Public cloud services providers often can host the cloud services for multiple users within the same infrastructure. Server and storage isolation may be physical or virtual depending upon the specific user requirements.
- **Workload Movement** - This characteristic is related to resiliency and cost considerations. Here, cloud-computing providers can migrate workloads across servers—both inside the data centre and across data centres (even in a different geographic area). This migration might be necessitated by cost (less expensive to run a workload in a data centre in another country based on time of day or power requirements) or efficiency considerations (for example, network bandwidth). A third reason could be regulatory considerations for certain types of workloads.

Cloud computing involves shifting the bulk of the costs from a capital expenditure (CapEx) model – i.e., buying and installing servers, storage, networking, and related infrastructure - to an operating expense (OpEx) model, where you pay for usage of these types of resources. Major Models in Cloud Computing The following is an explanation of some popular models of cloud computing that are offered today as services.

9.1.2 Cloud Classifications

Public, Private Clouds - So far, GDC have focused on cloud service providers whose data centres are external to the users of the service (businesses or individuals). These clouds are known as public clouds; both the infrastructure and control of these clouds is with the service provider.

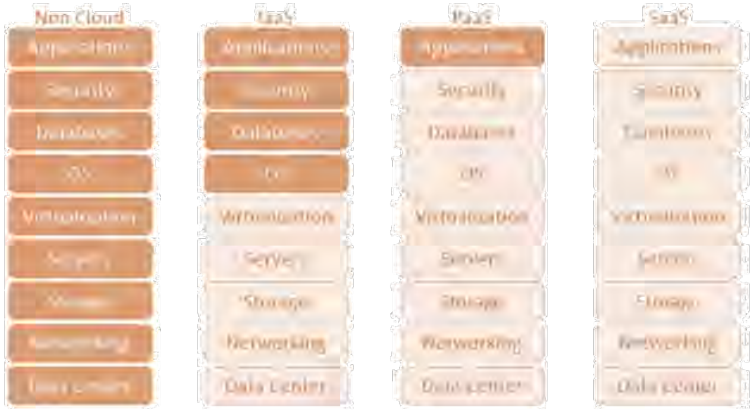
A variation on this scenario is the private cloud. Here, the cloud provider is responsible only for the infrastructure and not for the control. This setup is equivalent to a section of a shared data centre being partitioned for the sole use by a specific customer. Note that the private cloud can offer SaaS, PaaS, or IaaS services, though IaaS might appear to be a more natural fit.

Hybrid Cloud - A hybrid cloud is any combination of dedicated data centre services, public cloud services or private cloud services where one or several touch points exist between the environments. The goal is to combine services and data from a variety of computing models to create a unified, automated, and well-managed computing environment.

Hybrid solutions can be particularly useful in managing data and analytic services, largely due to the ability to scale capacity to demand for computing and storage resources, while collecting time series data from corporate and operational systems. Hybrid cloud solutions can provide considerable business value however they require careful planning and management to be effective.

9.1.3 Cloud Computing Service Types

If you look at the image below, the dark blue colors are what we are responsible for. The light blue color is what the cloud provider is responsible for.



Infrastructure as a Service (IaaS) - IaaS is a cloud computing offering in which a vendor provides users access to computing resources such as servers, storage, and networking. Organizations use their own platforms and applications within a service provider's infrastructure. Key features:

- Instead of purchasing hardware outright, users pay for IaaS on demand.
- Infrastructure is scalable depending on processing and storage needs.
- Saves enterprises the costs of buying and maintaining their own hardware.
- Because data is on the cloud, there is no single point of failure.
- Enables the virtualization of administrative tasks, freeing up time for other work.

Platform as a service (PaaS) - PaaS is a cloud computing offering that provides users a cloud environment in which they can develop, manage, and deliver applications. In addition to storage and other computing resources, users can use a suite of prebuilt tools to develop, customize and test their own applications. Key features:

- PaaS provides a platform with tools to test, develop, and host applications in the same environment.
- Enables organisations to focus on development without having to worry about underlying infrastructure.
- Providers manage security, operating systems, server software, and backups.
- Facilitates collaborative work even if teams work remotely.

Software as a Service (SaaS) - SaaS is a cloud computing offering that provides users with access to a vendor's cloud-based software. Users do not install applications on their local devices. Instead, the applications reside on a remote cloud network accessed through the web or an API. Through the application, users can store and analyse data and collaborate on projects.

Key features:

- SaaS vendors provide users with software and applications on a subscription model.
- Users do not have to manage, install, or upgrade software; SaaS providers manage this.
- Data is secure in the cloud; equipment failure does not result in loss of data.
- Use of resources can be scaled depending on service needs.
- Applications are accessible from almost any Internet-connected device, from virtually anywhere in the world. A variation of SaaS is Business Process as a Service (BPaaS). This is a form of Business Process Outsourcing (BPO) which leverages cloud computing services to delivery entire, cohesive business processes – such as payroll, HR, and customer care whereby the provider provides not just the application systems and infrastructure, but also the human expertise and labour. Along with the aim of "traditional" BPO to reduce labour costs, BPaaS provides the additional economies and efficiency of the cloud computing model.

3.3 WHISTLEBLOWERS QUARTERLY REPORT - DECEMBER 2023

File Number:

Report Author: Group Manager Support

Report Authoriser: Chief Executive

Appendices: 1. PwC Whistleblowers report - December 2023

1. REPORT PURPOSE

1.1. To provide the committee with an update on the whistleblowing report for the quarter ended 31 December 2023.

2. OFFICER RECOMMENDATION

That the Risk and Assurance Sub-Committee Meeting receive the report.

3. BACKGROUND

3.1. PwC has been engaged with the Whistleblowing duties of the Grey District Council, Buller District Council, Westland District Council and West Coast Regional Council on a combined approach.

3.2. The report for the quarter ended 31 December 2023 has been attached to appendix 1.

4. OPTIONS

4.1. That the Risk and Assurance Sub-Committee Meeting receive the report.

5. CONSIDERATIONS

5.1. Legal and Legislative Implications

5.1.1. None

5.2. Financial

5.2.1. None

5.3. Existing Policy and Strategy Implications

5.3.1. None

5.4. Fit with Purpose of Local Government Statement

5.4.1. None

5.5. Effects on Manawhenua

5.5.1. None

5.6. Significance and Engagement

Issue	Level of Significance	Explanation of Assessment
Is there a high level of public interest, or is decision likely to be controversial?	N/A	N/A
Is there a significant impact arising from duration of the effects from the decision?	N/A	N/A
Does the decision relate to a strategic asset? (refer Significance and Engagement Policy for list of strategic assets)	N/A	N/A
Does the decision create a substantial change in the level of service provided by Council?	N/A	N/A
Does the proposal, activity or decision substantially affect debt, rates or Council finances in any one year or more of the LTP?	N/A	N/A
Does the decision involve the sale of a substantial proportion or controlling interest in a CCO or CCTO?	N/A	N/A
Does the proposal or decision involve entry into a private sector partnership or contract to carry out the deliver on any Council group of activities?	N/A	N/A
Does the proposal or decision involve Council exiting from or entering into a group of activities?	N/A	N/A

5.7. Community Wellbeings and Outcomes

5.7.1. N/A

5.8. Other

5.8.1. N/A

6. CONCLUSIONS

6.1. That the Risk and Assurance Sub-Committee Meeting receive the report.

Confirmation of Statutory Compliance

Compliance with Statutory Decision-making Requirements (ss 76 - 81 Local Government Act 2002).

(a) This report contains:

(i) sufficient information about all reasonably practicable options identified and assessed in terms of their advantages and disadvantages; and

(ii) adequate consideration of the views and preferences of affected and interested persons bearing in mind any proposed or previous community engagement.

(b) The information reflects the level of significance of the matters covered by the report, as determined in accordance with the Council's significance and engagement policy.

Grey District Council

Quarterly Report on Whistleblower Services provided by PwC

1 October 2023 to 31 December 2023

pwc

Strictly private and confidential

Whistleblower line details:

PwC Disclosure Service –	**West Coast Regional Council** **Grey District Council** **Westland District Council**
Confidential free phone line	***0800 177 PWC or 0800 177 792***
Confidential email address	***pwcdisclose@pwc.com***

PwC Contacts:

Stephen Drain, Partner, Forensic Services, Auckland
Mobile: +64 21 1962 500
Email: stephen.c.drain@pwc.com

Philip Riley, Director, Forensic Services, Wellington
Mobile: +64 22 366 3314
Email: philip.r.riley@pwc.com

Miro Bilinski, Associate Director, Forensic Services, Auckland
Mobile: +64 21 892 914
Email: miro.j.bilinski@pwc.com

West Coast Local Authorities Contacts:

Darryl Lew, Chief Executive ***(Primary, West Coast Regional Council)***
DDI: +64 3 769 9096
Mobile: 027 217 9306
Email: darryl.lew@wcrc.govt.nz
Mail: PO Box 66, Greymouth, 7840

WCRC Finance ***(Quarterly Reporting Only, West Coast Regional Council)***
c/o Chantel Mills, Financial Consultant
DDI +64 3 768 0466 ext. 9072
Email: finance@wcrc.govt.nz

Gerhard Roux, Group Manager ***(Primary, Grey District Council)***
DDI: TBC
Mobile: TBC
Email: gerhard.roux@greydc.govt.nz
Mail: PO Box 382, Greymouth 7840

Lesley Crichton, Group Manager: Corporate Services ***(Primary, Westland District Council)***
DDI: +64 3 756 9081
Mobile: +64 27 531 3782
Email: lesley.crichton@westlanddc.govt.nz
Mail: Private Bag 704, Hokitika 7842

Simon Bastion ***(Backup, Westland District Council)***
DDI: 03 756 9033
Mobile: 027 838 5268
Email: simon.bastion@westlanddc.govt.nz
Mail: Private Bag 704, Hokitika 7842

Quarterly Reporting Distribution List:

West Coast Regional Council	Darryl Lew and WCRC Finance
Grey District Council	Gerhard Roux
Westland District Council	Lesley Crichton

Report on contact to the service during the quarter ended December 2023:

No call or contact was made to the whistleblower service during the quarter ended December 2023.

Other matters of interest:

We received one hang up/wrong number call(s) on the PwC Disclose service that could be specifically attributed to Grey District Council, and a further one hang up/wrong number call(s) on the overall PwC Disclose service that could not be attributed to any specific PwC Disclose subscriber during the quarter ended December 2023.

Procedure Note updated on 6 December 2023.

Individuals charged for 'pig butchering' cryptocurrency scheme

On 14 December 2023 the U.S. Department of Justice announced that they have charged four individuals for their alleged role in a fraudulent 'pig butchering' cryptocurrency (crypto) scheme.

'Pig butchering' scams involve fraudsters initiating a relationship with members of the public online, gaining their trust, and then convincing the victim to make financial investments into fictitious cryptocurrency schemes. The scams are run by criminal organisations out of Southeast Asia, and use victims of labour trafficking to contact victims around the world.

In this case, the funds were funnelled through shell companies to domestic and international bank accounts. The scheme resulted in victim losses of over US$80 million, and the seizure of digital currency worth approximately US$500 million. The individuals were charged with conspiracy to commit money laundering, concealment money laundering, and international money laundering.

With the emerging use of cryptocurrency within organised crime, 'pig butchering' scams have become a multibillion-dollar global industry. Detective Inspector Geoff Donoghue of the London Metropolitan Police Crypto Investigation Team said that "cryptocurrencies give a new dimension to the settlement of value transfer… everywhere that we have looked, we have found [crypto]".

The increase in 'pig butchering schemes' schemes, has seen cryptocurrency's role within organised crime labelled as "endemic". This threat is expected to grow here in New Zealand, as the rise of cryptocurrency scams poses additional risks to consumers, investors and financial systems.

Sources:

https://www.justice.gov/opa/pr/four-individuals-charged-laundering-millions-cryptocurrency-investment-scams

https://www.ft.com/content/378a05ac-a12b-41f9-a80c-fc79a36bc44b

3.4 UPDATE FROM MINISTER FOR LOCAL GOVERNMENT

File Number:

Report Author: Group Manager Support

Report Authoriser: Chief Executive

Appendices: 1. Correspondence Department of Internal Affairs

1. REPORT PURPOSE

To enable discussion to be placed around the option presented to Council about delivery of the Long Term Plan (LTP).

2. OFFICER RECOMMENDATION

That the Risk and Assurance Sub-Committee Meeting

1. Receive the report.
2. Recommend to Council that it supports the proposal to delay the Long Term Plan until 2025 – 26 year and produce an Annual Plan for the 2024 – 25 financial year.

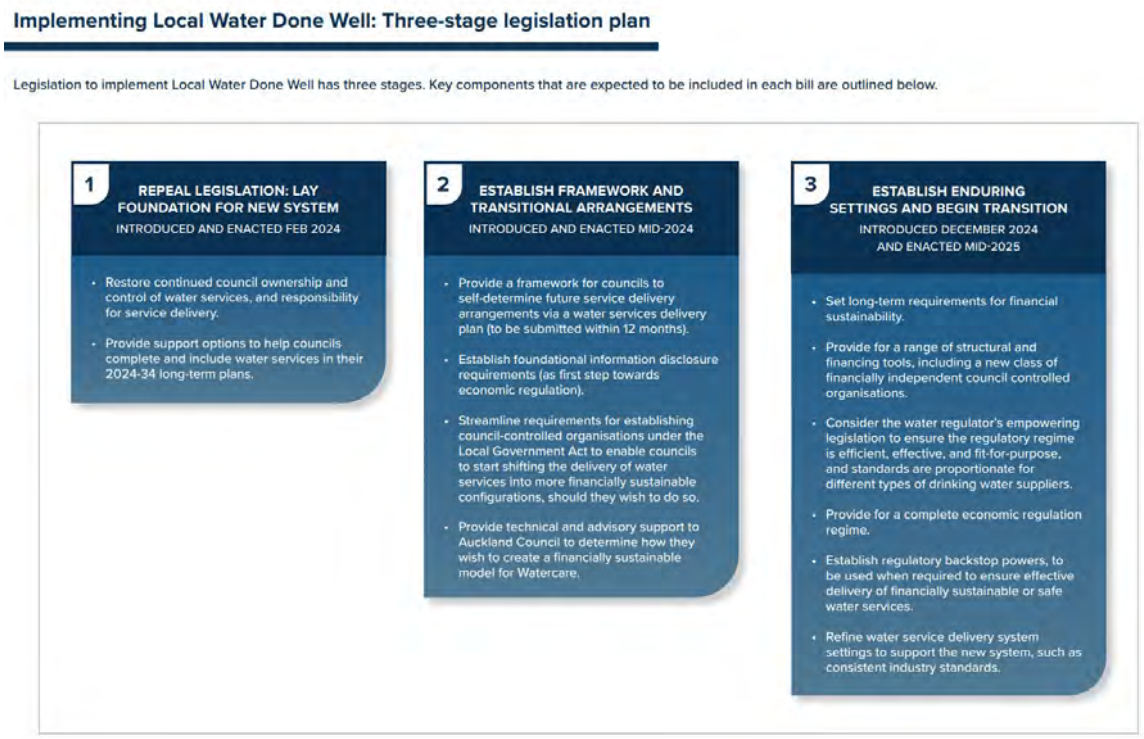
3. BACKGROUND

3.1. Update from the Minister for Local Government.

The Prime Minister and Minister of Local Government provided an update on progress and outlined the plan for the next 12-18 months to implement Local Water Done Well.

3.2. The Government will pass a bill that will repeal the previous Government's water services legislation by 23 February 2024. Further legislation to implement Local Water Done Well will progress in a two-stage approach. The first bill, which will establish the framework and transitional arrangements for the new water services system, will be passed by the middle of 2024. A second bill to provide for the long-term replacement of regime will be introduced in December 2024.

3.3. Below is a copy of the legislation plan here for your information, showing the different components expected to be included in each bill.



3.4. The Minister also announced the establishment of a Technical Advisory Group to provide expert advice to the Department and the Minister on the implementation of Local Water Done Well.

You can find out more about the Technical Advisory Group on the DIA website:

https://www.dia.govt.nz/Water-Services-Policy-and-Legislation

The Minister's press release is available on the Beehive website here:

https://www.beehive.govt.nz/release/government-advances-local-water-done-well

3.5. **An additional option that will enable councils to defer their 2024-34 long-term plan by 12 months**

In December 2023 the Minister communicated directly with mayors and council chief executives regarding options that will be available in the bill to assist councils to include water services in their 2024-34 long-term plans.

In addition, the bill will provide a further option that will enable councils to defer their 2024-34 long-term plan by 12 months, and to prepare an 'enhanced' annual plan for the 2024/25 financial year instead.

If a council chooses this option, it will be required to include additional information (about groups of activities and capital expenditure) in the 2024/25 annual plan, and to consult on that plan.

A council will be able to exercise this option by resolution by 30 April 2024, or if authorised to do so by an Order in Council, after that date.

Transitional provisions that enable councils to defer the review of water services bylaws

The bill will also include transitional provisions that enable councils to defer the review of water services bylaws (similar to the approach previously provided through the water services legislation).

The bill allows councils to defer a review, if that review would ordinarily be required between 15 December 2022 and the end of 2025. If there is a deferral, the review would need to be completed by 1 July 2026 at the latest.

Confirmation of Statutory Compliance

Compliance with Statutory Decision-making Requirements (ss 76 - 81 Local Government Act 2002).

(a) This report contains:

(i) sufficient information about all reasonably practicable options identified and assessed in terms of their advantages and disadvantages; and

(ii) adequate consideration of the views and preferences of affected and interested persons bearing in mind any proposed or previous community engagement.

(b) The information reflects the level of significance of the matters covered by the report, as determined in accordance with the Council's significance and engagement policy.

Implementing Local Water Done Well: Three-stage legislation plan

Legislation to implement Local Water Done Well has three stages. Key components that are expected to be included in each bill are outlined below.

1 REPEAL LEGISLATION: LAY FOUNDATION FOR NEW SYSTEM

INTRODUCED AND ENACTED FEB 2024

- Restore continued council ownership and control of water services, and responsibility for service delivery.
- Provide support options to help councils complete and include water services in their 2024-34 long-term plans.

2 ESTABLISH FRAMEWORK AND TRANSITIONAL ARRANGEMENTS

INTRODUCED AND ENACTED MID-2024

- Provide a framework for councils to self-determine future service delivery arrangements via a water services delivery plan (to be submitted within 12 months).
- Establish foundational information disclosure requirements (as first step towards economic regulation).
- Streamline requirements for establishing council-controlled organisations under the Local Government Act to enable councils to start shifting the delivery of water services into more financially sustainable configurations, should they wish to do so.
- Provide technical and advisory support to Auckland Council to determine how they wish to create a financially sustainable model for Watercare.

3 ESTABLISH ENDURING SETTINGS AND BEGIN TRANSITION

INTRODUCED DECEMBER 2024 AND ENACTED MID-2025

- Set long-term requirements for financial sustainability.
- Provide for a range of structural and financing tools, including a new class of financially independent council controlled organisations.
- Consider the water regulator's empowering legislation to ensure the regulatory regime is efficient, effective, and fit-for-purpose, and standards are proportionate for different types of drinking water suppliers.
- Provide for a complete economic regulation regime.
- Establish regulatory backstop powers, to be used when required to ensure effective delivery of financially sustainable or safe water services.
- Refine water service delivery system settings to support the new system, such as consistent industry standards.

Note: All timeframes are subject to parliamentary processes and timelines.

4 IN COMMITTEE ITEMS

COUNCIL IN-COMMITTEE

That the public is excluded from:

The following parts of the proceedings of this meeting

Agenda item(s) 4.1 – 4.8

The general subject of each matter to be considered while the public is excluded, the reason for passing this resolution in relation to each matter, and the specific grounds under section 48(1) of the Local Government Official Information and Meetings Act 1987 for the passing of this resolution are as follows:

OFFICER RECOMMENDATION

General subject of each matter to be considered	Reason for passing this resolution in relation to each matter	Ground(s) under section 48(1) for the passing of this resolution
4.1 - CONFIRMATION OF IN COMMITTEE MINUTES OF RISK AND ASSURANCE SUB-COMMITTEE MEETING HELD ON 24 OCTOBER 2023	s7(2)(c)(ii) - the withholding of the information is necessary to protect information which is subject to an obligation of confidence or which any person has been or could be compelled to provide under the authority of any enactment, where the making available of the information would be likely otherwise to damage the public interest	s48(1)(a)(i) - the public conduct of the relevant part of the proceedings of the meeting would be likely to result in the disclosure of information for which good reason for withholding would exist under section 6 or section 7
4.2 - LONG TERM PLAN 2024-2034 RISK REGISTER	s7(2)(j) - the withholding of the information is necessary to prevent the disclosure or use of official information for improper gain or improper advantage	s48(1)(a)(i) - the public conduct of the relevant part of the proceedings of the meeting would be likely to result in the disclosure of information for which good reason for withholding would exist under section 6 or section 7
4.3 - HEALTH AND SAFETY REPORT	s7(2)(d) - the withholding of the information is necessary to avoid prejudice to measures protecting the health or safety of members of the public	s48(1)(a)(i) - the public conduct of the relevant part of the proceedings of the meeting would be likely to result in the disclosure of information for which good reason for withholding would exist under section 6 or section 7

4.4 - ICT AND CYBERSECURITY IMPLEMENTATION PLAN ON AUDITS PERFORMED	s7(2)(j) - the withholding of the information is necessary to prevent the disclosure or use of official information for improper gain or improper advantage	s48(1)(a)(i) - the public conduct of the relevant part of the proceedings of the meeting would be likely to result in the disclosure of information for which good reason for withholding would exist under section 6 or section 7
4.5 - STRATEGIC PRIORITIES UPDATE	s7(2)(a) - the withholding of the information is necessary to protect the privacy of natural persons, including that of deceased natural persons	s48(1)(a)(i) - the public conduct of the relevant part of the proceedings of the meeting would be likely to result in the disclosure of information for which good reason for withholding would exist under section 6 or section 7
4.6 - SENSITIVE EXPENDITURE REPORT - DECEMBER 2023	s7(2)(b)(ii) - the withholding of the information is necessary to protect information where the making available of the information would be likely unreasonably to prejudice the commercial position of the person who supplied or who is the subject of the information	s48(1)(a)(i) - the public conduct of the relevant part of the proceedings of the meeting would be likely to result in the disclosure of information for which good reason for withholding would exist under section 6 or section 7
4.7 - REPORT ON AUDIT RECOMMENDATIONS FROM MANAGEMENT LETTER	s7(2)(g) - the withholding of the information is necessary to maintain legal professional privilege	s48(1)(a)(i) - the public conduct of the relevant part of the proceedings of the meeting would be likely to result in the disclosure of information for which good reason for withholding would exist under section 6 or section 7
4.8 - INSURANCE RENEWAL	s7(2)(b)(ii) - the withholding of the information is necessary to protect information where the making available of the information would be likely unreasonably to prejudice the commercial position of the person who supplied or who is the subject of the information	s48(1)(a)(i) - the public conduct of the relevant part of the proceedings of the meeting would be likely to result in the disclosure of information for which good reason for withholding would exist under section 6 or section 7

5 SUB-COMMITTEE RESUME IN OPEN MEETING

CLOSURE OR RATIFICATION OF DECISIONS IN OPEN MEETING