CENTRAL OTAGO
DISTRICT COUNCIL

AGENDA

Audit and Risk Committee Meeting
Friday, 3 June 2022

Date:	**Friday, 3 June 2022**
Time:	**9.30 am**
Location:	**Ngā Hau e Whā, William Fraser Building, 1 Dunorling Street, Alexandra**

(Due to COVID-19 restrictions and limitations of the physical space, public access will be available through a live stream of the meeting.

The link to the live stream will be available on the Central Otago District Council's website.)

Sanchia Jacobs

Chief Executive Officer

Notice is hereby given that an Audit and Risk Committee meeting will be held in Ngā Hau e Whā, William Fraser Building, 1 Dunorling Street, Alexandra and live streamed via Microsoft Teams on Friday, 3 June 2022 at 9.30 am. The link to the live stream will be available on the Central Otago District Council's website.

Order Of Business

Members Ms L Robertson (Chair), His Worship the Mayor T Cadogan, Cr N Gillespie, Cr S Jeffery, Cr N McKinlay

In Attendance S Jacobs (Chief Executive Officer), L Macdonald (Executive Manager - Corporate Services), J Muir (Executive Manager - Infrastructure Services), L van der Voort (Executive Manager - Planning and Environment), S Righarts (Chief Advisor), W McEnteer (Governance Manager)

1 APOLOGIES

2 PUBLIC FORUM

3 CONFIRMATION OF MINUTES

Audit and Risk Committee meeting - 25 February 2022

MINUTES OF CENTRAL OTAGO DISTRICT COUNCIL AUDIT AND RISK COMMITTEE HELD VIA MICROSOFT TEAMS AND LIVE STREAMED ON FRIDAY, 25 FEBRUARY 2022 AT 9.34 AM

PRESENT: Ms L Robertson (Chair), Cr S Jeffery, Cr N McKinlay

IN ATTENDANCE: Cr C Laws, L Macdonald (Executive Manager - Corporate Services), J Muir (Executive Manager - Infrastructure Services), L van der Voort (Executive Manager - Planning and Environment), L Fleck (Executive Manager – People and Culture), S Righarts (Chief Advisor), N McLeod (IS Manager), I Evans (Water Services Manager), A McDowall (Finance Manager), A Crosbie (Senior Policy Advisor), P Bain (Water Services Team Leader), R Williams (Governance Manager) and W McEnteer (Governance Support Officer)

1 APOLOGIES

COMMITTEE RESOLUTION

Moved: **Robertson**
Seconded: **Jeffery**

That apologies from His Worship the Mayor T Cadogan and Cr N Gillespie be received and accepted.

CARRIED

2 PUBLIC FORUM

There was no public forum.

3 CONFIRMATION OF MINUTES

COMMITTEE RESOLUTION

Moved: **Robertson**
Seconded: **Jeffery**

That the public minutes of the Audit and Risk Committee Meeting held on 3 December 2021 be confirmed as a true and correct record.

CARRIED

4 DECLARATION OF INTEREST

Members were reminded of their obligations in respect of declaring any interests. There were no further declarations of interest.

5 REPORTS

22.1.2 POLICY AND STRATEGY REGISTER

To consider the updated Policy and Strategy Register. A question was raised about the Staff Interests Policy and whether or not current practise reflected the policy or not in terms of the Executive Team considering staff interests on a six monthly basis. An update on this was requested for the June meeting.

COMMITTEE RESOLUTION

Moved: Robertson
Seconded: Jeffery

That the report be received.

CARRIED

22.1.3 AUDIT AND RISK COMMITTEE TERMS OF REFERENCE

To consider the terms of reference for the Audit and Risk Committee.

After discussion it was agreed that there should be two further amendments before the document was presented to Council. The first was to delete reference to the Deputy Chair as the position did not exist. The second was regarding the appointment cycle of the Chair, where an additional clarification was to be included to say that the Chair was appointed “each triennium following the year of election or as required.”

COMMITTEE RESOLUTION

Moved: Robertson
Seconded: Jeffery

That the Audit and Risk Committee

A. Receives the report and accepts the level of significance.

B. Recommends to Council that they accept the proposed amendments to the Audit and Risk Committee’s terms of reference as detailed in appendix 2 of the report.

C. Recommends to Council that the reference to the Deputy Chair is removed from the delegation and that the term of the appointment of the Chair is clarified to include the words “each triennium following the year of election or as required.”

CARRIED

22.1.4 EXTERNAL AND INTERNAL AUDIT UPDATES

To consider an update on the status of the external and internal audit programme and any outstanding actions for completed external and internal audits.

COMMITTEE RESOLUTION

Moved: Robertson
Seconded: Jeffery

That the report be received.

CARRIED

22.1.5 FINANCIAL REPORT FOR THE PERIOD ENDING 31 DECEMBER 2021

To consider the financial performance for the period ending 31 December 2021.

COMMITTEE RESOLUTION

Moved: Robertson
Seconded: Jeffery

That the report be received.

CARRIED

22.1.6 CYBER SECURITY PLAN 2018-2021 UPDATE

To consider an update on the 2018-2021 Cyber Security Plan.

COMMITTEE RESOLUTION

Moved: Robertson
Seconded: Jeffery

That the report be received.

CARRIED

22.1.7 LOCAL GOVERNMENT OFFICIAL INFORMATION AND MEETINGS ACT 1987 (LGOIMA) REQUEST POLICY

To review and recommend the Chief Executive approves the Local Government Official Information and Meetings Act 1987 (LGOIMA) Request Policy, which is related to Council granting requests for information under the Local Government Official Information and Meetings Act 1987.

After discussion it was decided that the Committee should not recommend Chief Executive approval, rather they could support it.

COMMITTEE RESOLUTION

Moved: Robertson
Seconded: Jeffery

That the Audit and Risk Committee

A. Receives the report and accepts the level of significance.

B. Supports the Chief Executive approval of this policy and issues to staff for implementation.

CARRIED

22.1.8 PRIVACY POLICY

To review and recommend the Chief Executive approves the Privacy Policy for council staff use, which is related to Council's code of practice and legal obligations in accordance with the Privacy Act 2020.

The Committee asked if the scope of the policy included the Council's obligations as an employer and it was agreed that the scope of the policy should be expanded to include this prior to final sign off.

It was also decided that the Committee should support the Chief Executive's approval of the policy rather than recommend it.

COMMITTEE RESOLUTION

Moved: Robertson
Seconded: Jeffery

That the Audit and Risk Committee

A. Receives the report and accepts the level of significance.

B. Supports the Chief Executive approval of the policy and suggests its scope is expanded to include internal privacy relating to staff prior to implementation.

CARRIED

22.1.9 HEALTH, SAFETY AND WELLBEING REPORT

To provide with information on health, safety and wellbeing risks and controls at Central Otago District Council.

COMMITTEE RESOLUTION

Moved: Robertson
Seconded: Jeffery

That the report be received.

CARRIED

6 CHAIR'S REPORT

22.1.10 FEBRUARY 2022 CHAIR'S REPORT

To consider the February Chair's report.

The Chair had nothing to report.

7 MEMBERS' REPORTS

22.1.11 FEBRUARY MEMBERS' REPORTS

To consider the February members' reports.

Councillor McKinlay reported that he was a member of subcommittee overseeing the Cromwell Hall project and noted that a timetable for the project was currently being put in place.

COMMITTEE RESOLUTION

Moved: **Robertson**
Seconded: **Jeffery**

That the reports be received.

CARRIED

8 STATUS REPORTS

22.1.12 FEBRUARY GOVERNANCE REPORT

To report on items of general interest, consider the Audit and Risk Committee's forward work programme and the current status report updates.

COMMITTEE RESOLUTION

Moved: **Robertson**
Seconded: **Jeffery**

That the report be received.

CARRIED

9 DATE OF THE NEXT MEETING

The date of the next scheduled meeting is 3 June 2022.

10 RESOLUTION TO EXCLUDE THE PUBLIC

COMMITTEE RESOLUTION

Moved: **Robertson**
Seconded: **Jeffery**

That the public be excluded from the following parts of the proceedings of this meeting.

The general subject matter 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 of the Local Government Official Information and Meetings Act 1987 for the passing of this resolution are as follows:

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
Confidential Minutes of the Audit and Risk Committee	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)(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 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 s7(2)(g) - the withholding of the information is necessary to maintain legal professional privilege s7(2)(i) - the withholding of the information is necessary to enable Council to carry on, without prejudice or disadvantage, negotiations (including commercial and industrial negotiations)	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
22.1.13 - Wastewater Overflow Procedure review	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
22.1.14 - Water Services Capital Projects Update	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)(i) - the withholding of the information is necessary to enable Council to carry on, without prejudice or disadvantage, negotiations	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

	(including commercial and industrial negotiations)	
22.1.15 - Strategic Risk Register	s7(2)(i) - the withholding of the information is necessary to enable Council to carry on, without prejudice or disadvantage, negotiations (including commercial and industrial negotiations)	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
22.1.16 - Litigation Register	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
22.1.17 - February 2022 Confidential Governance Report	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 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

CARRIED

The public were excluded at 10.33 am and the meeting closed at 11:37 am.

4 DECLARATION OF INTEREST

22.2.1 DECLARATIONS OF INTEREST REGISTER

Doc ID: 582671

1. Purpose

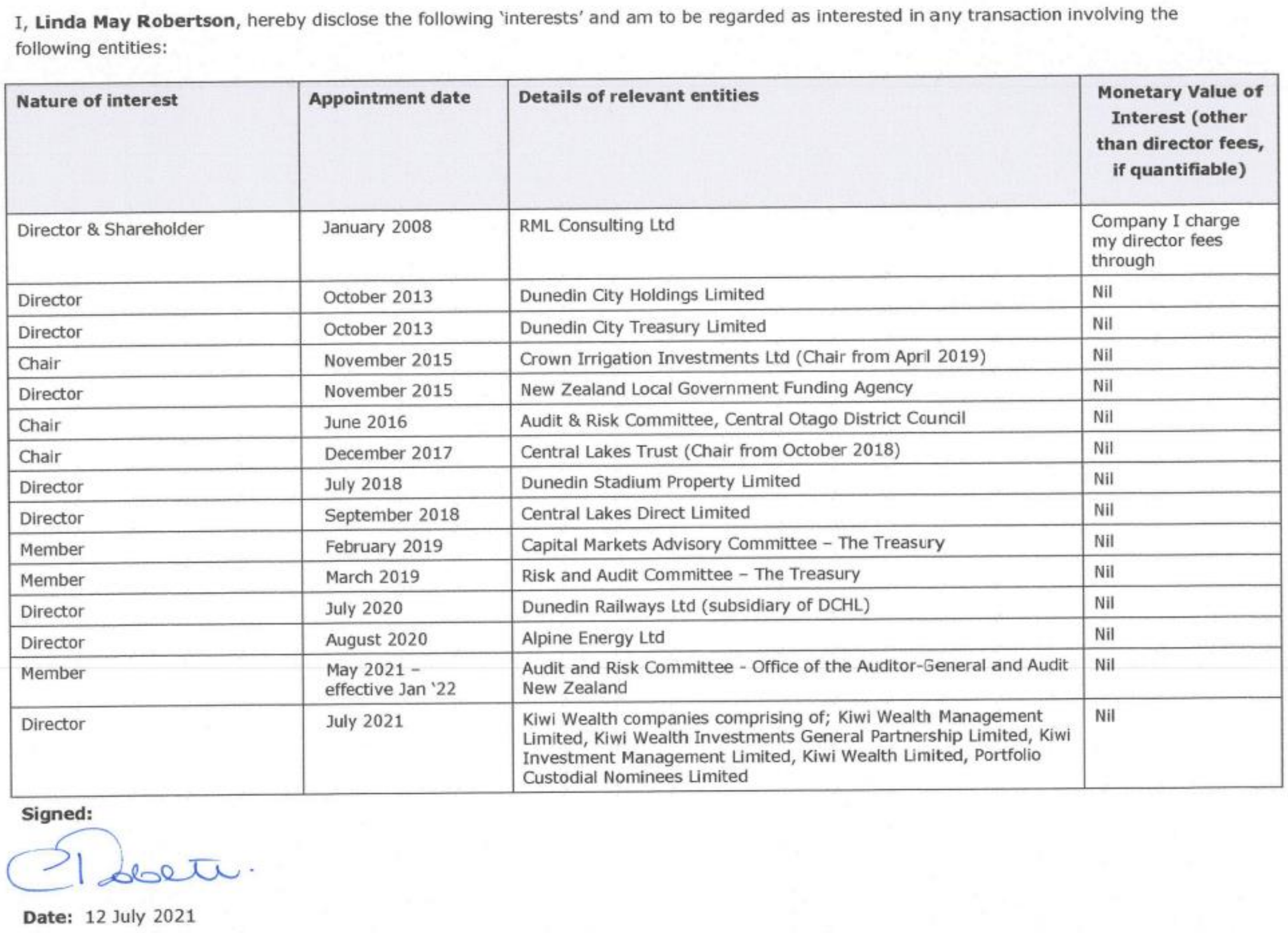
Members are reminded of the need to be vigilant to stand aside from decision making when a conflict arises between their role as a member and any private or other external interest they might have.

2. Attachments

Appendix 1 - Audit and Risk Declarations of Interest ⇩

Name	Member's Declared Interests	Spouse/Partner's Declared Interests	Council Appointments
Tim Cadogan	Business South Central Otago Advisory Group (member) Alexandra Squash Club (member)	Two Paddocks (employee)	Airport Reference Group Maniototo Curling International Inc Eden Hore Steering Group Tourism Central Otago Advisory Board Ministerial Working Group on Responsible Camping Ministerial Working Group on representation, governance and accountability of new water entities (member)
Neil Gillespie	Contact Energy (Specialist - Community Relations and Environment) Clyde & Districts Emergency Rescue Trust (Secretary and Trustee) Cromwell Volunteer Fire Brigade (Chief Fire Officer) Cromwell Bowling Club (patron) Otago Local Advisory Committee - Fire Emergency New Zealand Returned Services Association (Member)		Lowburn Hall Committee Tarras Community Plan Group Tarras Hall Committee

Stephen Jeffery	G & S Smith family Trust (Trustee) K & EM Bennett's family Trust (Trustee) Roxburgh Gorge Trail Charitable Trust (Chair) Roxburgh and District Medical Services Trust (Trustee) Central Otago Clutha Trails Ltd (Director) Teviot Prospects (Trustee) Teviot Valley Community Development Scheme Governance Group Central Otago Queenstown Network Trust		
Nigel McKinlay	Transition To Work Trust (Board member) Gate 22 Vineyard Ltd (Director) Everyday Gourmet (Director) Central Otago Wine Association (member) Long Gully Irrigation Scheme (member)		



I, **Linda May Robertson**, hereby disclose the following 'interests' and am to be regarded as interested in any transaction involving the following entities:

Nature of interest	Appointment date	Details of relevant entities	Monetary Value of Interest (other than director fees, if quantifiable)
Director & Shareholder	January 2008	RML Consulting Ltd	Company I charge my director fees through
Director	October 2013	Dunedin City Holdings Limited	Nil
Director	October 2013	Dunedin City Treasury Limited	Nil
Chair	November 2015	Crown Irrigation Investments Ltd (Chair from April 2019)	Nil
Director	November 2015	New Zealand Local Government Funding Agency	Nil
Chair	June 2016	Audit & Risk Committee, Central Otago District Council	Nil
Chair	December 2017	Central Lakes Trust (Chair from October 2018)	Nil
Director	July 2018	Dunedin Stadium Property Limited	Nil
Director	September 2018	Central Lakes Direct Limited	Nil
Member	February 2019	Capital Markets Advisory Committee – The Treasury	Nil
Member	March 2019	Risk and Audit Committee – The Treasury	Nil
Director	July 2020	Dunedin Railways Ltd (subsidiary of DCHL)	Nil
Director	August 2020	Alpine Energy Ltd	Nil
Member	May 2021 – effective Jan '22	Audit and Risk Committee - Office of the Auditor-General and Audit New Zealand	Nil
Director	July 2021	Kiwi Wealth companies comprising of; Kiwi Wealth Management Limited, Kiwi Wealth Investments General Partnership Limited, Kiwi Investment Management Limited, Kiwi Wealth Limited, Portfolio Custodial Nominees Limited	Nil

Signed:

Date: 12 July 2021

5 REPORTS

22.2.2 POLICY AND STRATEGY REGISTER

Doc ID: 580946

1. Purpose

To consider the updated Policy and Strategy Register.

Recommendations

That the report be received.

2. Discussion

The following updates were made to the register:

People and Culture

- Violence and Aggression Management Policy has been added as new work item

Regulatory

- Dangerous and Insanitary Building Policy was adopted at the March Council meeting
- Easter Sunday Trading Policy was readopted for a further five-year period at the June Council meeting

Information Management

- Acceptable Use of Public WiFi Policy review is underway
- Digital Strategy is on track for finalisation in June 2022
- Privacy Policy implemented following approval, subject to amendments, at the February Audit and Risk Committee meeting
- LGOIMA Policy implemented following approval, subject to amendments, at the February Audit and Risk Committee meeting

Libraries

- Review of five library policies underway, proposed to be replaced with one new library policy in quarter three of 2021/22

General

- An element of the Housing Strategy is currently out for public feedback. Timeframe has been adjusted accordingly.

3. Attachments

Appendix 1 - Policy and Strategy Register ⇩

Report author:	Reviewed and authorised by:
Alix Crosbie Senior Strategy Advisor 13/05/2022	Saskia Righarts Chief Advisor 17/05/2022

Name	Date Issued / Review Beginning	Due for Review / Completion	Responsibility
People and Culture			
Equal Employment Opportunity (EEO), Discrimination, Harassment and Bullying Policy	September 2021	September 2023	CEO
Performance Management Policy	August 2021	August 2023	CEO
Staff Interests Policy	December-2021	December-2023	AR > CEO
Working From Home Guidelines	August-2020	August-2023	CEO
Respect at Work Guidelines	February-2020	February-2022	CEO
Leave Management Policy	December-2020	December-2023	CEO
Vehicle User Policy	February-2020	February-2023	CEO
Future Work Items			
Drug and Alcohol Policy		2022 (second quarter)	CEO
Child Protection and Safeguarding Policy		Q1 2024	CEO
Violence and Aggression Management Policy		2022	CEO
Information Services			
Acceptable Use of Public Wi-Fi Policy	March-2019	June-2022	Council
Copyright Policy	September 2021	September-2024	CEO
Cyber Security Policy	August 2021	August 2024	AR > Council
Information and Records Management Policy	February 2022	February-2025	Council
Privacy Policy	February 2022	February-2025	AR > CEO
LGOIMA Policy	February 2022	February-2025	AR > CEO
Future Work Items			
Digital Strategy		June-2022	Council
CCTV Policy		Q2 2022	Council
Governance			
Appointment and Remuneration of Directors Policy	October-2019	October-2022	Council
Code of Conduct	October-2019	October-2022	Council
Delegations Register (incl. Audit and Risk Terms of Reference)	August-2020	October-2022	Council
Elected Members Allowances and Reimbursements Policy	October-2019	October-2022	Council
Standing Orders	October-2019	October-2022	Council
Parks and Property			
Outdoor Recreation Strategy	June-2012	June-2022	Council
Council-owned Earthquake-prone Buildings Policy	June-2020	June-2023	Council
Cemeteries Bylaw	November-2020	November-2025	Council
Community Leasing and Licensing Policy	February-2021	February-2024	Council
District Tree Policy	August-2020	February-2022	Council
Public Toilet Strategy	July-2008	March-2022	Council
11x Reserve Management Plans	Various	Various	Council
Smokefree and Vapefree Policy	September-2021	September-2024	Council
Future Work Items			
Playground Strategy		2022	Council
Reserve Management Plans		2022	Council
Reserve Naming Policy		2022	Council
Responsible Camping Strategy		Hold pending government policy decision	Council
Plaques and Memorials Policy		2022	Council
Regulatory			
Alcohol Restrictions in Public Places Bylaw	May-2019	May-2024	Council
Dangerous and Insanitary Building Policy	March-2022	March-2025	Council
Dog Control Bylaw	December-2020	December-2025	Council
Dog Control Policy	December-2020	December-2025	Council
Easter Sunday Trading Policy	July-2018	June-2027	Council
Gambling and Board Venue Policy	June-2020	June-2023	Council
Lighting Policy	March-2019	Q4-2022	Council
Litter Offences	July-2019	July-2022	Council
Psychoactive Substances Policy	June-2019	June-2024	Council
Future Work Items			
Enforcement Strategy		2022	Council
Environmental Engineering			
Development and Financial Contributions Policy	June-2021	June-2024	Council
Subdivision Engineering Standards	September-2019	September-2024	Council
Sustainability Strategy	April-2019	April-2024	Council
Waste Management and Minimisation Plan	June-2018	June-2023	Council
Waste Management and Minimisation Bylaw	March 2021	March 2026	Council

Three Waters			
Leakage Remissions Policy*	June-2021	December-2023	Council
Sewer Lateral Policy	July-2016	December 2022	Council
Drinking Water Quality Policy Statement	March-2020	March-2023	Council
Trade Waste Bylaw	June-2001	To be replaced by Water Bylaw	Council
Water Supply Bylaw	May-2008	To be replaced by Water Bylaw	Council
Future Work Items			
Water Bylaw		December 2022	Council
Water Policy		December 2022	Council
Roading			
Roading Bylaw	November-2020	November-2025	Council
Roading Policy	January-2016	Q4-2022	Council
Speed Limit Bylaw	November-2007	June-2022	Council
Transportation Procurement Strategy	May-2020	May-2025	AR > Council
Libraries			
Cataloguing Policy	July-2018	March-2022	CEO
Collection Development Policy	October-2018	March-2022	CEO
Deselection Policy	March-2019	March-2022	CEO
Donations Policy	August-2018	March-2022	CEO
Interloans Policy	May-2020	May-2023	CEO
Lost Property Policy	May-2019	May-2022	CEO
Community and Engagement			
Arts Strategy	April-2013	April-2024	Community Owned
14x Community Plans	Various	Various	Community Owned
Grants Policy	June 2021	August-2022	Council
Heritage Strategy	April-2018	April-2023	Community Owned
Film Friendly Policy	June-2018	June-2023	Council
Media Policy	January-2020	January-2023	Council
Museum Strategy (Sector-led)	August 2020	August 2025	Community Owned
Significance and Engagement Policy*	June-2021	December 2023	AR > Council
Social Media Policy	January-2020	January-2023	Council
Community Development Strategy	March 2021	May 2023	Council
Future Work Items			
Wellbeing Strategy		Expected Completion: 2022	CEO
Communications and Engagement Strategy		Expected Completion: 2022	Council
Council lead Museum Investment Strategy		Expected Completion: 2022	Council
Finance			
Credit Card Policy	June 2021	June 2024	AR > CEO
Financial Reserves Policy	July 2021	June 2024	Council
Financial Strategy*	June-2021	December-2023	Council
Fixed Asset and Disposal Policy	June 2021	June 2024	AR > CEO
Fraud Bribery and Corruption Policy	October 2021	October-2022	AR > Council
Investment Policy*	June-2021	December-2023	AR > Council
Liability Management Policy*	June-2021	December-2023	AR > Council
Procurement Policy	August-2020	June 2022	AR > Council
Protected Disclosures (Whistleblowing) Policy	May-2020	June 2022	AR > Council
Rates Remission Policy*	June-2021	December-2023	AR > Council
Rating Policy*	June-2021	December-2023	AR > Council
Revenue and Financing Policy*	June-2021	December-2023	AR > Council
Risk Management Policy and Process	August-2020	June-2022	AR > Council
Sensitive Expenditure Policy	June 2021	June 2024	AR > Council
Staff Delegations Manual	June 2021	June 2024	AR > Council
Travel Policy	June 2021	June 2024	AR > Council
Vehicle Procurement Maintenance and Disposal Policy	Ocotber-2020	October-2023	CEO
Future Work Items			
Health, Safety and Wellbeing			
Health and Safety Policy Statement	September-2021	September-2022	CEO
Future Work Items			
Health and Safety Framework		Expected Completion: 2022	CEO
General			

Annual Plan/LTP	June-2021	June-2022	Council
Asset Management Policy	January-2022	January-2025	AR > Council
District Plan	April-2008	December-2022	Council
Economic Development Strategy	May-2019	May-2024	Council
Infrastructure Strategy*	June-2021	December-2023	AR > Council
Tourism Strategy	June-2019	June-2024	Council
Future Work Items			
Housing Strategy		Expected Completion: Q3 2022	Council

*Updated through Long-term plan process

22.2.3 AUDIT NZ AND INTERNAL AUDIT UPDATE

Doc ID: 581117

1. Purpose

To consider an update on the status of the external and internal audit programme and any outstanding actions for completed internal and external audits.

Recommendations

That the report be received.

2. Discussion

Council has a legislative requirement to complete external audits of annual reports and the long-term plan through Audit New Zealand. Audit New Zealand complete a governance report on their findings and any recommendations for improvements. A schedule of actions is then created and allocated to staff to manage the completion of these recommendations.

The 2019-2020 Audit New Zealand Management Report was presented to the Audit and Risk Committee at the June 2021 meeting. There were eight recommendations, of which all eight are now completed, with the last two updated in May 2022. The Audit Action Register contains two remaining actions which are pending Audit New Zealand signing off as part of the 2020-21 Management Report, with one completed in this quarter.

In addition to external audits, council carries out several internal audits annually to provide assurance over compliance and to mitigate business risks. One recommendation remained in progress in the payroll area. This is now completed as no further progress is able to be made in regard to the Ranfurly pool due to technology constraints.

Appendix 1 and 2 list the outstanding tasks and any progress with these tasks. Once the Committee have viewed the completed tasks these are removed from the schedule.

The internal audit programme is reviewed every three years to provide assurance over compliance and to mitigate business risks. In August 2020, Deloitte's recommended a four-year internal audit programme based on factors such as budgetary constraints, recently completed engagements and the current view of the risk landscape in the local government sector. This was then prioritised, and the Committee approved the programme of work as detailed below for the next four years (2021 – 2024) ending June 2024. This programme will be reviewed at the December 2022 Audit and Risk Committee meeting, post the Council elections. This is to ensure this programme reflects the appropriate priorities, and to consider whether the remining items in red should be included in the next three-year programme.

The proposed audits, in the information and records management, cyber security and procurement activities, are planned and scheduled to happen this financial year. All of these commence in June 2022.

Internal Audit Review Programme	FY 20-21	FY 21-22	FY 22-23	FY 23-24
Information and Records Management	x	✓		
Procurement		✓		
Cyber Security		✓		
Contract Management			✓	
Capital Expenditure Planning and Monitoring			✓	
Health & Safety				✓
Recruitment Review				✓
Environmental Management (including Sustainability)				
Business Continuity / Disaster Recovery				
Asset Management				
Benefits Realisation				
Legislative Compliance				

Red – denotes suggested alternative audit review options

3. Attachments

Appendix 1 - Audit New Zealand - Audit Action Register ⇩
Appendix 2 - Internal Audit Action Register ⇩

Report author:	Reviewed and authorised by:
	Sanchia Jacobs
Leanne Macdonald Executive Manager - Corporate Services 23/05/2022	Sanchia Jacobs Chief Executive Officer 23/05/2022

	Urgent	Necessary	Beneficial	Assigned	Estimated Completion	Status	Comments
udit NZ 2020 Management Report							
yments for hurt and humiliation (5.5) eview the policy regarding out of court settlements for hurt and humiliation and consider making voluntary disclosure to the IRD			✓	Executive Manager - People and Culture		Closed	No further feedback from Audit New Zealand
ird party acknowledgement of Council's security policies (5.8) roduce a formal process whereby third parties such as IT vendors or other non-staff knowledges that they have received and read these Security Policies and that they understand eir responsibilities to comply with those policies.			✓	Information Services Manager	May-22	Closed	Agreements are with the suppliers to be finalised.
udit NZ 2019 Management Report							
sset valuation recommendations and processes (4.1)							
Waters – the valuers noted that detailed component information for new plant projects mpleted since the previous valuation, have not been included in the plant asset register. stead, high level project costs have been used.				Executive Manager - Infrastructure Services		In progress	Plant data has been collected and is being valued this year by Council's insurance company
nual report preparation process (4.2)							
ouncil should introduce a robust internal quality review process over the draft annual report to prove the quality of the draft information provided for audit.		✓		Executive Manager - Corporate Services / Finance Manager		Closed	Preparation for the Annual Report has been completed for 2020-21. Audit NZ acknowledged an improvement in the process.
Control Environment							
strengthen the Council's overall IT control environment, we recommend the Council considers e following: formal IT strategic plan that supports the overall business strategic objectives usiness led IT governance group with clear terms of reference formal IT risk management process formal management reporting that provide the organisation with the level of service that IT ovides and insights as to value of its IT investments.			✓	Information's Services Manager		In progress	To strengthen the Council's overall IT control environment, we recommend the Council considers the following: • **A formal IT strategic plan that supports the overall business strategic objectives** Leadership Group workshop has occurred, draft strategy with Leadership Group for final feedback until end of May 2022, finalised June 2022. • **Business led IT governance group with clear terms of reference** A proposal for an Information Services (IS) Steering Committee has been drafted, this is yet to be presented to the Executive Manager for feedback. This forms part of the IS Activity Management Plan and IS Management & Governance Framework. This will be implemented following the Digital and Information Strategy being finalised. • **A formal IT risk management process** Information Services uses the CODC Risk Management Policy and framework. The IS Risk Register forms part of the IS Activity Management Plan and IS Management & Governance Framework. Cyber security, and information and records management risk will be reviewed as part of the upcoming Cyber Security, and Information and Records Management audits. • **A formal management report that provides the organisation with the level of service that IT provides and insights as to the value of its IT investments.** Executive Manager – Corporate Services reporting on IS projects was initiated April 2022. This will be expanded to the Information Services (IS) Steering Committee once this committee is implemented.

APPENDIX 1

Detailed Findings: Payroll

Description	Detail	Risk Rating	Recommendation	Determination Date	Status	Due Date	Person Responsible	Any additional Comments
Payroll								
Enhancement required for manual timesheets	Central Otago District Council has both waged and salaried employees. Timesheets for waged employees are manually entered into the Pay Global system.	Moderate	Implementing an automated process of capturing the time worked by the waged staff will increase efficiency and reduce the possibility of errors.	Aug-20	Completed	Moved to 31 July 2022 ~~1/03/2021~~	Finance Manager	The pools are now using electronic timesheet entry, except for Ranfurly as they don't have access to a computer and the pool is only open over summer. There are a handful of manual timesheets but these are only for salaried staff that are working any additional hours to their salary.

22.2.4 FINANCIAL REPORT FOR THE PERIOD ENDING 31 MARCH 2022

Doc ID: 580293

1. Purpose

To consider the financial performance for the period ending 31 March 2022.

Recommendations

That the report be received.

2. Discussion

The quarterly financial report is presented to the Committee as part of regular updates.

3. Financial Reporting

The financials for March 2022 show an overall favourable variance of $1.274M. Development contributions are higher than budget by $967k. Offsetting this, are unfavourable variances in grants and subsidies, interest and dividends, and user fees and charges. Cost of Sales of $1.964M have come through for stage one of the Dunstan Park subdivision. The budgets for subdivision cost of sales are recognised in June.

Income of $52.068M against the year-to-date budget of $51,420M

Overall income has a favourable variance against the revised budget by $648k. This is being driven by the timing of development contributions with a favourable variance of $967k. This variance is offset by the timing of water meter readings and Waka Kotahi subsidies.

The main variances are:

- Government grants and subsidies revenue has an unfavourable variance of ($106k). This is mainly due to the timing of the Waka Kotahi New Zealand Transport Agency (Waka Kotahi) roading subsidy contributing an unfavourable variance of ($264k). Subsidies are claimed for both the operational and capital roading work programmes and fluctuate based on the work programme. This unfavourable variance is offset by Tourism Infrastructure funding (TIF) of $165k for the Clyde Historic Precinct toilet upgrades. The budget for this is recognised in other income, however this funding has been correctly recognised in grants and subsidies.
- User fees and other has an unfavourable variance of ($350k). This is being driven by the timing of the water meter reading, with a variance of ($286k). There is another water meter read due before the end of the financial year. Other income has a variance of ($56k). This is due to the grants budget being included in 'other income' rather than the correct place of grants and subsidies. This budget includes the TIF funding for the new Clyde toilet and Miners Lane carparks.

- Regulatory fees has a favourable variance of $140k. This variance continues to be driven by building consent revenue received, which year-to-date is $158k ahead of budget.
- Development Contributions has a favourable variance of $967k. This variance relates to the timing of development contributions which are dependent on the resource consent process and developer timeframes. Cromwell development contributions in wastewater, water and roading are higher than budgeted.
- Interest and dividends revenue is unfavourable against budget by ($129k). Interest rates received on term deposit investments are continuing to remain low, due to low market interest rates. Large project costs are also being managed with current cashflows while waiting for income to be received. This includes subdivision development costs. This results in less cash available to be invested and reduces the length of time term deposits can be locked in for. The current investment with Kiwibank is only returning 0.7% interest.

Expenditure of $37.686M against the year-to-date budget of $38.312M

Expenditure has a favourable variance of $626k. The main drivers behind the favourable variance are contracts, staff, professional fees, and other costs. Offsetting this favourable variance is the cost of sales from stage 1 of the Dunstan Park subdivision, along with depreciation.

The main variances are:

- Staff costs have a favourable variance of $303k. The is due in part to the lag between staff movement and the replacement of new staff, plus the relevant recruitment costs. It also includes staff training, made up of conferences and planned attendance at workshops, travel and accommodation. Attendance and travel plans have been delayed due to the on-going impact of COVID-19.
- Contracts has a favourable variance of $356k. Contract expenditure is determined by workflow and the time of the contract. The outcome of this is that the phased budgets will not necessarily align with actual expenditure, meaning some work appears favourable, and some contracts spend year-to-date appear unfavourable. Planned maintenance $147k; contracts $187k; and roading contracts $31k are the key timing variances year-to-date. The contracts variance of $187k is being driven by the timing of the Three Waters Stimulus operational improvements projects.
- Professional fees has a favourable variance of $291k. This is similar to contract expenditure where budget and actuals do not align throughout the year but typically align by the end of year. Major variances include, engineers fees $76k; management consultants $178k; planning consultants $112k and recoverable professional fees ($178k).
- Depreciation has an unfavourable variance of ($75k). This is mainly due to a difference between the actual and budgeted wastewater depreciation. Wastewater assets reflect the updated valuations which occurred after the 2021-31 Long-term Plan was approved. The depreciation budget has been brought into alignment for the 2022-23 Annual Plan. Areas with major variances include, parks and reserves recreation $213k; roading $64k; and wastewater ($234k).
- Costs of sales has an unfavourable variance of ($1.104M). This is due to the costs incurred for stage 1 of the Dunstan Park subdivision and is offset by land sales revenue of $3.7M received for the first stage of this development. The costs of sales budget is

reflected with 50% expenditure in April and 50% in June. Development costs from Cemetery Road for stage 1 have not yet been finalised and allocated to cost of sales. The subdivision development costs are held on the balance sheet in property intended for sale until each stage is complete and land sales are received.

- Repairs and maintenance has a favourable variance of $117k, mainly due to the timing of various projects as well as building maintenance requirements. Weed control of $33k, buildings repairs and maintenance $44k and equipment hire $27k are the key timing variances.
- Projects has a favourable variance of $147k, due to the phasing schedule of Tourism Central Otago projects.
- Other costs has a favourable variance of $332k. A detailed breakdown for other costs is tabled below.

2021/22	9 MONTHS ENDING 31 MARCH 2022					2021/22
		YTD	YTD	YTD		
Annual Plan $000		Actual $000	Revised Budget $000	Variance $000		Revised Budget $000
	Income					
33,270	Rates	25,215	25,180	35	🟢	33,270
7,248	Govt Grants & Subsidies	12,084	12,190	(106)	🔴	16,890
7,323	User Fees & Other	5,003	5,353	(350)	🔴	7,737
17,286	Land Sales	4,769	4,767	2	🟡	14,739
2,155	Regulatory Fees	2,033	1,893	140	🟢	2,157
2,104	Development Contributions	2,505	1,538	967	🟢	2,114
388	Interest & Dividends	57	186	(129)	🔴	392
-	Reserves Contributions	293	196	97	🟢	196
-	Profit on Sale of Assets	14	-	14	🟢	-
55	Other Capital Contributions	95	117	(22)	🟡	150
69,829	**Total Income**	**52,068**	**51,420**	**648**	🟢	**77,645**
	Expenditure					
13,565	Staff	9,317	9,620	303	🟢	13,482
587	Members Remuneration	378	413	35	🟢	587
8,904	Contracts	6,532	6,888	356	🟢	9,811
2,902	Professional Fees	2,279	2,570	291	🟢	3,869
9,997	Depreciation	7,881	7,806	(75)	🔴	10,383
13,926	Costs of Sales	1,964	860	(1,104)	🔴	7,229
3,920	Refuse & Recycling Costs	2,971	3,037	66	🟢	4,029
-	Cost Allocations	(9)	(2)	7	🟢	(2)
1,723	Repairs & Maintenance	1,149	1,266	117	🟢	1,940
1,410	Electricity & Fuel	1,031	1,042	11	🟢	1,419
-	Loss on Sale of Asset	262	262	0	🟡	262
652	Grants	461	496	35	🟢	631
1,115	Technology Costs	704	760	56	🟢	1,100
303	Projects	704	851	147	🟢	1,231
639	Rates Expense	555	605	50	🟢	712
423	Insurance	451	450	(1)	🟡	455
2,037	Other Costs	1,056	1,388	332	🟢	2,087
62,103	**Total Expenses**	**37,686**	**38,312**	**626**	🟢	**59,225**
7,726	**Operating Surplus / (Deficit)**	**14,382**	**13,108**	**1,274**		**18,420**

This table has rounding (+/- 1)

- Other costs has been configured to include only needs-based costs which will fluctuate against budget. There are no large variances of note to report on at present.

Other costs breakdown is as below:

2021/22			YTD			2021/22
Annual	Other Costs breakdown	YTD	Revised	YTD		Revised
Plan		Actual	Budget	Variance		Budget
$000		$000	$000	$000		$000
535	Administrative Costs	232	344	112	●	562
690	Office Expenses	371	448	77	●	655
234	Operating Expenses	154	178	24	●	234
327	Advertising	135	229	94	●	374
175	Valuation Services	123	134	11	●	175
76	Retail	41	55	14	●	87
2,037	**Total Other Costs**	**1,056**	**1,388**	**332**		**2,087**

This table has rounding (+/- 1)

Council Property and Facilities $2.376M favourable against budget:
This is mainly due to the timing of the Cromwell Town Centre Projects currently underspent by $1.954M. This includes the Memorial Hall project, Cromwell Administration Buildings projects and Grounds, paths and fences around the Town Centre. Other areas behind budget include community buildings $379k, council offices $162k and elderly person housing $17k.

Waste Management $187k favourable against budget:
The transfer station reconfiguration projects are contributing to $192k of the underspend. Some of this work is underway but not all work will be completed this year.

Vehicle Fleet $28k favourable against budget:
Vehicle renewals and purchases are under budget with 54% of the $256k total revised budget being spent.

Information Services $161k favourable against budget:
Information Services projects are behind budget. Projects include enhanced customer experience digital services $22k, enterprise resource planning information services $16k, financial performance improvement $89k and information and records management $24k.

Libraries $150k favourable against budget:
This favourable variance is due to the timing of the Alexandra Library building upgrade. Currently this project is in the design phase.

Parks and Recreation $1.072M favourable against budget:
This favourable variance is driven by a mixture of the timing of project budgets and contractor's availability to perform the work. Projects include landscaping, signage and irrigation. The Cromwell pool replacement heat pump accounts for half of the capital budget variance. The work on installing the heat pump is well underway and is expected to be completed in late June.

Roading ($1.639) unfavourable against budget:
This unfavourable variance is due to the timing of the budget and work programme. Year-to-date $1.226M of the $1.365M annual revised budget has been spent. There is currently no budget allocated year-to-date March 2022, with the budget being allocated out over April, May and June. Other roading projects include footpath renewals $127k, carpark renewals $161k, structures renewals $173k, sealed road renewals ($584k), gravel road renewals ($206k) and drainage renewals ($50k). These variances are due to the timing of budgets and the work programme.

Three Waters is $2.1M favourable against budget:
The favourable variance is due to the timing of construction projects. The main drivers include the Lake Dunstan water supply $1.062M, water treatment plant and capacity upgrades $2.3M, wastewater improvements $135k and water stimulus fund projects $383k.

2021/22 Annual Plan $000	CAPITAL EXPENDITURE	YTD Actual $000	YTD Revised Budget $000	YTD Variance $000		2021/22 Revised Budget $000	Progress to date against revised budget
6,058	Council Property and Facilities	1,088	3,464	2,376	🟢	9,305	12%
382	Waste Management	384	571	187	🟢	913	42%
-	i-SITEs	-	1	1	🟡	4	0%
50	Customer Services and Administration	15	33	18	🟢	62	24%
204	Vehicle Fleet	139	167	28	🟢	256	54%
248	Planning	-	139	139	🟢	348	0%
352	Information Services	193	354	161	🟢	1,369	14%
164	Libraries	98	248	150	🟢	512	19%
1,713	Parks and Recreation	729	1,801	1,072	🟢	3,755	19%
7,420	Roading	5,289	3,650	(1,639)	🔴	8,129	65%
14,243	Three Waters	18,444	20,546	2,102	🟢	40,295	46%
30,834	**Grand Total**	**26,379**	**30,974**	**4,595**		**64,948**	**41%**

Statement of Financial Position

The Statement of Financial Position (Balance Sheet) is a new report which will be included in the reports to both Council and to the Audit and Risk Committee. It is included to show the comparisons between actuals and budget. Below the financial position is a table summarising the reserves and the cash balances. This gives assurance that there are available funds to meet the cash financial reserve balances typically included in Council's set of financial reports.

2020/21 Full Year Actual	2020/21 YTD March Actual	STATEMENT OF FINANCIAL POSITION	2021/22 YTD March Actual	2021/22 Full Year Revised Budget	2021/22 Full Year Annual Plan
$000	$000	for the period ended 31 March 2022	$000	$000	$000
		EQUITY			
392,499	382,751	Ratepayers equity	404,031	410,719	389,661
12,318	10,009	Surplus/(Deficit)	14,382	18,420	7,726
7,035	14,638	Council Reserves	7,905	4,176	4,177
487,476	483,506	Property revaluation reserve	487,404	496,640	496,629
(17)	(20)	Investment shares fair value revaluation reserve	(17)	(20)	(20)
80	80	Restricted reserves	80	80	80
899,391	**890,964**	**Total equity**	**913,785**	**930,015**	**898,253**
		REPRESENTED BY:			
		Current assets			
6,514	15,051	Cash and cash equivalents	3,594	19,896	19,896
10,000	5,000	Other financial assets	5,000	8,000	8,000
4,852	1,054	Receivables	3,078	3,171	3,171
-	-	Non Current assets held for sale	-	-	-
5,394	2,342	Inventories	6,988	(815)	1,509
-	-	Investment Bond	-	625	625
26,760	**23,447**	**Total current assets**	**18,660**	**30,877**	**33,201**
		Less current liabilities			
256	495	Agency and deposits	259	273	273
13,254	4,078	Payables and deferred revenue	8,900	4,705	4,705
673	581	Employee entitlements	697	1,010	1,010
-	-	Borrowings and other financial liabilities	-	-	-
14,183	**5,154**	**Total current liabilities**	**9,856**	**5,988**	**5,988**
12,577	**18,293**	**Working capital**	**8,804**	**24,889**	**27,213**
		Non-current assets			
111	109	Available for sale financial assets	111	109	109
282	295	Loans and receivables	241	333	333
26,030	22,830	Work in Progress	47,424	60,961	26,929
852,766	846,563	Property, plant and equipment	849,599	864,417	864,363
1,272	845	Intangible assets	1,250	2,271	
431	355	Forestry assets	431	357	357
5,925	1,675	Investment property	5,925	1,683	1,683
886,817	**872,672**	**Total non-current assets**	**904,981**	**930,131**	**896,045**
		Less non-current liabilities			
-	1	Provisions	-	5	5
-	-	Borrowings and other financial liabilities	-	25,000	25,000
-	**1**	**Total non-current liabilities**	**-**	**25,005**	**25,005**
899,394	**890,964**	**Net assets (assets minus liabilities)**	**913,785**	**930,015**	**898,253**

This table has rounding (+/- 1)

4. Accounts Receivable

As at 31 March 2022, Council had $47k outstanding in accounts receivables greater than 90 days. The key contributors over $5k include:

Sundry debtors:

- Top Shelf Productions $5.7k (agreement to fund People on Bikes Series 2)

Resource consents:

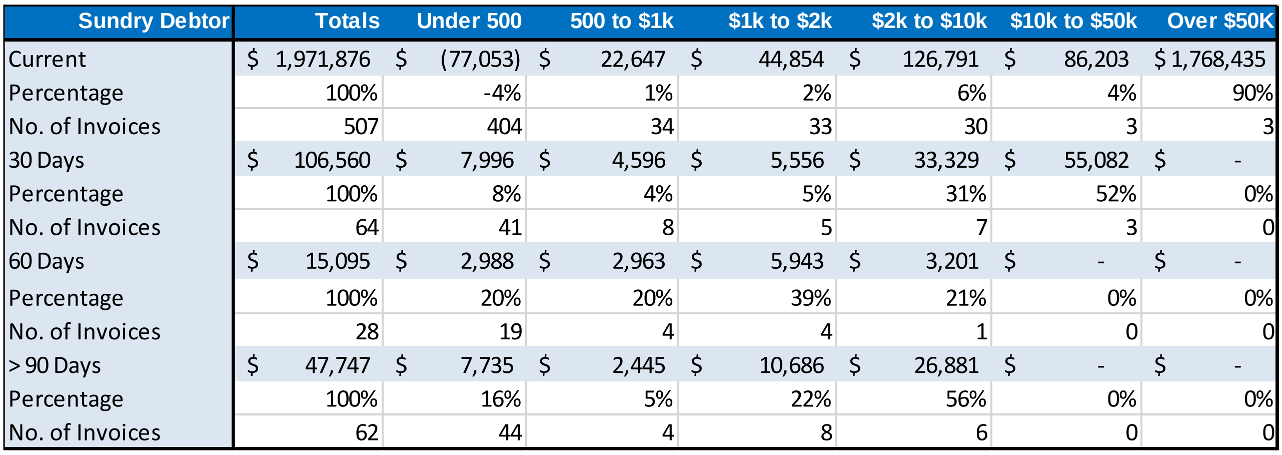
- M N Shaw $6.8k (payment plan in place – balance to be paid by 30 June 2022)

Type of Debtor	Current	30 Days	60 Days	> 90 Days
Other	$ 945,991	$ 19,260	$ 6,479	$ 14,769
Building Consents	$ 52,248	$ 40,097	$ 3,201	$ 18,166
Resource Consents	$ 973,637	$ 47,203	$ 5,415	$ 14,813
TOTAL	**1,971,876**	**$ 106,560**	**$ 15,095**	**$ 47,747**

Type of Debtor	Mar-22	Feb-22	Jan-22	Mar-21
Other	$ 986,498	$ 726,097	$ 175,546	$ 92,016
Building Consents	$ 113,711	$ 132,621	$ 97,148	$ 34,002
Resource Consents	$ 1,041,069	$ 92,396	$ 84,218	$ 192,312
TOTAL	**$ 2,141,278**	**$ 951,114**	**$ 356,912**	**$ 318,330**

Debt is actively managed and monitored and if a debtor is past our three-month threshold, their information is sent to our debt collection agency, Receivables Management Limited.

There is a credit balance of ($77k) in current month outstanding invoices in “under 500”. This relates to building and resource consent debtors where payment has been made in advance of the invoice.



Sundry Debtor	Totals	Under 500	500 to $1k	$1k to $2k	$2k to $10k	$10k to $50k	Over $50K
Current	$ 1,971,876	$ (77,053)	$ 22,647	$ 44,854	$ 126,791	$ 86,203	$ 1,768,435
Percentage	100%	-4%	1%	2%	6%	4%	90%
No. of Invoices	507	404	34	33	30	3	3
30 Days	$ 106,560	$ 7,996	$ 4,596	$ 5,556	$ 33,329	$ 55,082	$ -
Percentage	100%	8%	4%	5%	31%	52%	0%
No. of Invoices	64	41	8	5	7	3	0
60 Days	$ 15,095	$ 2,988	$ 2,963	$ 5,943	$ 3,201	$ -	$ -
Percentage	100%	20%	20%	39%	21%	0%	0%
No. of Invoices	28	19	4	4	1	0	0
> 90 Days	$ 47,747	$ 7,735	$ 2,445	$ 10,686	$ 26,881	$ -	$ -
Percentage	100%	16%	5%	22%	56%	0%	0%
No. of Invoices	62	44	4	8	6	0	0

5. Investment

As at 31 March 2022, Council had cash balances of $8.59M, of which term deposits totalling $5M mature within 90 days.

Bank	Amount	Term (Month)	Start Date	End Date	Fixed Rate
KiwiBank	5,000,000	1	16 March 2022	19 April 2022	0.70%

Weighted average interest rates for all council term deposits is 0.70%.

6. Internal Loans

Forecast closing balance for 30 June 2022 is $4.075M.

OWED BY	Original Loan	1 July 2021	30 June 2022 Forecast
		Opening Balance	Closing Balance
Public Toilets	670,000	491,239	468,048
Tarbert St Bldg	25,868	13,067	11,574
Alex Town Centre	94,420	49,759	44,545
Alex Town Centre	186,398	91,041	79,921
Alex Town Centre	290,600	155,412	139,137
Centennial Milkbar	47,821	21,284	18,192
Vincent Grants	95,000	19,000	9,500
Pioneer Store Naseby	21,589	10,949	9,609
Water	867,000	717,829	691,212
ANZ Bank Seismic Strengthening	180,000	149,030	143,504
Molyneux Pool	650,000	571,900	539,400
Māniōtoto Hospital	1,873,000	1,775,142	1,723,630
Alexandra Airport	218,000	204,485	197,216
Total	**5,219,695**	**4,270,138**	**4,075,488**

7. External Community Loans

The total amount of external loans at the beginning of the financial year 2021-22 was $189k. As at 31 March 2022, the outstanding balance was $148k. Council has received $40.9k in principal payments and $7.1k in interest payments.

Owed By	Original Loan	1 July 2021 Actual Opening Balance	Principal	Interest	31 March 2022 Actual Closing Balance
Cromwell College	400,000	130,770	26,369	5,218	104,400
Māniōtoto Curling	160,000	35,662	10,248	1,167	25,413
Oturehua Water	46,471	22,623	4,307	795	18,316
	606,471	**189,055**	**40,924**	**7,180**	**148,129**

8. Reserve Funds table

- As at 30 June 2021 the Council has an audited closing reserve funds balance of $7.035M. This reflects the whole district's reserves and factors in the district-wide reserves which are in deficit at ($16.7M). Refer to Appendix 1.
- Taking the 2020-21 audited Annual Report closing balance and adding 2021-22 income and expenditure, carry forwards and resolutions, the whole district is projected to end the 2021-22 financial year with a closing deficit of ($12.825M).

9. Attachments

Appendix 1 - Council Wide Reserve Funds 2021-2022.pdf ⇩

Report author:	Reviewed and authorised by:
Ann McDowall Finance Manager 16/05/2022	Leanne Macdonald Executive Manager - Corporate Services 16/05/2022

CODC RESERVE FUNDS

	AUDITED - 2020/21 Annual Report				2021/22 AP	Adjusted 2021/22 AP Closing*	Approved By Council forecast includes carry forwards	
RESERVES BY RATE TYPE	Opening Balance	Transfers In	Transfers Out	Closing Balance	Net Transfers In and Out	Adjusted AP Closing Balance*	2021/22 Forecast	2021/22 Revised Closing Balance
	A	B	C	D = (A + B - C)	E	F = (D + E)	H	I = (F + G + H)
General Reserves	5,140,942	1,461,175	(5,790,676)	811,442	(3,256,179)	(2,444,737)	(552,456)	(2,997,193)
Uniform Annual General Charge Reserves	186,374	9,717	(22,829)	173,261	(43,347)	129,914	(37,967)	91,947
	5,327,316	**1,470,892**	**(5,813,505)**	**984,703**	**(3,299,526)**	**(2,314,824)**	**(590,422)**	**(2,905,246)**
TARGETED RESERVES								
Planning and Environment Rate	1,949,635	424,331	-	2,373,966	31,214	2,405,180	(822,674)	1,582,506
Economic Development Rate	-	-	-	-	-	-	(8,541)	(8,541)
Tracks and Waterways Charge	442,590	43,362	(9,107)	476,845	14,952	491,797	10	491,807
Tourism Rate	238,245	54,424	(41,898)	250,771	18,528	269,299	279,734	549,033
Waste Management and Collection Charge	(1,344,674)	7,738	(866,131)	(2,203,067)	(341,821)	(2,544,888)	(826,398)	(3,371,286)
District Library Charge	99,517	38,009	(71,831)	65,694	(161,236)	(95,542)	(439,965)	(535,507)
Molyneux Park Charge	(22,805)	-	(55,941)	(78,746)	(204,243)	(282,989)	(84,569)	(367,557)
District Works and Public Toilets Rate	4,079,979	664,517	(317,935)	4,426,561	(212,876)	4,213,685	(988,086)	3,225,600
District Water Supply	(12,273,932)	1,495,595	(783,526)	(11,561,863)	2,230,636	(9,331,227)	(8,077,833)	(17,409,060)
District Wastewater	(10,340,895)	1,714,354	(3,141,747)	(11,768,288)	2,317,851	(9,450,437)	(10,397,812)	(19,848,250)
	(17,172,340)	**4,442,330**	**(5,288,116)**	**(18,018,126)**	**3,693,004**	**(14,325,122)**	**(21,366,134)**	**(35,691,255)**
Specific Reserves	315,692	4,694	-	320,386	6,303	326,688	-	326,688
Other Reserves	518,608	20,004	(515,342)	23,270	(22,524)	746	(1,440,513)	(1,439,767)
	834,300	**24,698**	**(515,342)**	**343,655**	**(16,221)**	**327,434**	**(1,440,513)**	**(1,113,079)**
WARD TARGETED RATES								
Vincent Community Board Reserves								
Vincent Promotion Rate	-	-	-	-	-	-	-	-
Vincent Recreation and Culture Charge	(1,706,400)	320,321	-	(1,386,080)	(333,560)	(1,719,640)	(635,373)	(2,355,013)
Vincent Ward Services Rate	2,906,503	139,599	(542,563)	2,503,538	3,109,890	5,613,429	3,924,771	9,538,200
Vincent Ward Services Charge	1,133	15	(11,398)	(10,251)	(3,243)	(13,493)	(31,526)	(45,019)
Vincent Ward Specific Reserves	1,165,253	24,458	(2,823)	1,186,888	35,415	1,222,303	2,582	1,224,885
Vincent Ward Development Fund	455,132	54,842	(1,910)	508,064	9,080	517,144	103,988	621,132
Alex Town Centre Upgrade 1991	(60,558)	283	(49,540)	(109,815)	380	(109,435)	-	(109,435)
	2,761,062	**539,516**	**(608,234)**	**2,692,345**	**2,817,962**	**5,510,307**	**3,364,442**	**8,874,749**
Cromwell Community Board Reserves								
Cromwell Promotion Rate	-	-	-	-	-	-	-	-
Cromwell Recreation and Culture Charge	(785,036)	122,790	(19,707)	(681,953)	(159,891)	(841,844)	(1,602,230)	(2,444,074)
Cromwell Ward Services Rate	19,596,874	2,813,940	(4,268,599)	18,142,215	557,468	18,699,682	(1,698,481)	17,001,202
Cromwell Ward Services Charge	1,899	28	(402)	1,525	(7,550)	(6,024)	1,550	(4,474)
Cromwell Ward Specific Reserves	(296,409)	9,319	(42,404)	(329,494)	8,776	(320,718)	(240)	(320,958)
Cromwell Ward Development Fund	1,555,686	222,649	(7,640)	1,770,695	30,992	1,801,687	64,304	1,865,991
	20,073,014	**3,168,727**	**(4,338,753)**	**18,902,988**	**429,795**	**19,332,783**	**(3,235,096)**	**16,097,686**
Maniototo Community Board Reserves								
Maniototo Promotion Rate	-	-	-	-	-	-	-	-
Maniototo Recreation and Culture Charge	(995,980)	1,883,384	(48,250)	839,154	11,474	850,629	(42,828)	807,801
Maniototo Ward Services Rate	1,418,766	188,340	(1,880,899)	(273,793)	133,178	(140,615)	(13,999)	(154,614)
Maniototo Ward Services Charge	3,104	8,260	-	11,363	(8,459)	2,904	(9,993)	(7,089)
Maniototo Ward Specific Reserves	212,789	23,274	-	236,063	4,246	240,309	12,331	252,640
Maniototo Ward Development Fund	-	-	-	-	-	-	-	-
	638,679	**2,103,258**	**(1,929,149)**	**812,788**	**140,439**	**953,227**	**(54,489)**	**898,738**
Teviot Valley Community Board Reserves								
Teviot Valley Promotion	14,683	213	-	14,897	234	15,130	(500)	14,630
Teviot Valley Recreation and Culture	285,234	19,851	(1,447)	303,639	(232,588)	71,051	(94,408)	(23,358)
Teviot Ward Services Rate	900,620	37,447	(29,457)	908,610	35,264	943,874	(14,466)	929,408
Teviot Ward Services Charge	-	-	-	-	-	-	-	-
Teviot Ward Specific Reserves	1,557	116	(1,838)	(165)	13	(152)	-	(152)
Teviot Ward Development Fund	77,962	12,667	(903)	89,726	1,554	91,280	955	92,235
	1,280,057	**70,293**	**(33,644)**	**1,316,706**	**(195,523)**	**1,121,183**	**(108,419)**	**1,012,763**
Grand Total Surplus/(Deficit)	**13,742,087**	**11,819,714**	**(18,526,743)**	**7,035,058**	**3,569,929**	**10,604,988**	**(23,430,631)**	**(12,825,644)**

* The Annual Plan closing balance has been adjusted to reflect the closing balance of the Annual Report and the Annual Plan movement. This is to enable a running estimate of the total Council Reserves balance.

22.2.5 CYBER SECURITY, INFORMATION AND RECORDS MANAGEMENT, AND PRIVACY UPDATE

Doc ID: 581244

1. Purpose

To consider an update on:

- Cyber Security Plan 2022-2025
- Information and Records Management Plan 2022-2025
- Privacy Plan

Recommendations

That the report be received.

2. Discussion

Information Services in addition to cyber security have been working on plans for information and records management and privacy.

In this report, the following topics will be covered:

Cyber Security Plan 2022-2025

- Audit and plan status
- What is happening in New Zealand?
- What is happening at Central Otago District Council?
- ALGIM Cyber Security Programme update
- Cyber Security programme of work by actions.

Information and Records Management Plan 2022-2025

- Audit and plan status

Future reports will include the following:

- Archives New Zealand Information Management Maturity Assessment update
- Information and Records Management programme of work by actions

Privacy Plan

- Audit and plan status

Future reports will include the following:

- Department of Internal Affairs Privacy Maturity Assessment Framework update

- Privacy programme of work by actions

Cyber Security Plan 2022-2025

Audit and plan status

The new Cyber Security Plan 2022-2025 will be based on the external audit scheduled to start 1 June 2022.

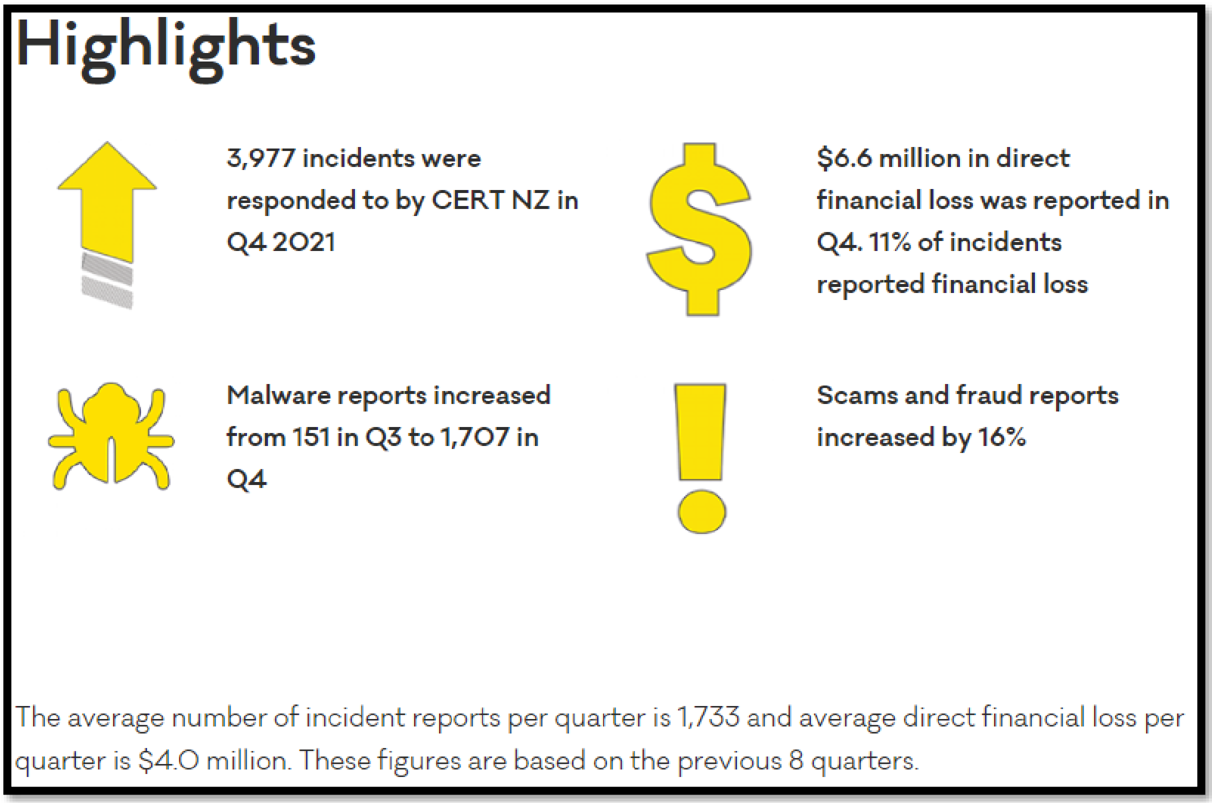
Attached is the draft Cyber Security Plan 2022-2025 that will form the basis of this audit. Focus areas of cyber security focus since the last report have been on:

- Preparing for the external audit
- User education, training and awareness
- Protective technology improvements to maximise value
- Updating and reviewing actions related to the requirements and controls for the Association of Local Government Information Management (ALGIM) Cyber Security Programme framework

What is happening in New Zealand?

Council utilise Computer Emergency Response Team (CERT) as a resource for cyber security support. CERT NZ works to support businesses, organisations and individuals who are affected (or may be affected) by cyber security incidents. CERT provide trusted and authoritative information and advice, while also collating a profile of the threat landscape in New Zealand.

The following highlights quarter four 2021 cyber security incidents across New Zealand:



Highlights

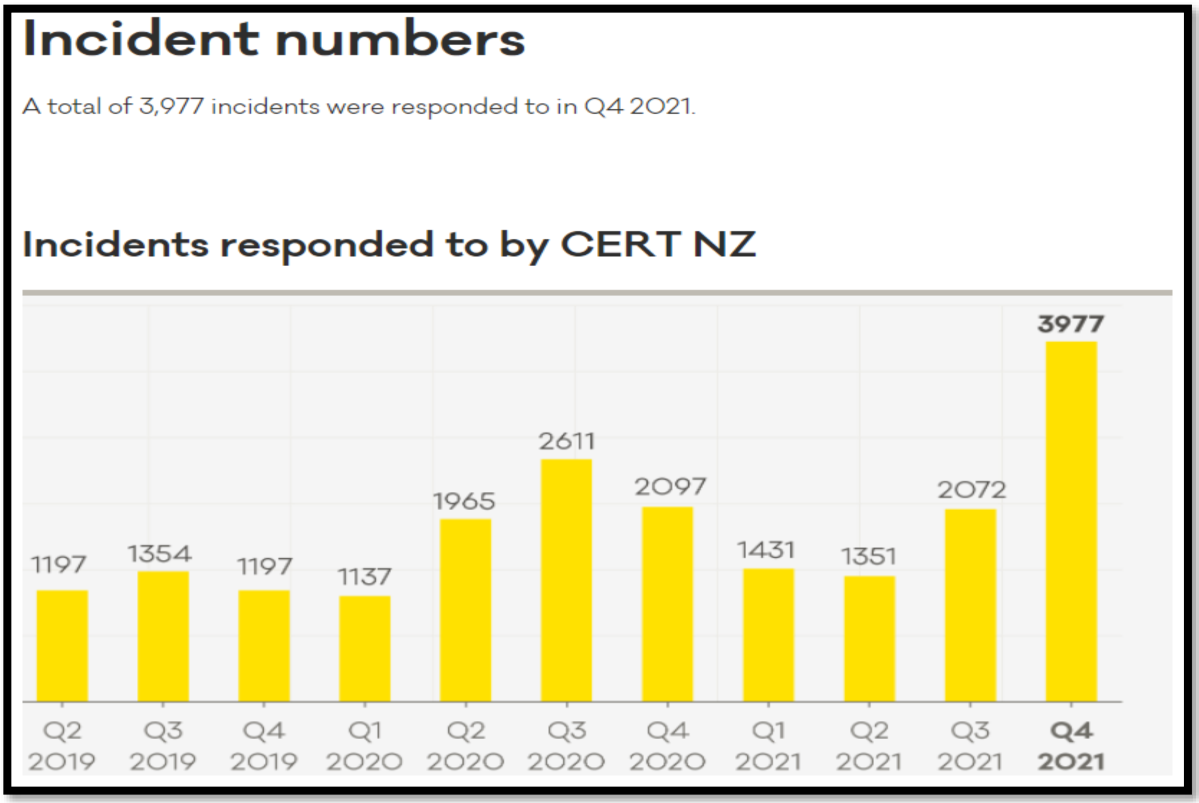
3,977 incidents were responded to by CERT NZ in Q4 2021

$6.6 million in direct financial loss was reported in Q4. 11% of incidents reported financial loss

Malware reports increased from 151 in Q3 to 1,707 in Q4

Scams and fraud reports increased by 16%

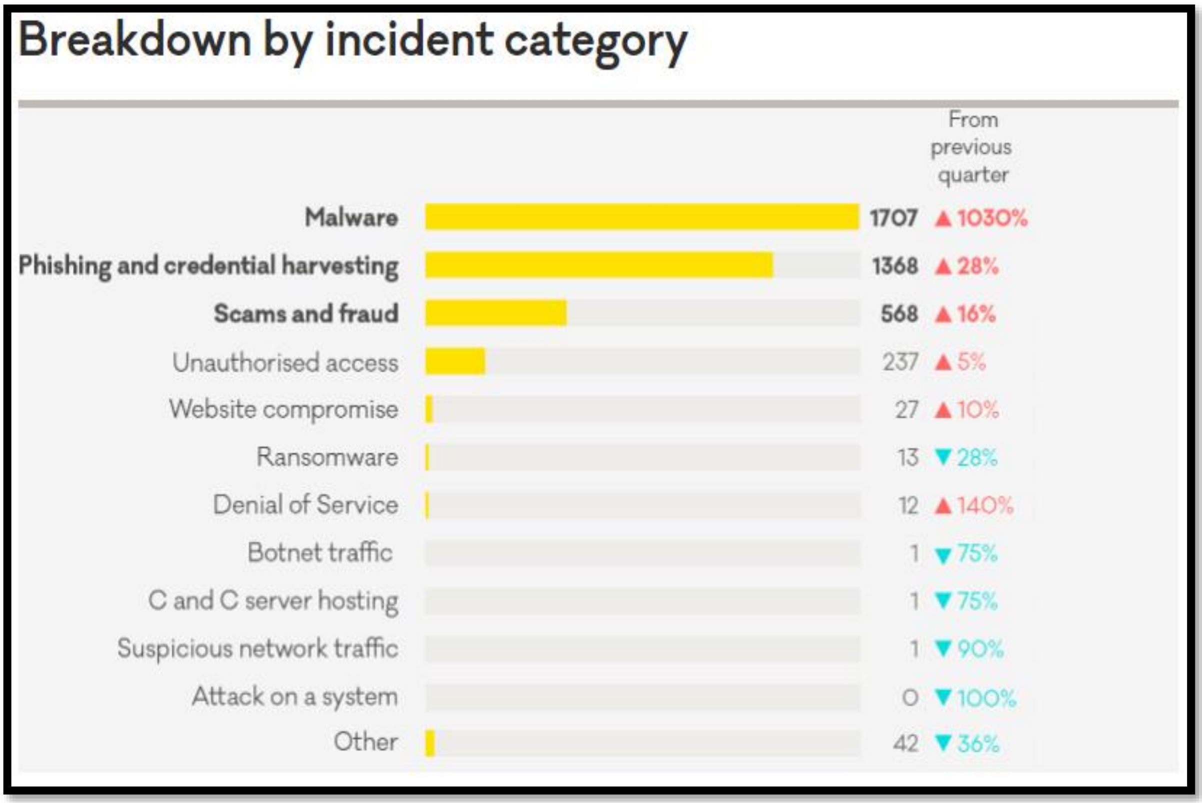
The average number of incident reports per quarter is 1,733 and average direct financial loss per quarter is $4.0 million. These figures are based on the previous 8 quarters.



Incident numbers

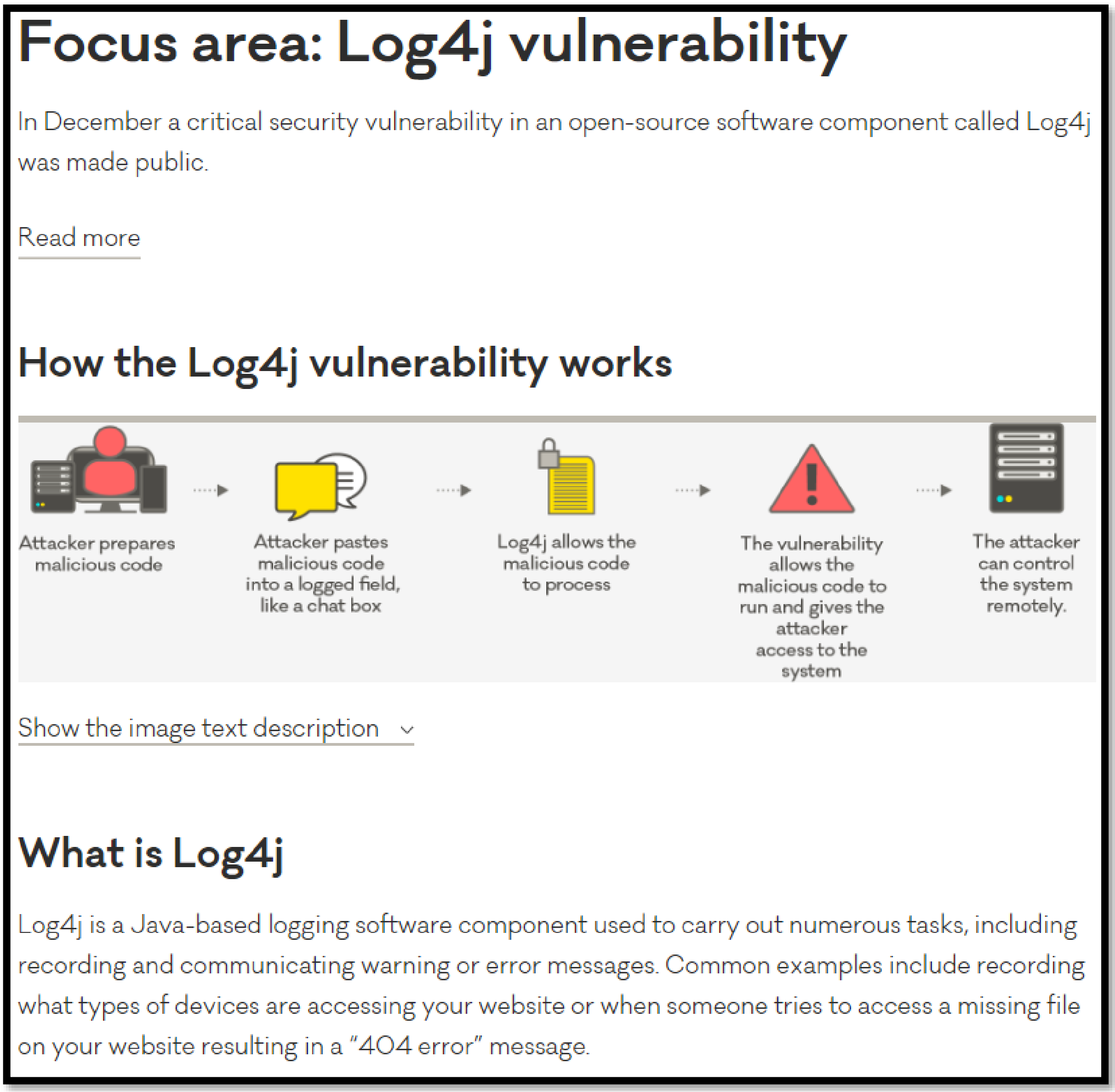
A total of 3,977 incidents were responded to in Q4 2021.

Incidents responded to by CERT NZ



Breakdown by incident category

		From previous quarter
Malware	**1707**	▲ 1030%
Phishing and credential harvesting	**1368**	▲ 28%
Scams and fraud	**568**	▲ 16%
Unauthorised access	237	▲ 5%
Website compromise	27	▲ 10%
Ransomware	13	▼ 28%
Denial of Service	12	▲ 140%
Botnet traffic	1	▼ 75%
C and C server hosting	1	▼ 75%
Suspicious network traffic	1	▼ 90%
Attack on a system	0	▼ 100%
Other	42	▼ 36%



Focus area: Log4j vulnerability

In December a critical security vulnerability in an open-source software component called Log4j was made public.

Read more

How the Log4j vulnerability works

Attacker prepares malicious code

Attacker pastes malicious code into a logged field, like a chat box

Log4j allows the malicious code to process

The vulnerability allows the malicious code to run and gives the attacker access to the system

The attacker can control the system remotely.

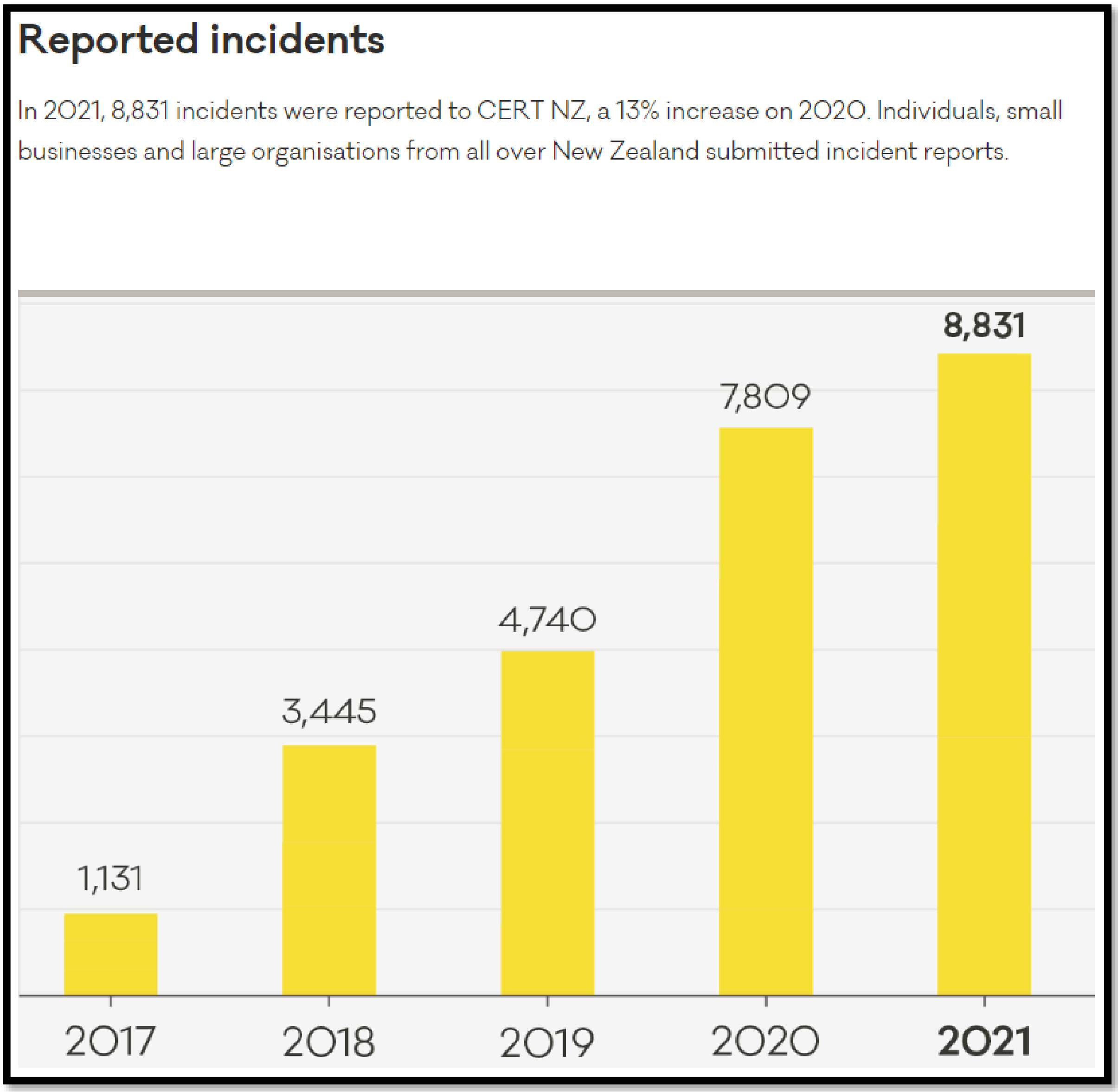
Show the image text description ⌄

What is Log4j

Log4j is a Java-based logging software component used to carry out numerous tasks, including recording and communicating warning or error messages. Common examples include recording what types of devices are accessing your website or when someone tries to access a missing file on your website resulting in a "404 error" message.

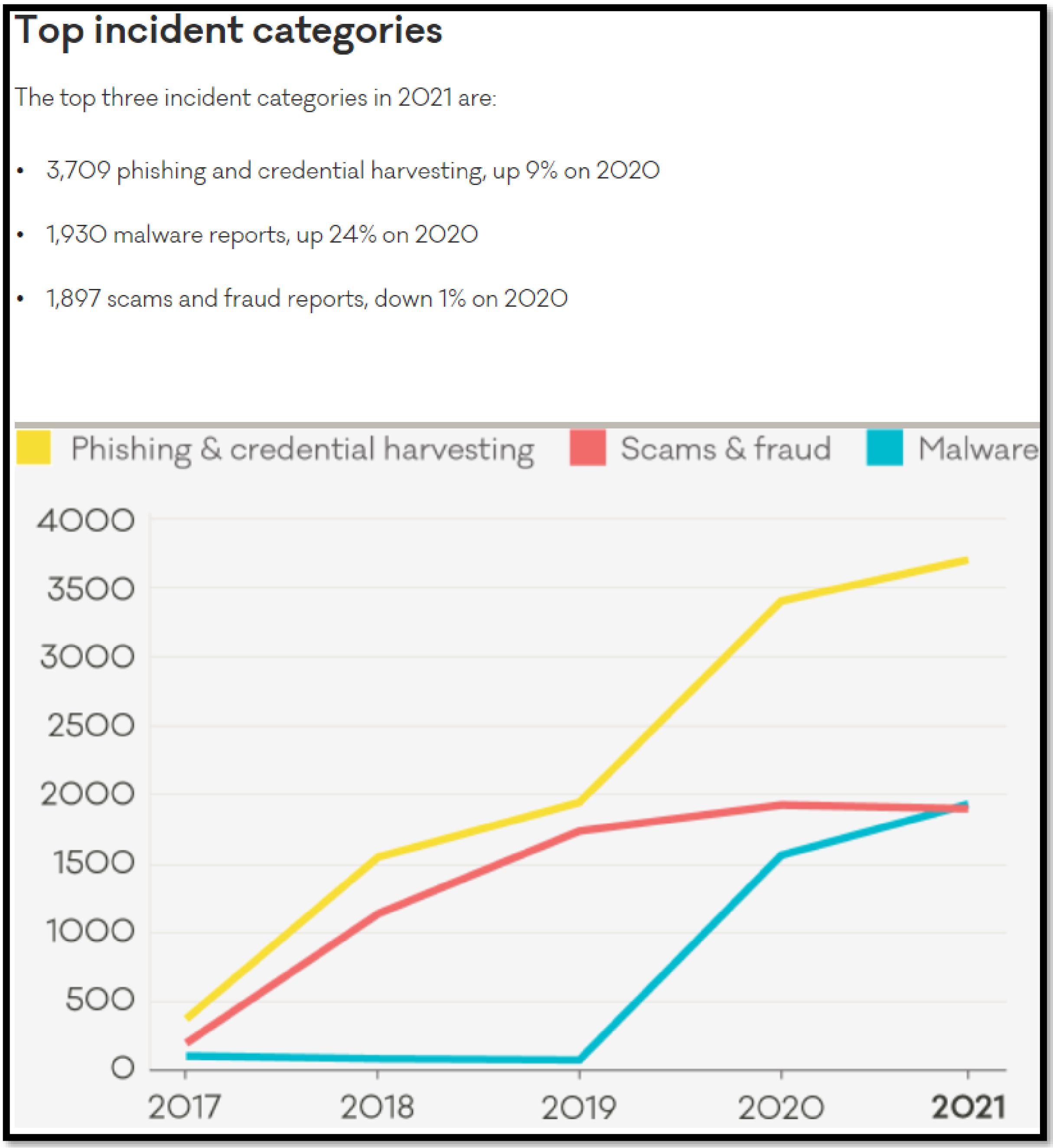
More details on the current threat landscape can be found here: [Quarter Four Report 2021 | CERT NZ]

In addition to the quarterly report, a summary of 2021 is now available: 2021 Report Summary | CERT NZ. Highlights of 2021:



Reported incidents

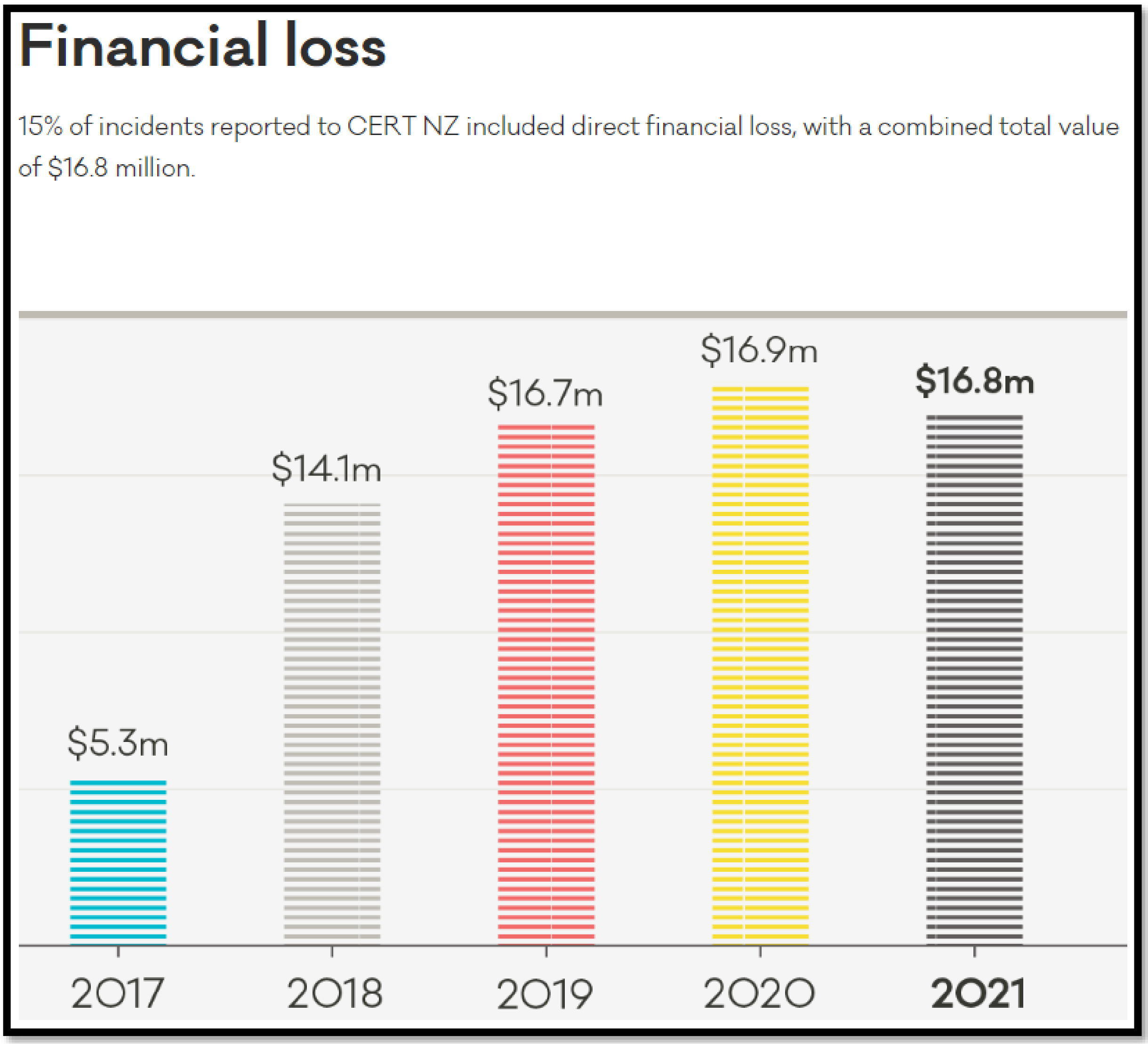
In 2021, 8,831 incidents were reported to CERT NZ, a 13% increase on 2020. Individuals, small businesses and large organisations from all over New Zealand submitted incident reports.



Top incident categories

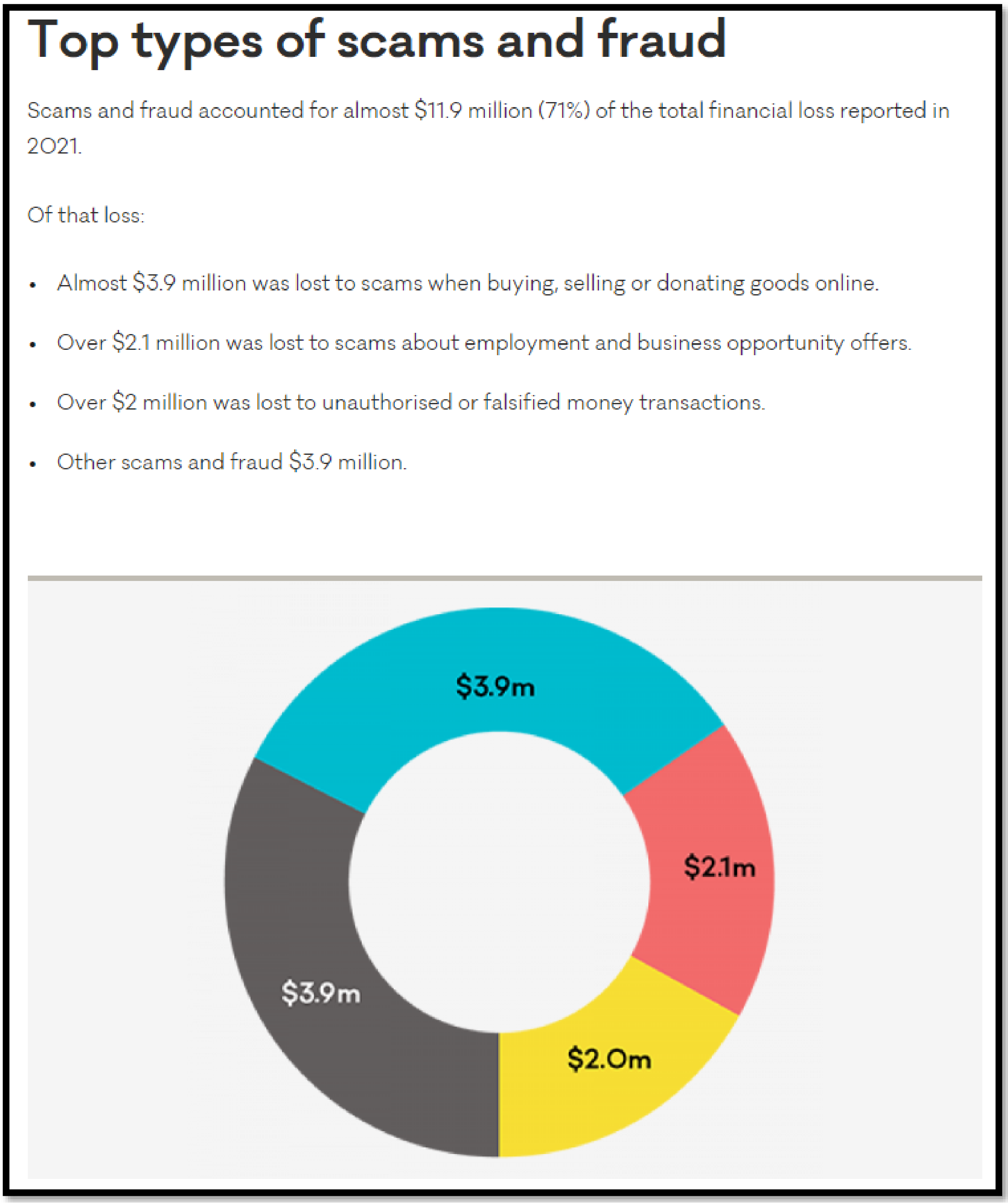
The top three incident categories in 2021 are:

- 3,709 phishing and credential harvesting, up 9% on 2020
- 1,930 malware reports, up 24% on 2020
- 1,897 scams and fraud reports, down 1% on 2020



Financial loss

15% of incidents reported to CERT NZ included direct financial loss, with a combined total value of $16.8 million.



Top types of scams and fraud

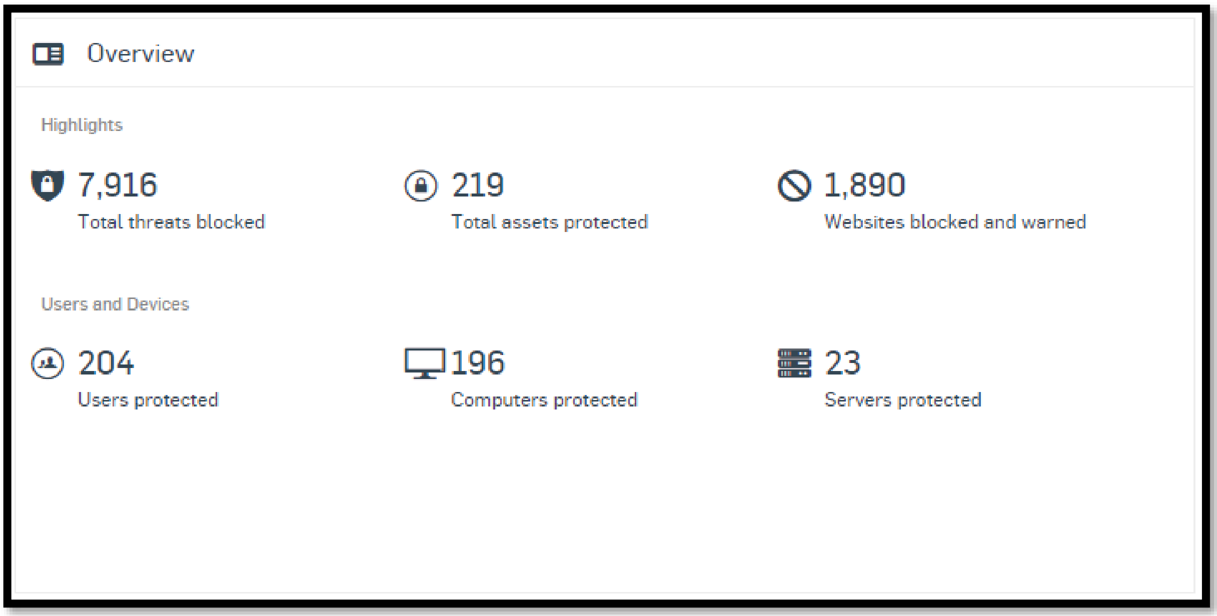
Scams and fraud accounted for almost $11.9 million (71%) of the total financial loss reported in 2021.

Of that loss:

- Almost $3.9 million was lost to scams when buying, selling or donating goods online.
- Over $2.1 million was lost to scams about employment and business opportunity offers.
- Over $2 million was lost to unauthorised or falsified money transactions.
- Other scams and fraud $3.9 million.

What is happening at Central Otago District Council?

The following outlines what Council protective technologies are doing for the 17 April 2022 to 17 May 2022 period:



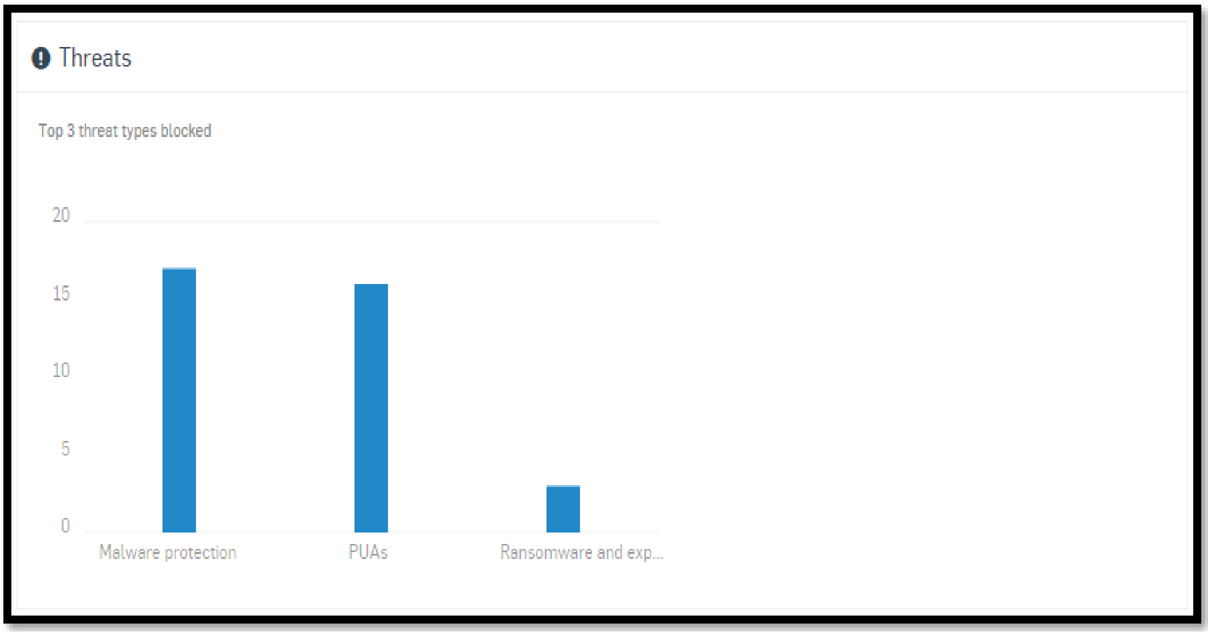
Overview

Highlights

7,916	Total threats blocked
219	Total assets protected
1,890	Websites blocked and warned

Users and Devices

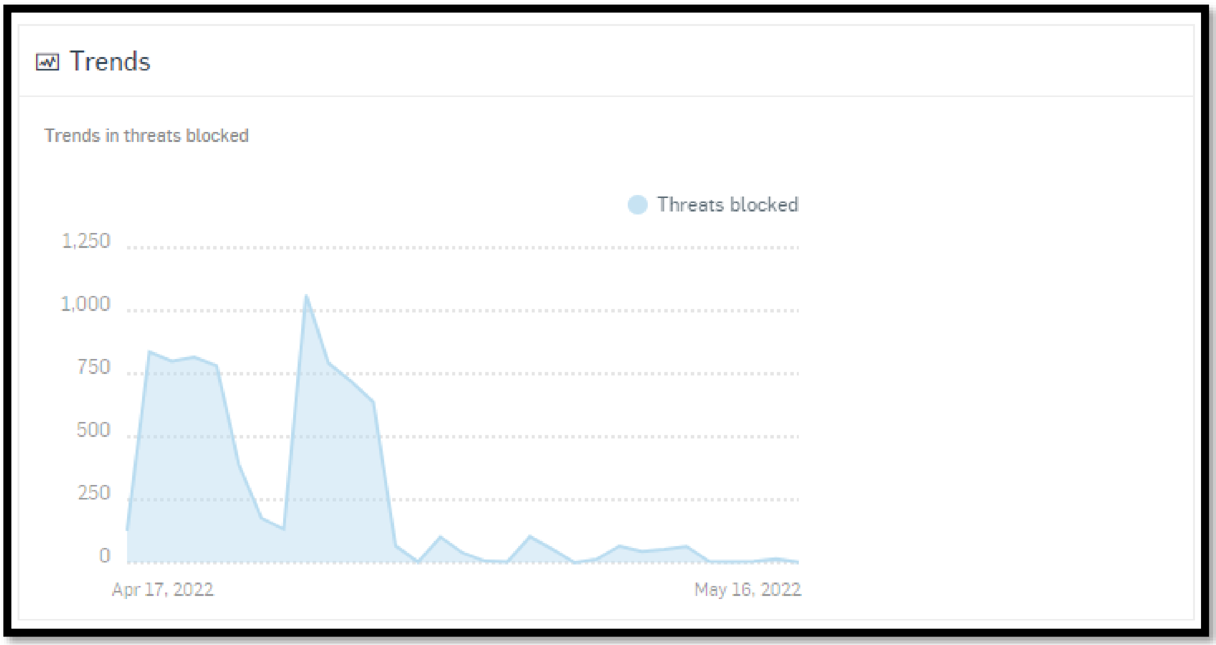
204	Users protected
196	Computers protected
23	Servers protected



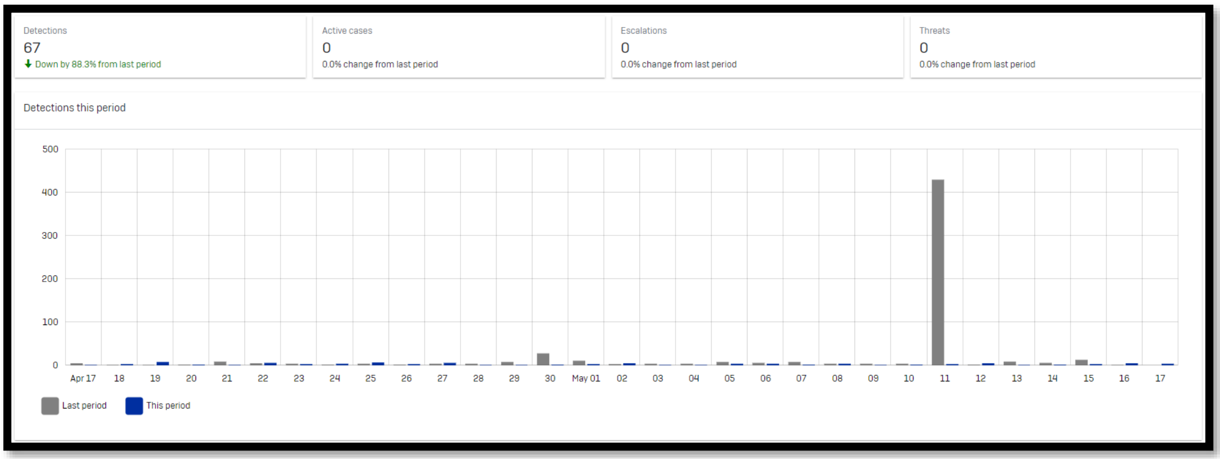
Threats

Top 3 threat types blocked

- Potentially unwanted applications (PUAs)



Managed Threat Response service over the last 30 days:



Detections
67
Down by 88.3% from last period

Active cases
0
0.0% change from last period

Escalations
0
0.0% change from last period

Threats
0
0.0% change from last period

<u>ALGIM Cyber Security Programme update</u>

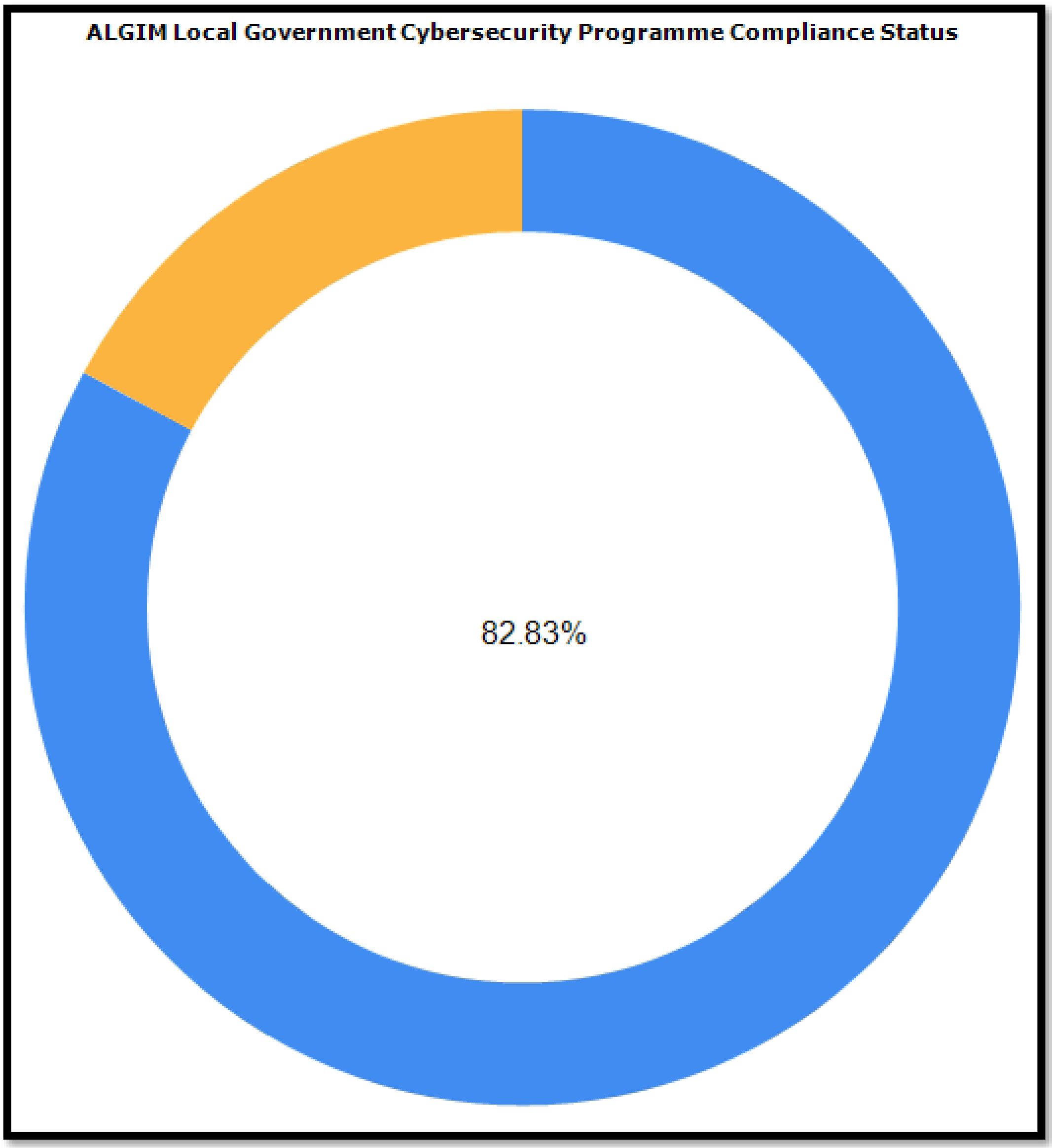
Association of Local Government Information Management (ALGIM) has defined a Cyber Security framework which is powered by SAM for Compliance giving councils the ability to manage and reduce organisational Cyber Security related risk. As part of the programme, councils that demonstrate defined levels of achievement and improvement will receive awards at the ALGIM annual conference.

The latest ALGIM Cyber Security Programme Management Status Report is attached for your information (Appendix 1).

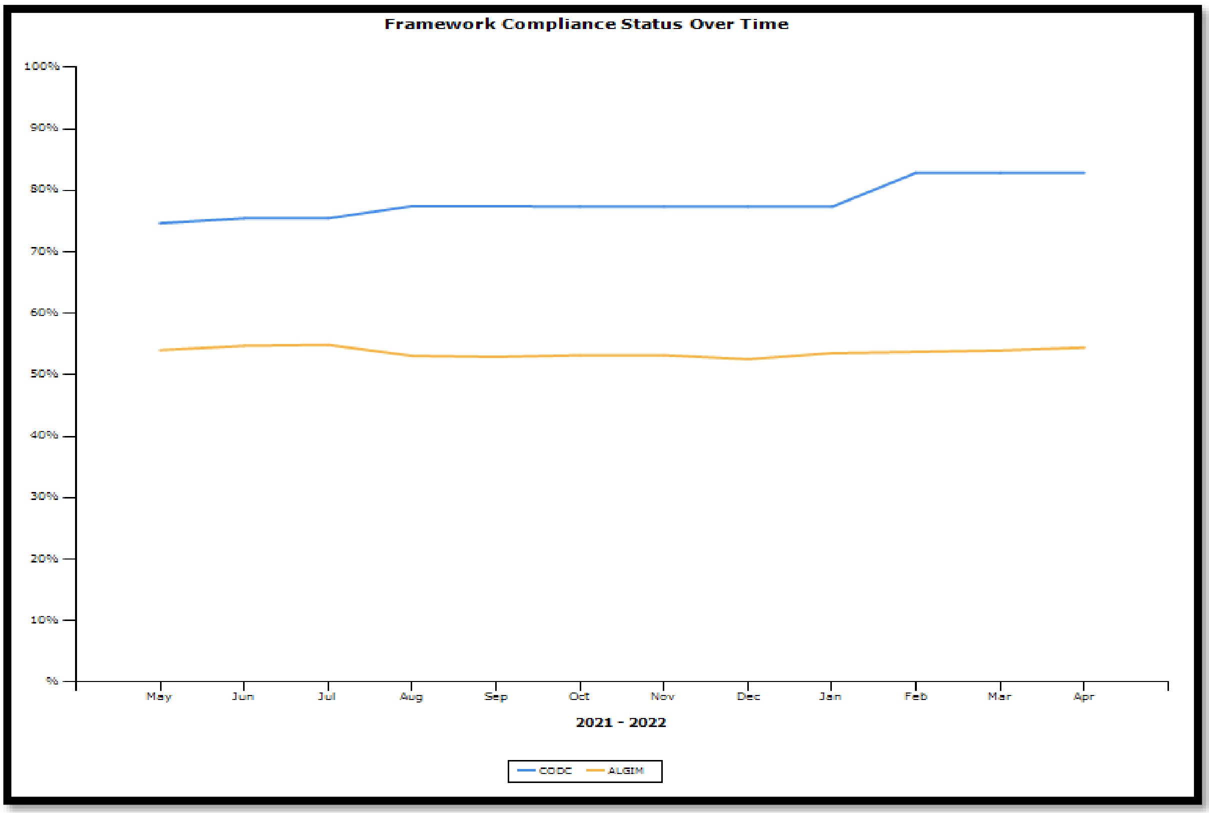
The upcoming external audit will reset Council’s compliance levels.

The following details the current snapshot of how Council is preforming within this framework benchmarked against other Councils:

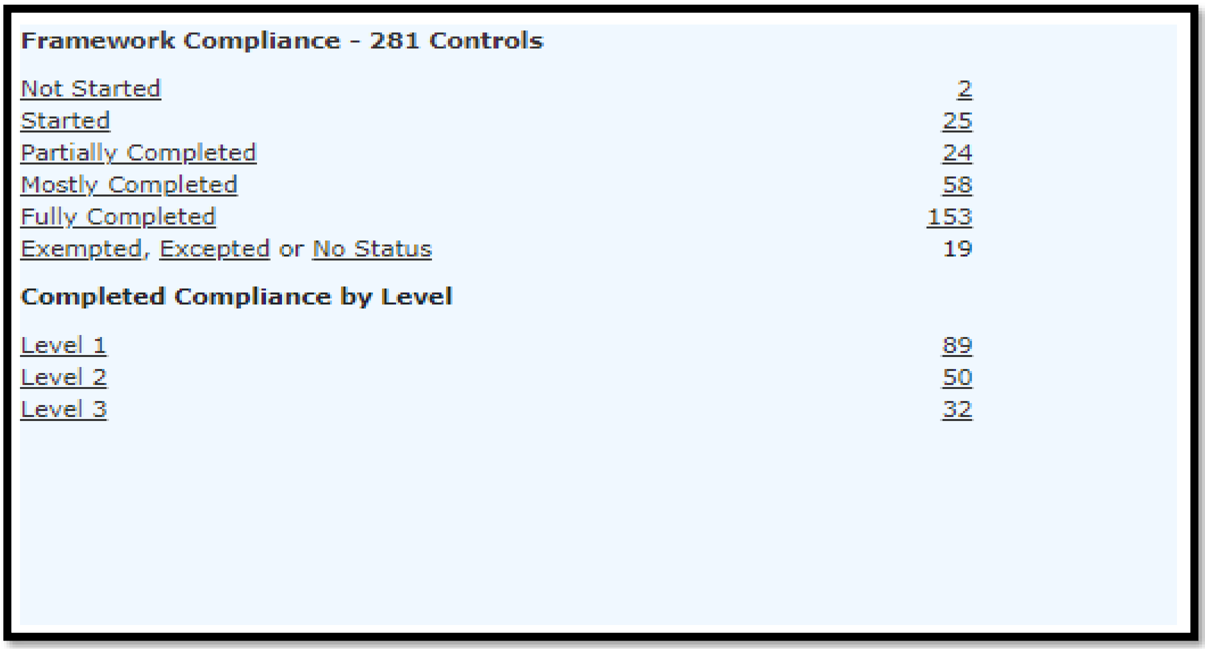
- The following shows that Council is 82.83% compliant with the framework controls:



- The following shows how Council is tracking against other councils within this framework over the last 12 months:



- The following is a summary of the controls by status:



Framework Compliance - 281 Controls

Not Started	2
Started	25
Partially Completed	24
Mostly Completed	58
Fully Completed	153
Exempted, Excepted or No Status	19

Completed Compliance by Level

Level 1	89
Level 2	50
Level 3	32

Overall, Information Services are regularly reviewing the framework once a month, updating controls and working on outstanding actions and improvements.

The following is summary of the improvements within each function:

Identify:

- Governance – Digital and Information Strategy is due to be finalised June 2022, which will include Cyber Security. This is currently with the Leadership Group for final feedback.

Manage

- Access Control – Planned physical security work has been delayed due to COVID-19. Work on remote access agreements with our contractors is being progressed.
- Information and Data Security – USB portable drives access restriction testing is progressing; exemptions are yet to be agreed.

Protect

- Awareness and Training – this is currently the focus, Phriendly Phishing virtual training, reporting and staff education is ongoing. Onsite specialist training has been delayed due to COVID-19.
- Protective Technology – After the core functionality was initially deployed and bedded in, improvements to maximise its value are being investigated and deployed to meet Council policies and standards.

Detect

- Anomalies and Events – Events Management Procedure has been finalised and implemented.

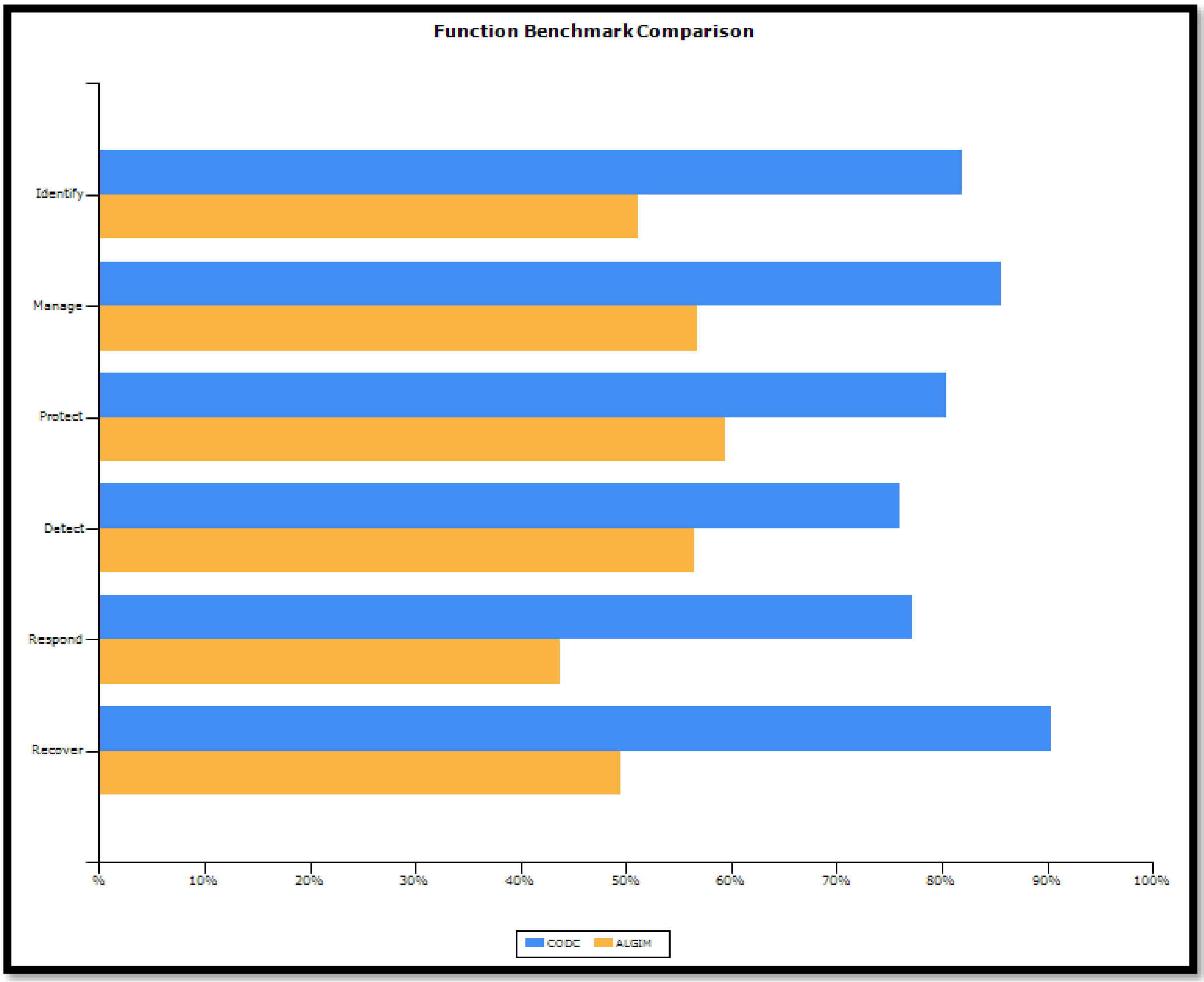
Respond

- Review of the Information and Communication Technology (ICT) Disaster Recovery Plan has been completed. Testing of this updated plan will confirm our ability to respond and meet the business continuity requirements.

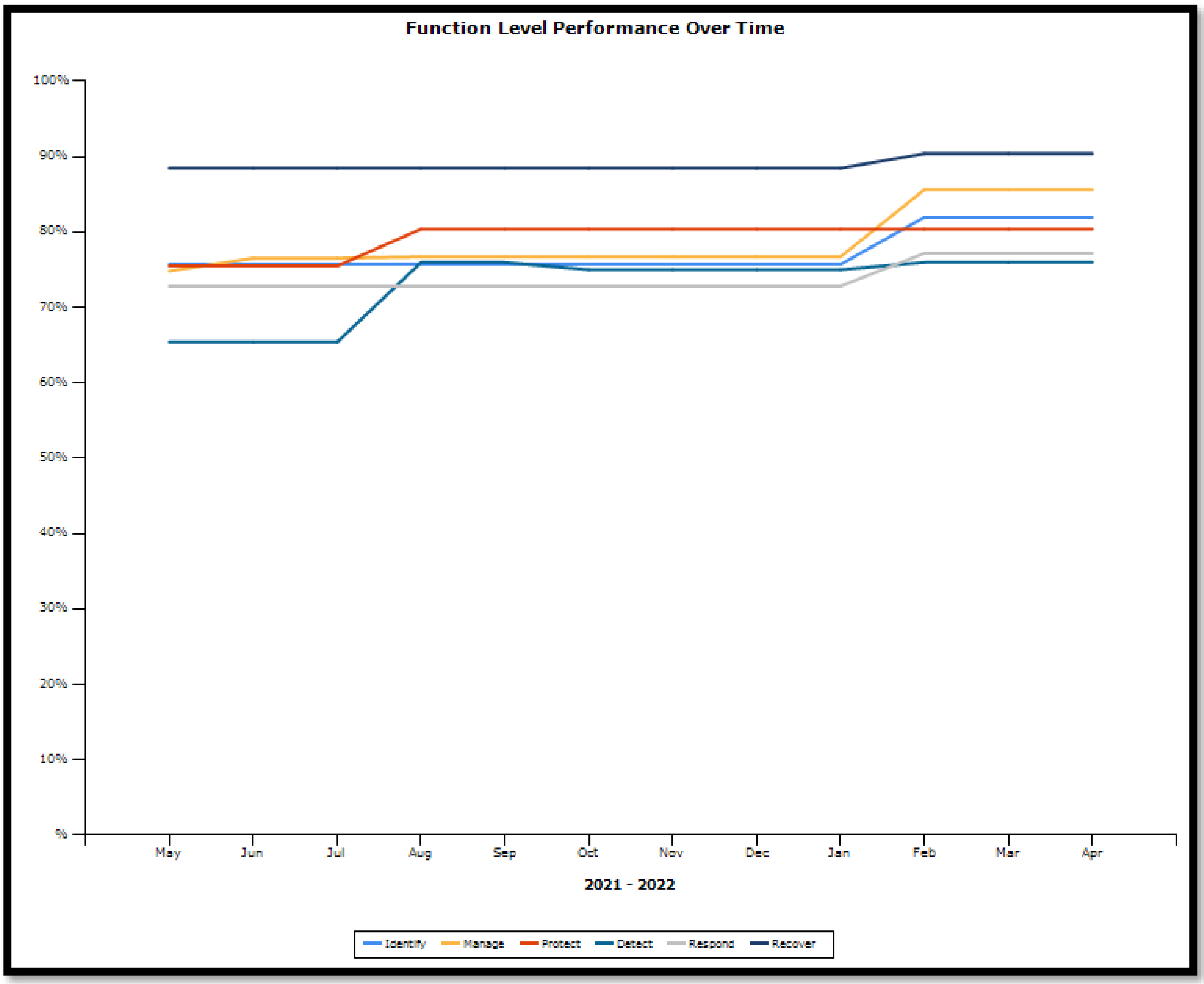
Recover

- ICT Disaster Recovery Plan and the Back-up and Recovery Procedure have been completed. Minor testing of recovery solution has been completed. Major testing is being worked through.

The following shows how Council is tracking by each function within the framework when compared to other councils:



The following shows the trend by each function over the last 12 months.



Cyber Security programme of work

The Cyber Security Plan is supported by Cyber Security programme of work. A new programme of work will be prepared as part of the audit and new Cyber Security Plan 2022-2025.

Information and Records Management Plan 2022-2025

Audit and plan status

Staff have been preparing the first Information and Records Management (IRM) Plan.
The purpose of the information and records management plan is to assess how Council currently manages its information and records what actions it needs to undertake to improve that management.

Information and records are key strategic assets of an organisation. These assets need to be actively managed to maintain and improve value. Information and records management assets take many forms, including data and business systems. Our digital and information strategy and this information and records management plan will guide Council to make its current operations more effective by managing information and records.

The new Information and Records Management Plan 2022-2025 will be based on the external audit scheduled to start 1 June 2022.

Attached is the draft Information and Records Management Plan 2022-2025 that will form the basis of this audit.

The Information and Records Management Plan is supported by Information and Records Management programme of work. A new programme of work will be prepared as part of the audit and Information and Records Management Plan 2022-2025.

Privacy Plan

Audit and plan status

Staff have been preparing the first Privacy Plan.
Central Otago customers need to have trust and confidence in the way Council manages its personal information. This plan has a close relationship with Cyber Security Plan, and Information and Records Management Plan.

The purpose of this Privacy Plan is to assess how Council currently protects customer's personal information and what actions it needs to undertake to improve that protection.

The next steps for the Privacy Plan is to be reviewed by the Executive Team.

Attached is the draft Privacy Plan, including the self-assessment carried out in early 2022. Further assessments will be carried out once the plan is finalised.

3. Attachments

Appendix 1 - ALGIM Cyber Security Programme Management Status Report ⇩
Appendix 2 - DRAFT Cyber Security Plan 2022-2024 ⇩
Appendix 3 - DRAFT Information and Records Management Plan 2022-2024 ⇩
Appendix 4 - DRAFT Privacy Plan ⇩

Report author:

Nathan McLeod
IS Manager

17/05/2022

Reviewed and authorised by:

Leanne Macdonald
Executive Manager - Corporate Services

18/05/2022

CENTRAL OTAGO
DISTRICT COUNCIL

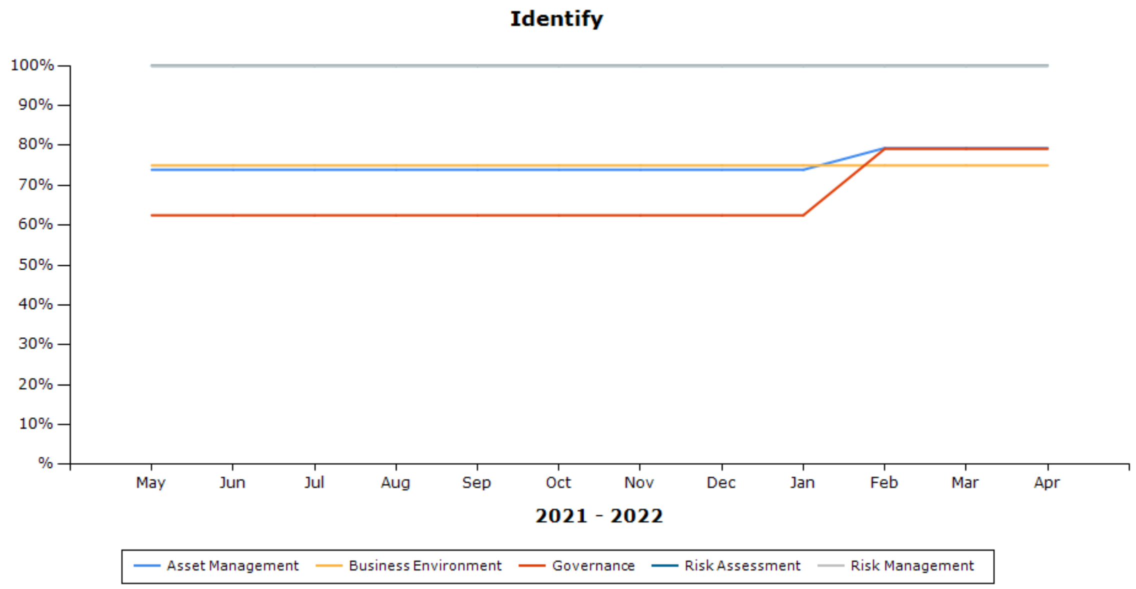
Management Status Report for Central Otago District Council

ALGIM Local Government Cybersecurity Programme as at 17 May 2022

🟥	🟥	🟧	🟨	🟩
0% - 5.00% complete	5.01% - 35.00% complete	35.01% - 65.00% complete	65.01% - 95.00% complete	95.01% - 100% complete

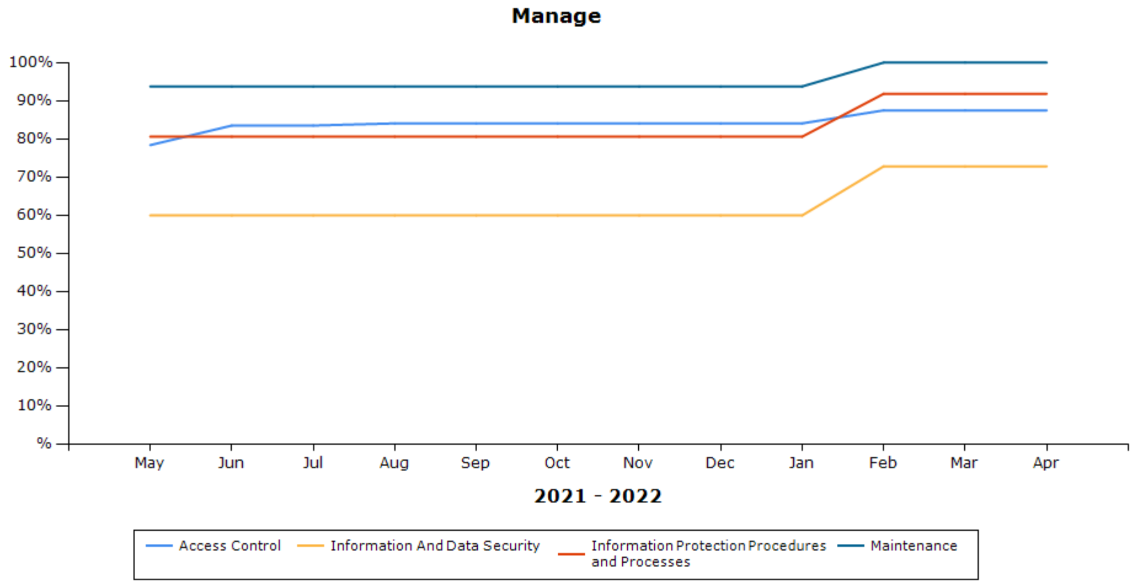
Identify - 81.95%

Function	Category	Description	Status
Identify (ID)	Asset Management (ID.AM)	Assets are managed consistent with their relative importance to business objectives and Council's risk management strategy	**79.35%**
	Business Environment (ID.BE)	The Council's mission, objectives, stakeholders and activities are understood and prioritised and this information is used to derive security roles, responsibilities and risk management decisions	**75.00%**
	Governance (ID.GV)	Management understand the importance of information and information systems and assign the appropriate cybersecurity roles and responsibilities	**79.17%**
	Risk Assessment (ID.RA)	Council understands the cyber security risk to operations, information, information systems assets and individuals	**100.00%**
	Risk Management (ID.RM)	Council's priorities, constraints and risk tolerances are established and documented within a Risk Management Strategy. This document is used to support operational risk decisions	**100.00%**



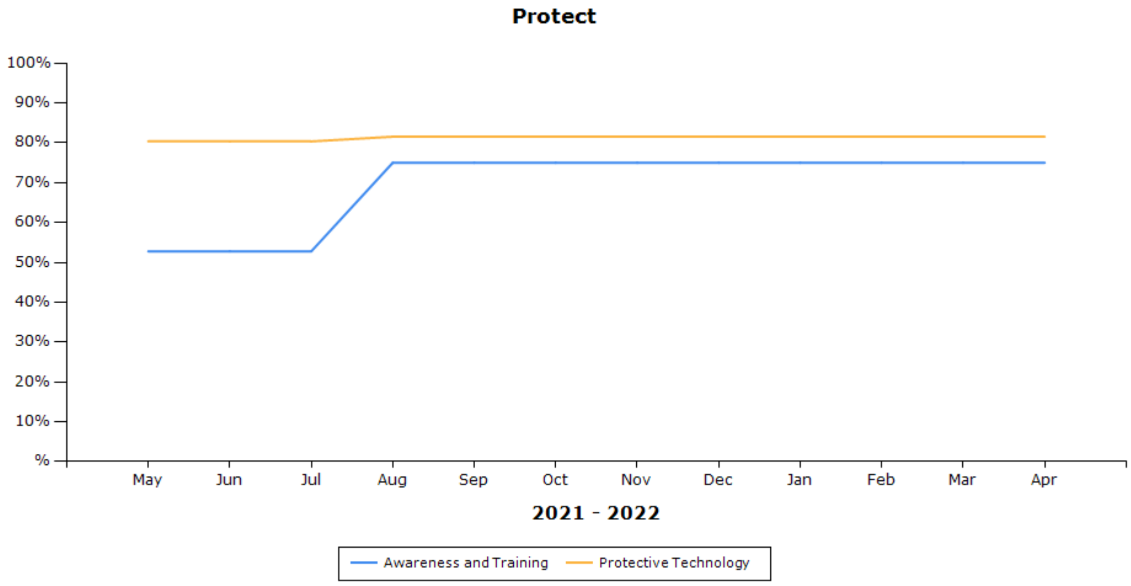
Manage - 85.61%

Function	Category	Description	Status
Manage (MN)	Access Control (MN.AC)	Access to assets and associated facilities is limited to authorised users, processes or devices and to authorised activities and transactions	**87.50%**
	Information And Data Security (MN.DS)	Information and records (data) are managed consistent with Council's risk strategy to protect the confidentiality, integrity and availability of information	**72.86%**
	Information Protection Procedures and Processes (MN.IP)	Information, assets and resources are protected through the implementation of effective procedures and processes	**91.84%**
	Maintenance (MN.MA)	Information systems and industrial control systems are maintained to ensure continuity of operations	**100.00%**



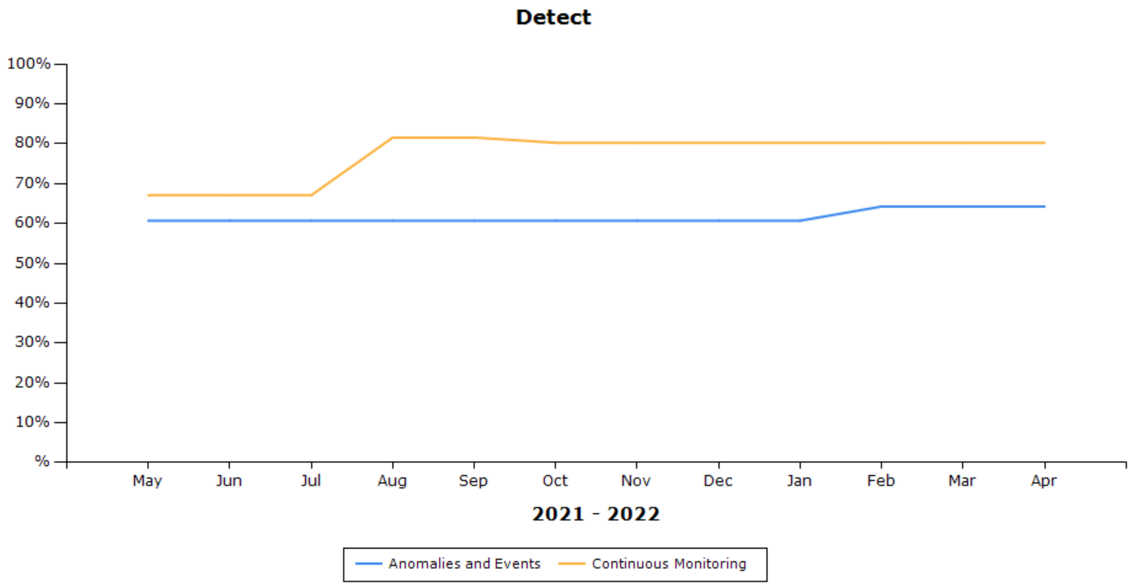
Protect - 80.39%

Function	Category	Description	Status
Protect (PR)	Awareness and Training (PR.AT)	Council personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security related duties and responsibilities consistent with related policies, procedures and agreements	**75.00%**
	Protective Technology (PR.PT)	Technology is implemented and managed to ensure the security and resilience of systems and assets	**81.55%**



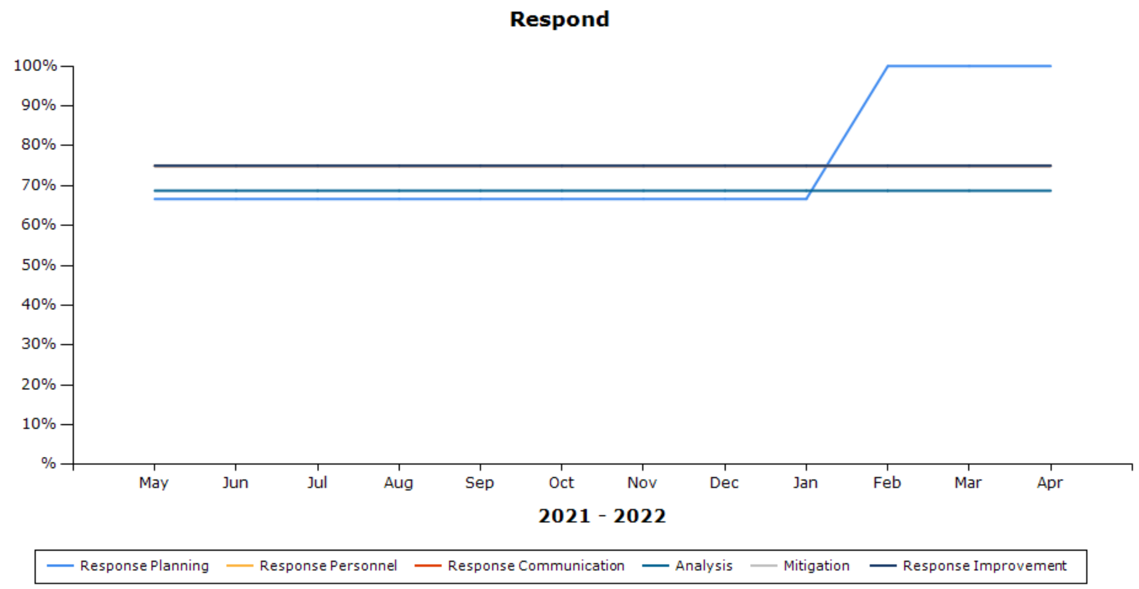
Detect - 75.96%

Function	Category	Description	Status
Detect (DE)	Anomalies and Events (DE.AE)	Anomalous activity is detected in a timely manner	**64.29%**
	Continuous Monitoring (DE.CM)	Information systems and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures	**80.27%**



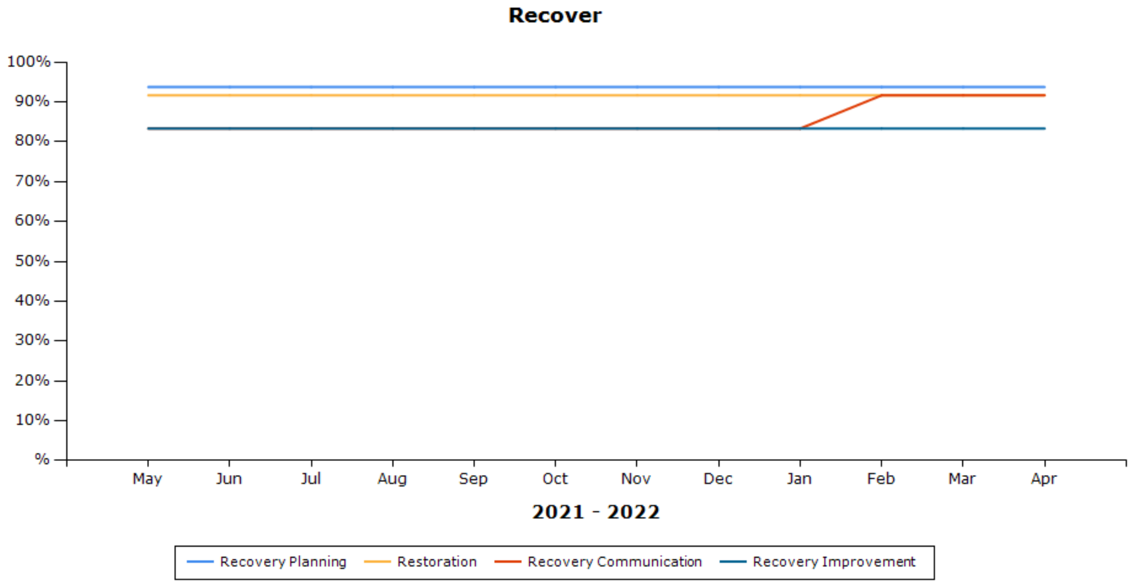
Respond - 77.17%

Function	Category	Description	Status
Respond (RS)	Response Planning (RS.RP)	Response documentation that ensures an appropriate response to incidents and events is available	**100.00%**
	Response Personnel (RS.PS)	Human resources with appropriate skill levels to successfully manage and mitigate an incident or event are available	**75.00%**
	Response Communication (RS.CO)	Response activities are co-ordinated with, and communicated to internal and external stakeholders, as appropriate, to include external support from law enforcement and regulatory agencies	**75.00%**
	Analysis (RS.AN)	Capability exists to carry out accurate analysis of an incident situation to ensure an appropriate response and actions	**68.75%**
	Mitigation (RS.MI)	Capability exists to effectively manage an event, prevent its expansion, mitigate its effects and eradicate residual content causing least impact to the organisation	**75.00%**
	Response Improvement (RS.IM)	Incident response capability subject to continuous improvement	**75.00%**



Recover - 90.39%

Function	Category	Description	Status
Recover (RC)	Recovery Planning (RC.PL)	Council has documentation available to support a successful recovery	**93.75%**
	Restoration (RC.RS)	Sufficient resources and facilities are available to facilitate a successful recovery operation	**91.67%**
	Recovery Communication (RC.RC)	Council is able to minimise any negative impacts caused by an incident or event	**91.67%**
	Recovery Improvement (RC.RI)	Recovery capabilities are subject to continuous improvement	**83.34%**



CENTRAL OTAGO
DISTRICT COUNCIL

1 Dunorling Street
PO Box 122, Alexandra 9340
New Zealand

03 440 0056

Info@codc.govt.nz
www.codc.govt.nz

Cyber Security Plan 2022-2025

Department	Information Services
Final (PDF) Doc ID:	Insert CentralDocs Doc ID
Final Versions:	Insert CentralDocs version URL
Draft (Word) Doc ID:	558511
Draft Versions:	https://cdocs.codc.govt.nz/Versions.aspx?DocumentID=558511
Approved by:	Executive Team, Audit and Risk
Effective date:	Month 2022
Next review:	Month 2025

Table of Contents

Introduction

Purpose

Cyber security's core function is to protect all council users of council information, and information systems, including personal information. This plan has a strong relationship with Council Privacy Plan and Information and Records Management Plan.

The purpose of this cyber security plan is to assess how Council currently protects Council's information and information systems and what actions it needs to undertake to improve that protection.

Scope

The Cyber Security Plan is supported by Council's Digital and Information Strategy, Cyber Security Policy, and standards, which cover the protection of information and information systems.
This plan ensures Council is adhering to the requirements outlined in Council's information and information systems standards.
Information Services (IS) is responsible for the management and implementation of this plan.

Why information security matters

Council relies on the confidentiality, integrity, and availability of the information it processes, stores, and communicates.

Robust information security is a business enabler.
Strong information security helps Council to:

- Maintain the trust and confidence of the public, customers, and partners
- Keep Councils important information safe and available to those who need it
- Reduce the risks of Council information being lost, damaged, or compromised
- Provides confidence around Council's ability to operate effectively and safely in an increasing digital world
- Allows Council the potential to introduce new services and features when coming from a robust security base
- Avoid costs of recovery after an incident, as well as costs of downtime and lost productivity
- Comply with regulation and legislation
- Allows Council to 'lead by example'

Threats and risks are increasing and evolving.
Threats to the security of Councils information can come from inside and outside Council. Council information in all forms (for example, digital, printed or spoken) needs to be appropriately protected.

Information stored and processed on Council information systems or mobile devices is vulnerable to cyber-specific threats:

- Council is far more exposed today than ever before
- Council have increasing quantities of digital information, and we are heavily dependent on it to function
- Council has cloud, social media, mobile, and other emerging technologies, which have increased the ways critical information can be accessed
- Council faces increasing and continually evolving threats that make detection challenging.

External actors and disgruntled insiders have been known to:

- Expose or publish sensitive information in the public domain
- Encrypt and then ransom critical information
- Sell information to competitors and interested parties
- Steal intellectual property (IP)
- Compromise organisations by destroying or denying access to records.

Council staff may also accidentally compromise Council information because they:

- Lack awareness of your security practices and why they're important
- Get distracted or complacent while handling Council's information
- May feel their own need for ease of access and/or use, override the need for good security practices and procedures
- Provide access to other parties seeking information for criminal or other inappropriate purposes. For instance, 'social engineering' attacks attempt to manipulate people into breaking normal security controls, often disguising themselves as someone trusted through phishing, pretexting, baiting, quid pro quo, and tailgating or other means

Cyber Security Culture

Everyone in Council needs to be part of our cyber security culture, otherwise security processes and tools won't be as effective.

It only takes one malicious email attachment to potentially compromise Council. Council needs to make sure our people and partners:

- Understand the security risks
- Understand your information security policies
- Adopt the right security behaviours

To get everyone on board, it is critical to provide security awareness training and ongoing support. It is also vital to continually check and challenge staff behaviours to ensure that a good level of security awareness is being maintained and used on a day-to-day basis.

Relevant Legislation

- Intelligence and Security Act 2017
- Privacy Act 2020
- Public Records Act 2005
- Local Government Official Information and Meetings Act 1987
- Official Information Act 1982
- Evidence Act 2006
- Electronic Transactions Act 2002
- Health and Safety at Work Act 2015

Related Documents

- Digital and Information Strategy
- Cyber Security Policy
- Privacy Policy
- Protection of Information and Information Standards

Cyber Security Incidents

Cyber security incidents will be treated as a Critical Incident as outlined within our Incident and Problem Management Procedure.

Standards

Council has chosen to the following standards for the protection of information and information systems:

Standard	Purpose
Acceptable Use Standard	The purpose of this Acceptable User Standard (standard) is to outline the acceptable use of information system assets and information. Information system assets include any equipment or service provided by the Council that can be used for communication or to create, process, reproduce or distribute information. Examples include but are not limited to: • desktop computers • laptops • network shares • document management systems • email systems • instant messaging (IM) systems • internet connections • mobile devices including phones and tablets • printers • plotters • fax machines • telephones and cell phones • portable storage devices (USB) • Council purchased Cloud services • Council moderated Social Media services
Access Control Standard	The purpose of this Standard is to ensure that access to assets and associated facilities is limited to authorised users, processes, or devices and to authorised activities and transactions.
Anomalies and Event Identification Standard	The purpose of this Standard is to ensure that anomalous activity is detected in a timely manner.
Asset Management Standard	The purpose of this Standard is to ensure that Assets are managed consistent with their relative importance to business objectives and the Council's risk strategy.
Awareness and Training Standard	The purpose of this Standard is to ensure that personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security related duties and responsibilities consistent with related policies, standards, procedures, and agreements.
Continuous Monitoring Standard	The purpose of this Standard is to ensure that information systems and assets are monitored at discrete intervals to identify cyber security events and verify the effectiveness of protective measures.
Data Security Standard	The purpose of this Standard is to ensure that information systems and assets are monitored at discrete intervals to identify cyber security events and verify the effectiveness of protective measures.

Standard	Purpose
Governance Standard	The purpose of this Standard is to ensure that Council's business environment is understood, and that policies, standards, procedures, and processes are established to manage and monitor performance so that activities are conducted in accordance with regulatory, legal, risk, environmental and operational requirements. Risks to business assets and individuals are understood and Council's priorities, constraints and risk tolerances are established, documented, and used to support operational risk decisions.
Information Protection Standard	The purpose of this Standard is to ensure that information, assets, and resources are protected through the implementation of effective procedures and processes.
Maintenance Standard	The purpose of this Standard is to ensure that information systems and industrial control systems are maintained to ensure continuity of operations.
Protective Technology Standard	The purpose of this Standard is to ensure that Technology is implemented and managed to ensure the security and resilience of systems and assets.
Recovery Management Standard	The purpose of this Standard is to ensure that Council has appropriate documentation, resources, and facilities to support an information systems recovery operation.
Response Management Standard	The purpose of this Standard is to ensure that Council has adequate documentation and resources available to successfully manage and mitigate a cybersecurity incident or event and that the incident response capability is subject to continuous improvement.
Response Operations Standard	The purpose of this Standard is to ensure that incidents are reported in a timely manner and internal and external stakeholders remain informed. Accurate analysis of an incident is carried out to ensure an appropriate response and remediation operations minimise the impact to Council.

Cyber Security Risk

Information Services manages it's risks as per the Risk Management Policy. Risk management forms of Information Services Activity Management Plan.
For a detailed view of the Information Services Risk Register (Doc ID: 447956), please click here.
The following is an extract from the Information Services Risk Register:

Risk description	Risk driver	Risk consequence	Residual risk	Risk management plan/control
Cyber Security Risks are being reviewed by the external auditor. The risk register and plan will be updated following the review.				

Information Security Risk Review and Framework

Council has chosen to undertake an independent information security risk review by an external party every 3 years. This is the second such review and will be undertaken by SAM for Compliance Ltd, who provides professional services in New Zealand, Australia, and the United States to support governance, risk reduction and compliance activities.

Review Methodology

The information security operational risk review has been undertaken using the Center for Internet Security (CIS) Critical Security Controls as a base standard for establishing the level of information system operational risk.

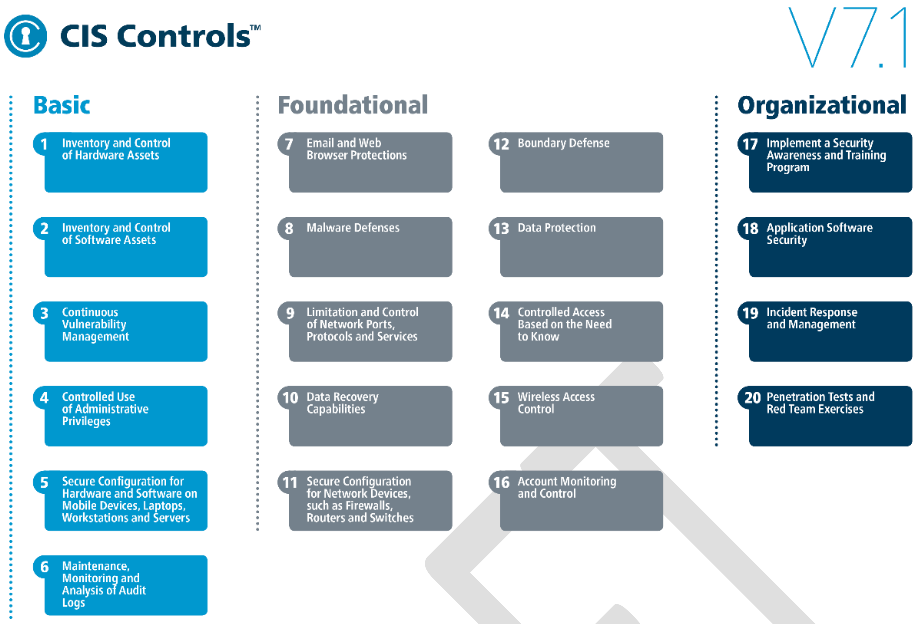
Developed from the SAN Top 20 Controls, the CIS Critical Security Controls (CIS Controls) are a concise, prioritised set of cyber practices created to stop today's most pervasive and dangerous cyber-attacks.

The CIS Controls are developed, refined, and validated by a community of leading experts from around the world with input from information security technology providers, Council agencies and information security practices.

The CIS Critical Security Controls have been developed from information gathered from actual attacks, information leakage incidents, loss of service incidents, and evidence of effective defences where these have prevented incidents from occurring. These together reflect the combined knowledge of experts within many sectors who have banded together to create, adopt, and support the Controls.

Top experts from organisations have pooled their extensive first-hand knowledge to evolve the consensus list of Controls, representing the best defensive techniques to prevent incursion and loss or corruption of information.

Each requirement within the CIS Controls therefore is a direct response to known and identified threat and is only included if it is proven in practice to minimise threat level.



CIS Controls™ V7.1

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

The CIS Controls embrace the Pareto 80/20 Principle, the idea that taking just a small portion of all the security actions an organisation could possibly take, yields a very large percentage of the benefit of taking all those possible actions.

The CIS Controls complement strategic information security standards such as the ISO27001/ISO27002, however, unlike the ISO series of standards which have a long gestation period between updates (being typically 5-8 years), CIS Controls updates are responsive to current threat levels.

This review also takes into consideration the requirements of the National Institute of Standards and Technology (NIST) Cyber Security Framework as a means of determining the effectiveness of protecting nationally sensitive information.

Also incorporated in are other checks for operational risk because of previous experience of the risk reviewer in identifying areas in similar Council organisations where a failure to implement effective procedures, processes and checks has been shown to make a system be susceptible to compromise.

When examining the level of risk to systems, information, and the Council operational requirements we take into consideration deliberate attack from external agents, deliberate attack from internal staff or associated third parties, inadvertent “attack” by staff or associated third parties, effects of natural disaster and system or service failures.

Irrespective of the source, any ability to compromise, modify, extract, destroy or restrict access to information systems and the information stored or transmitted across those systems has been a risk.

The network environment was scanned using several open source and commercially available tools to assess the level of vulnerability present on Council owned systems.

Sample testing will be performed against several internal and external systems to identify if stated controls do in fact exist or where common errors in configuration or operation are known to create opportunities for risk.

When considering the risk levels that may be present in the organisation, the reviewer takes into consideration the key functions associated with the effective management and protection of information and systems used to protect that information.

ALGIM Cybersecurity Programme

Association of Local Government Information Management (ALGIM) has defined a Cyber Security framework which is powered by SAM for Compliance giving councils the ability to manage and reduce organisational Cyber Security related risk. As part of the programme, councils that demonstrate defined levels of achievement and improvement will receive awards at the ALGIM annual conference.

Framework Functions and Categories

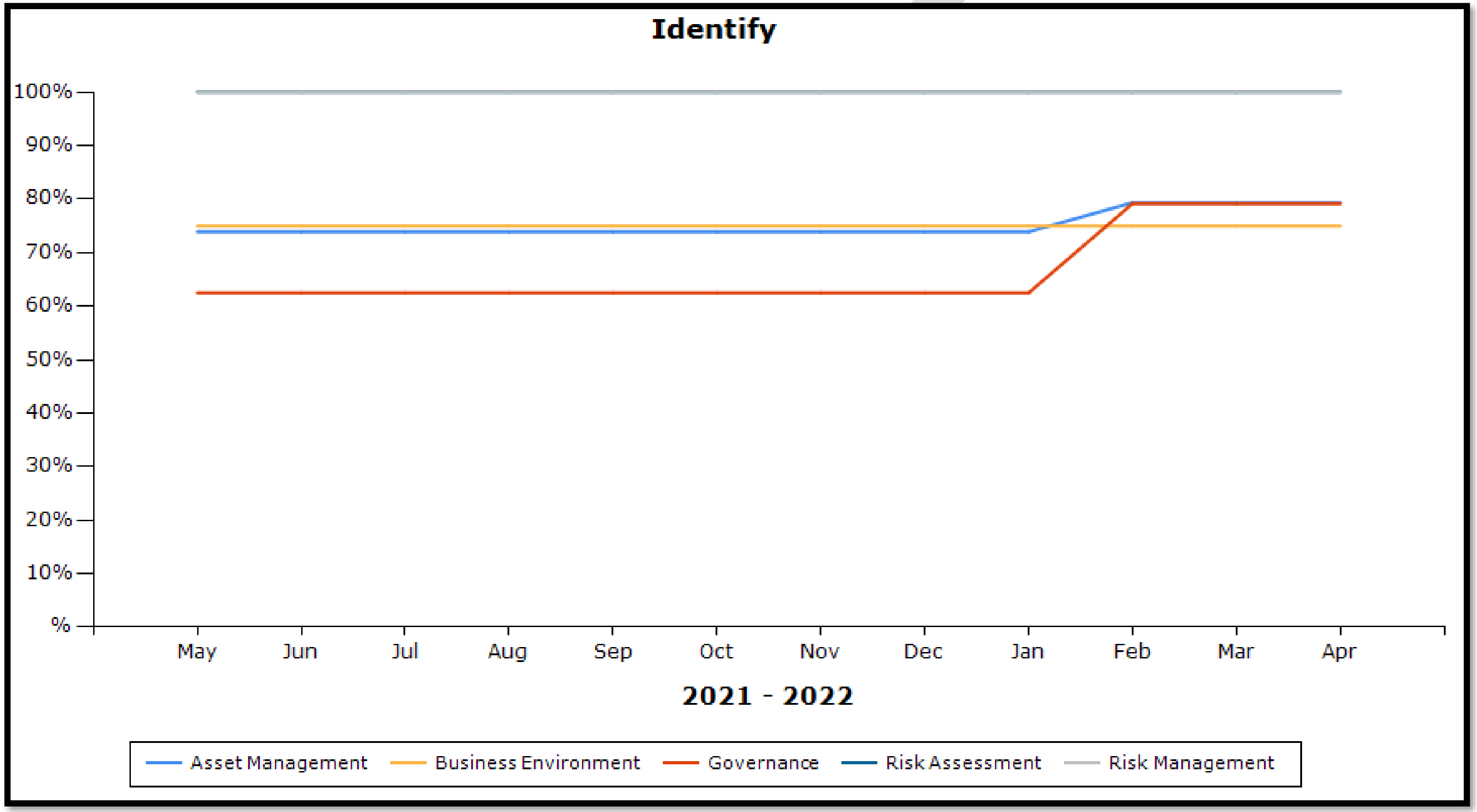
Function	Scope	Category	Description
Identity	The organisation should have effective governance over its systems and should understand its own operational environment. It should have the ability to assess risks associated with its information systems and be able to manage that risk.	**Asset Management**	Assets are managed consistent with their relative importance to business objectives and Council's risk management strategy
		Business Environment	The Council's mission, objectives, stakeholders, and activities are understood and prioritised and this information is used to derive security roles, responsibilities, and risk management decisions
		Governance	Management understands the importance of information and information systems and assign the appropriate cybersecurity roles and responsibilities.
		Risk Assessment	Council understands the cyber security risk to operations, information, information systems assets and individuals.
		Risk Management	Council's priorities, constraints and risk tolerances are established and documented within a Risk Management Strategy. This document is used to support operational risk decisions.
Manage	The organisation should have information protection procedures and processes in place. It should be able to manage access control and data security and should also have systems in place for appropriate maintenance of its systems and assets.	**Access Control**	Access to assets and associated facilities is limited to authorised users, processes, or devices and to authorised activities and transactions.
		Information and Data Security	Information and records (data) are managed consistent with Council's risk strategy to protect the confidentiality, integrity, and availability of information.
		Information Protection Procedures and Process	Information, assets, and resources are protected through the implementation of effective procedures and processes.
		Maintenance	Information systems and industrial control systems are maintained to ensure continuity of operations

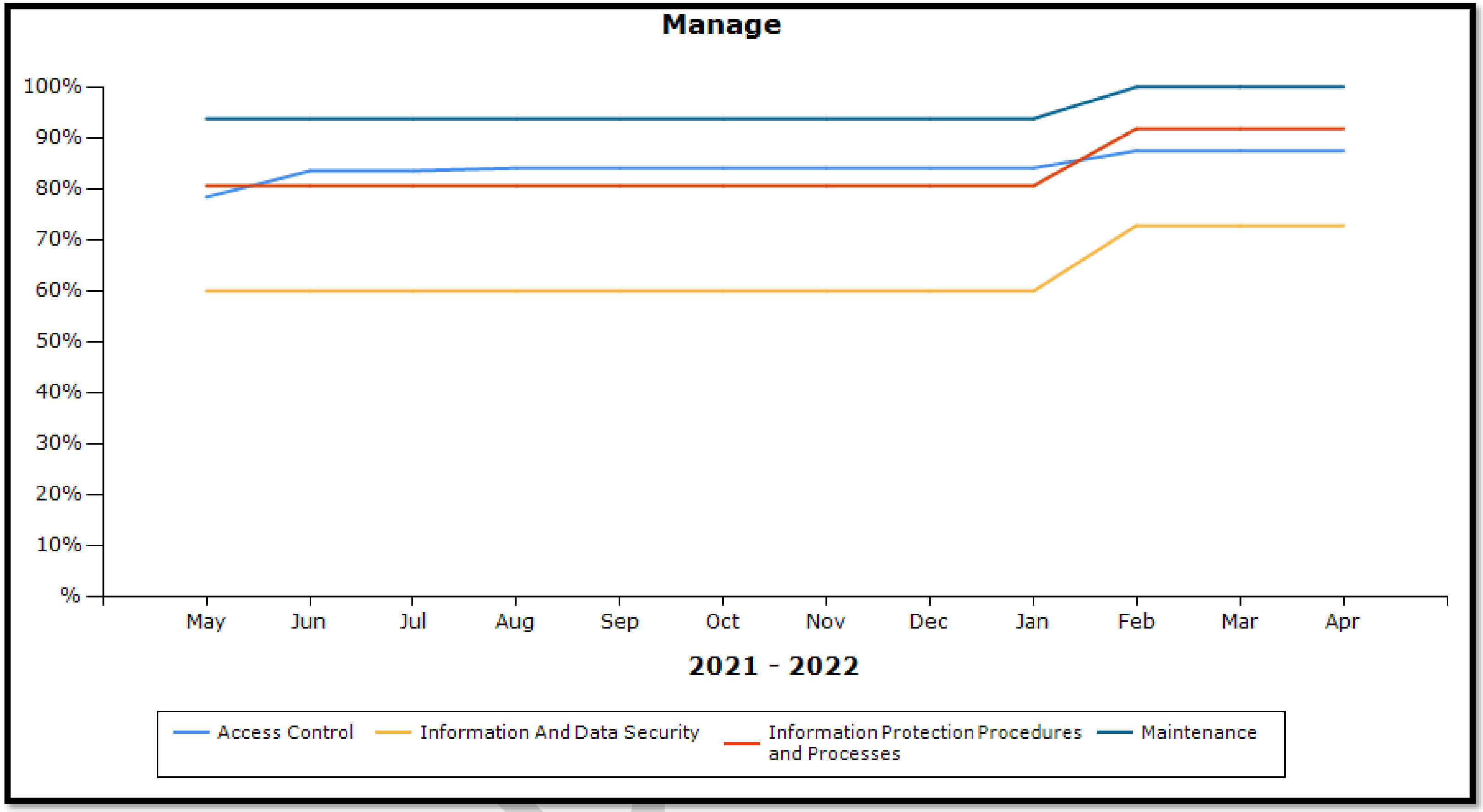
Function	Scope	Category	Description
Protect	The organisation should have protective technology in place to minimise risk associated with external and internal threats and should have processes to increase awareness and provide training to staff.	**Awareness and Training**	Council personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security related duties and responsibilities consistent with related policies, procedures and agreements.
		Protective Technology	Technology is implemented and managed to ensure the security and resilience of systems and assets.
Detect	The organisation should have systems in place to detect anomalies and events. These systems should provide continuous monitoring and appropriate processes should be in place to enable effective use of the information provided by the detection systems.	**Anomalies and Events**	Anomalous activity is detected in a timely manner.
		Continuous Monitoring	Information systems and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
Respond	The organisation should have plans in place to be able to respond to events. Analysis tools should be available and trained personnel should be available to use these tools to mitigate the effects of the events.	**Response Planning**	Response documentation that ensures an appropriate response to incidents and events is available.
		Response Personnel	Human resources with appropriate skill levels to successfully manage and mitigate an incident or event are available.
		Response Communication	Response activities are co-ordinated with, and communicated to internal and external stakeholders, as appropriate, to include external support from law enforcement and regulatory agencies.
		Analysis	Capability exists to carry out accurate analysis of an incident situation to ensure an appropriate response and actions.
		Mitigation	Capability exists to effectively manage an event, prevent its expansion, mitigate its effects, and eradicate residual content causing least impact to the organisation.

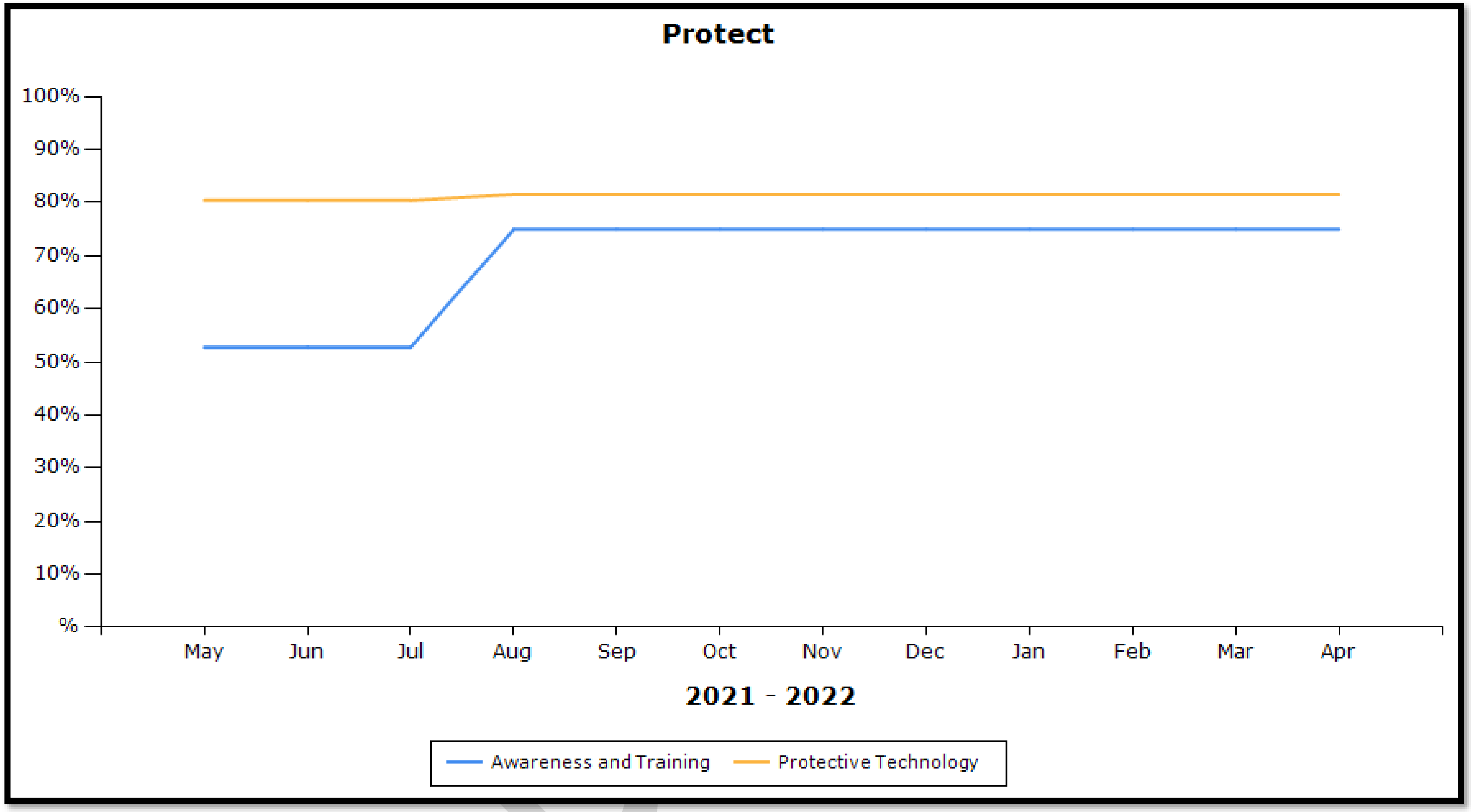
Function	Scope	Category	Description
		Response Improvement	Incident response capability subject to continuous improvement.
Recover	The organisation should have systems and processes in place for it to be able to recover from an event, and these should be supported by effective event response plans. There should be processes and systems in place to facilitate restoration of information and systems and there should also be a process to improve the capabilities of the organisation following an event.	**Recovery Planning**	Council has documentation available to support a successful recovery.
		Restoration	Sufficient resources and facilities are available to facilitate a successful recovery operation.
		Recovery Communication	Council can minimise any negative impacts caused by an incident or event.
		Recovery Improvement	Recovery capabilities are subject to continuous improvement.

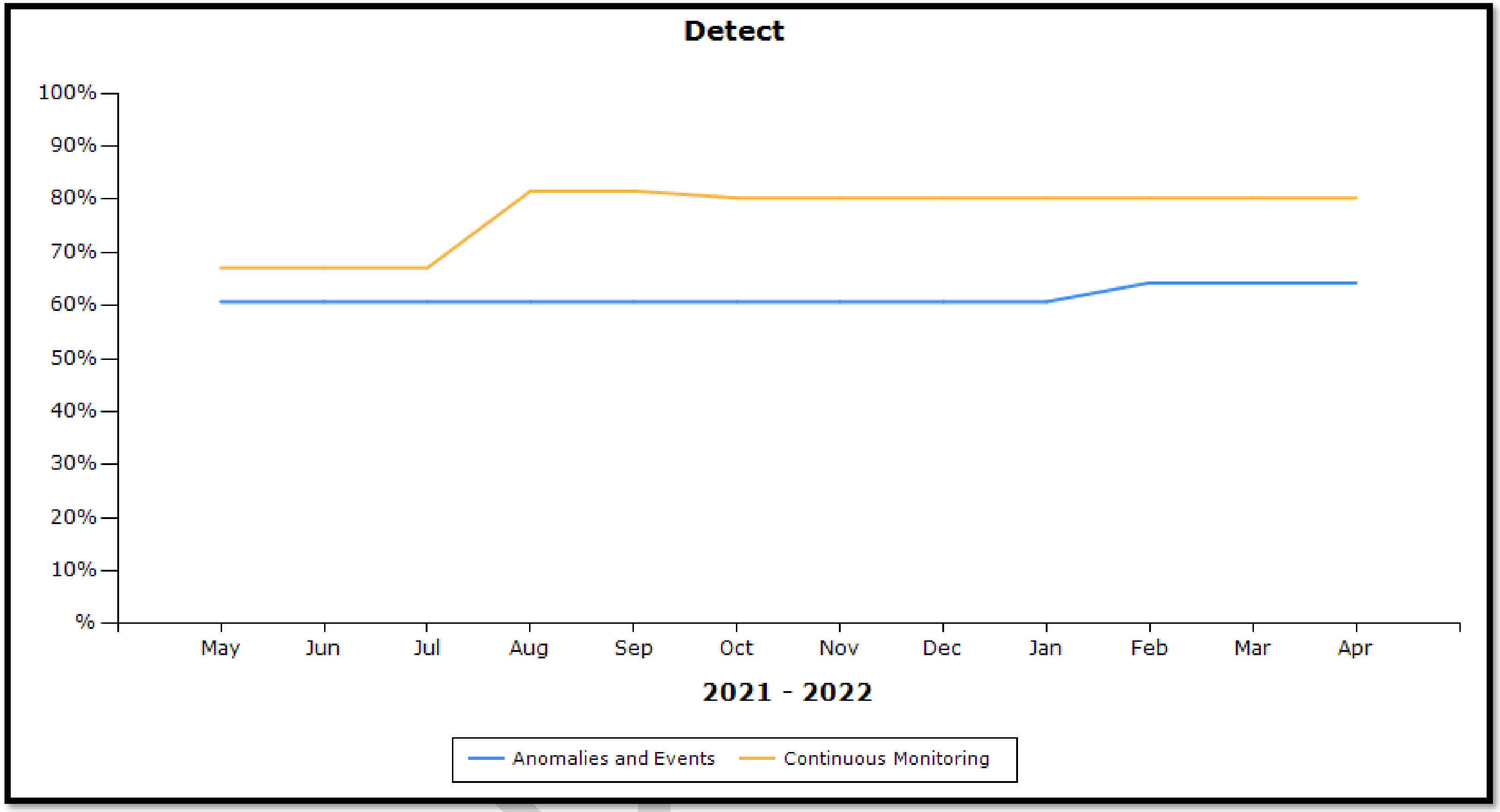
Current state by Functions and Categories

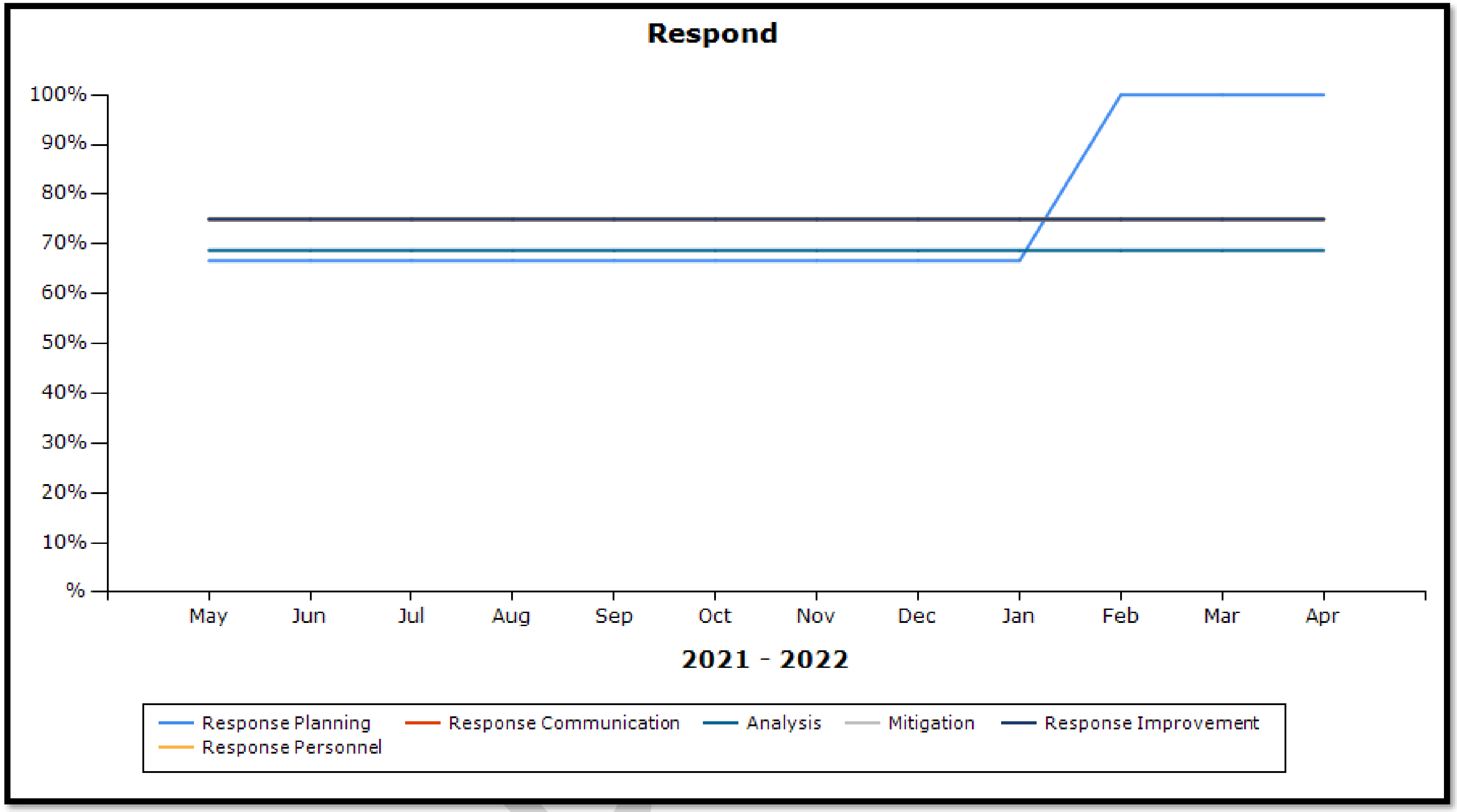
The following is the trends and current state by the Functions and Category of the Framework since the last review in May 2018:



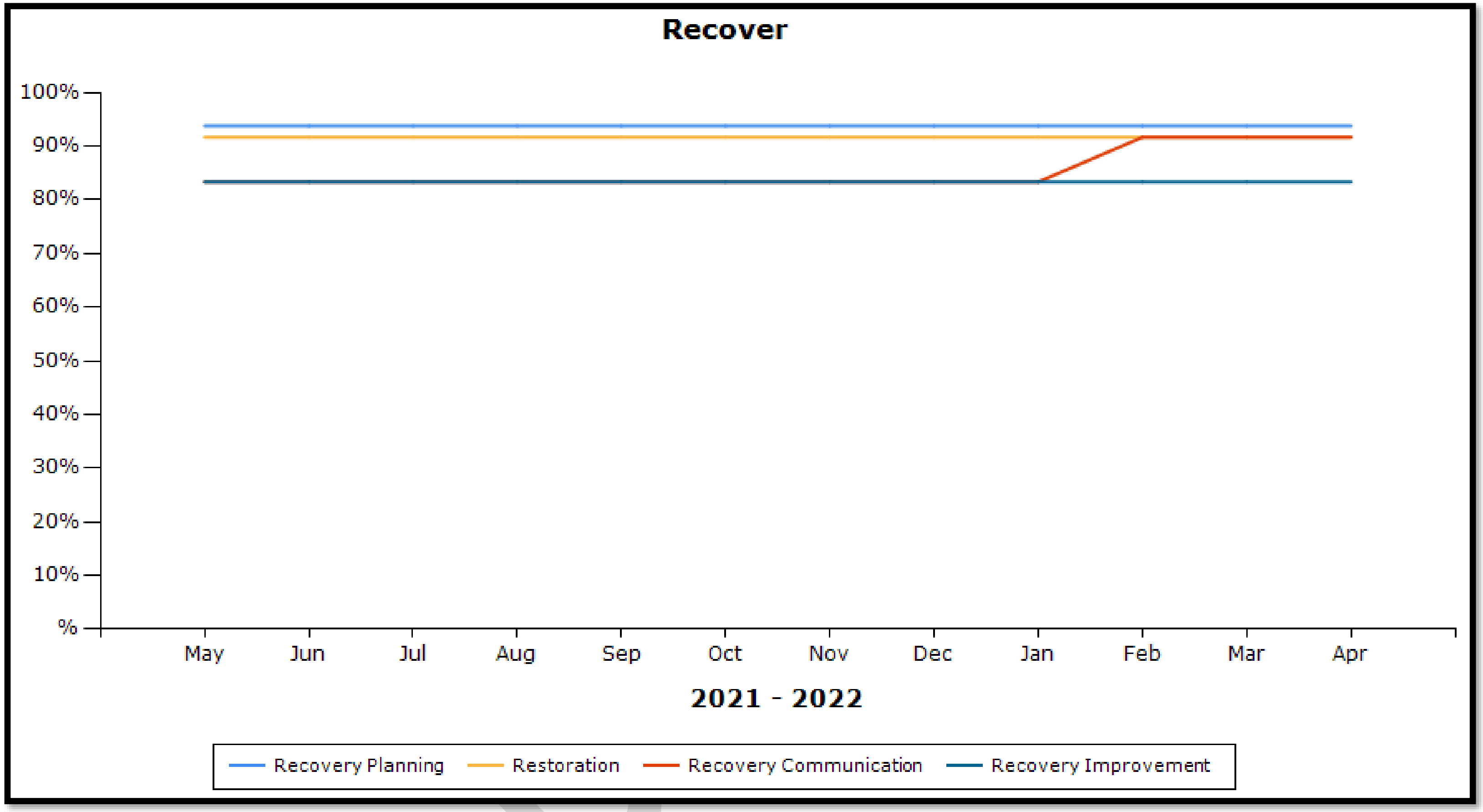

Manage
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
%
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
2021 - 2022
Access Control
Information And Data Security
Information Protection Procedures and Processes
Maintenance


Protect
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
%
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
2021 - 2022
Awareness and Training
Protective Technology


Detect
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
%
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
2021 - 2022
Anomalies and Events
Continuous Monitoring


Respond
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
%
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
2021 - 2022
Response Planning
Response Communication
Analysis
Mitigation
Response Improvement
Response Personnel

Page **18** of **25**


Recover
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
%
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
2021 - 2022
Recovery Planning
Restoration
Recovery Communication
Recovery Improvement

Actions

Action management and reporting on progress will occur within the SAM for Compliance - compliance management tool. Tasking of these actions will occur within the IS Portal.

The following is a summary of the actions at the time of preparing this plan, including recommendations from the information security risk review. The actions are grouped by the functions and categories of the ALGIM Cybersecurity Programme Framework.

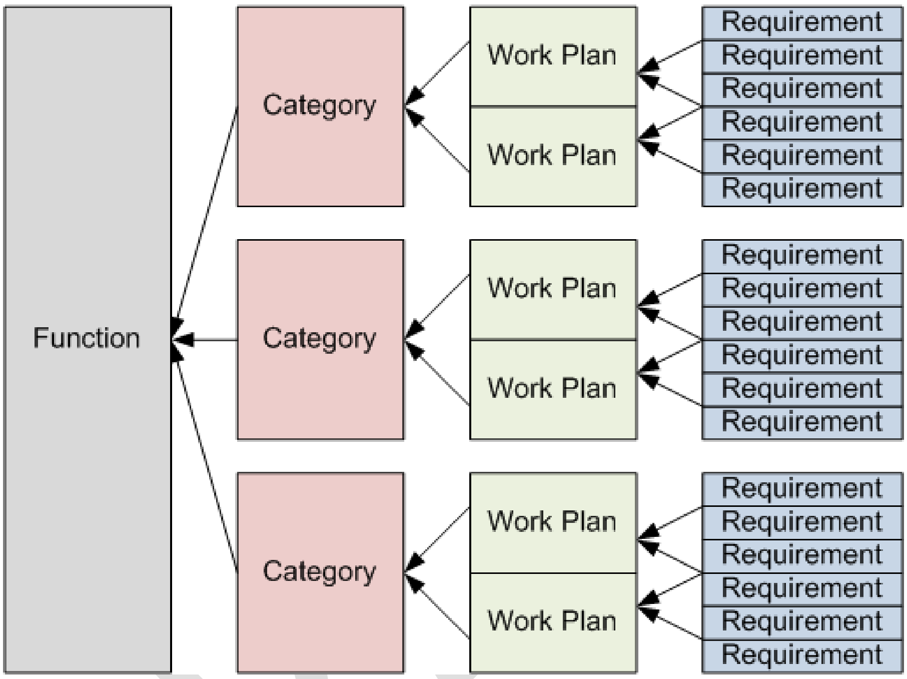
Status key: Not Started, Started, Partially Completed, Mostly Completed, Fully Completed

Function	Category	Actions	Responsibility	Due Month/Year	Status	Notes
Identity	Asset Management	Actions will be populated following the external audit.				
	Business Environment					
	Governance					
	Risk Assessment					
	Risk Management					
Manage	Access Control					
	Information and Data Security					
	Information Protection Procedures and Process					
	Maintenance					
Protect	Awareness and Training					

Function	Category	Actions	Responsibility	Due Month/Year	Status	Notes
	Protective Technology					
Detect	Anomalies and Events					
	Continuous Monitoring					
Respond	Response Planning					
	Response Personnel					
	Response Communication					
	Analysis					
	Mitigation					
	Response Improvement					
Recover	Recovery Planning					
	Restoration					
	Recovery Communication					
	Recovery Improvement					

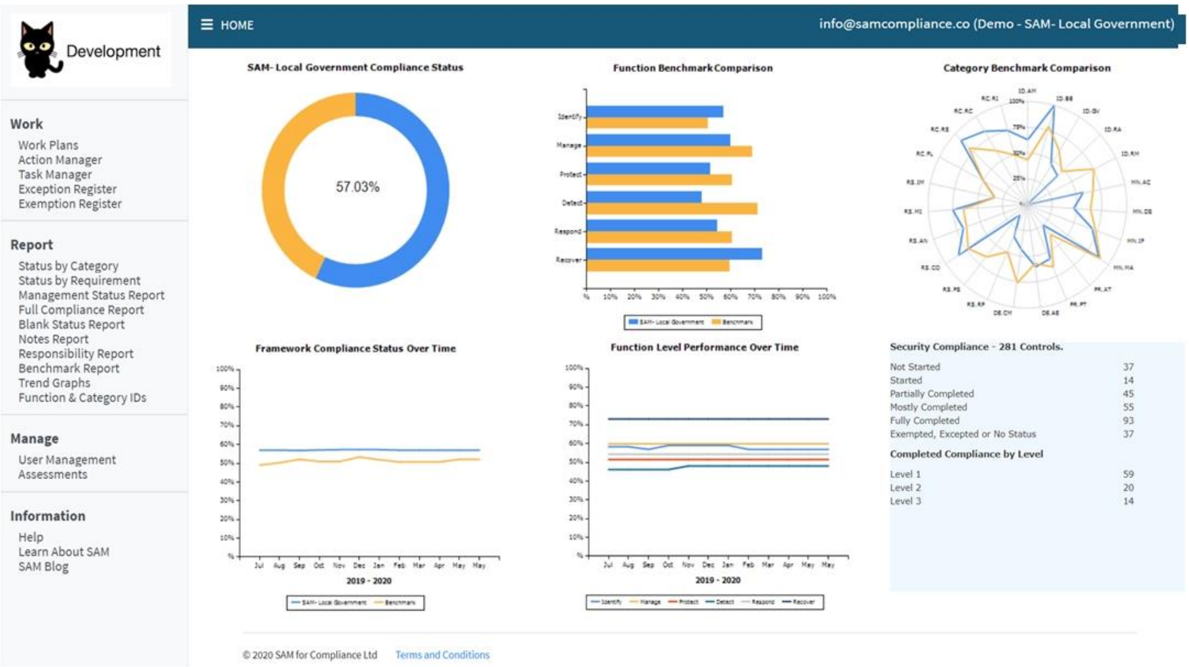
Compliance Management

Council has chosen to utilise SAM for Compliance. SAM for Compliance is a compliance management tool which can be applied to any standard or framework that is comprised of specific requirements or controls. SAM for Compliance contains frameworks which are broken down into key performance areas based on the NIST CSF model of Framework, Function, Category, Sub-Category and Controls.



SAM for Compliance relies on self-assessment to ascertain the current compliance status. The system simply calculates totals based on Council input.

The controls are assessed based on a pre-defined maturity model individual to each framework instance and dynamically update the dashboard view and all system reports.



Development
HOME
info@samcompliance.co (Demo - SAM- Local Government)
SAM- Local Government Compliance Status
57.03%
Function Benchmark Comparison
Identify
Manage
Protect
Detect
Respond
Recover
SAM- Local Government
Benchmark
Category Benchmark Comparison
Framework Compliance Status Over Time
2019 - 2020
Function Level Performance Over Time
Identify
Manage
Protect
Detect
Respond
Recover

Work
- Work Plans
- Action Manager
- Task Manager
- Exception Register
- Exemption Register

Report
- Status by Category
- Status by Requirement
- Management Status Report
- Full Compliance Report
- Blank Status Report
- Notes Report
- Responsibility Report
- Benchmark Report
- Trend Graphs
- Function & Category IDs

Manage
- User Management
- Assessments

Information
- Help
- Learn About SAM
- SAM Blog

Security Compliance - 281 Controls.

Not Started	37
Started	14
Partially Completed	45
Mostly Completed	55
Fully Completed	93
Exempted, Excepted or No Status	37

Completed Compliance by Level

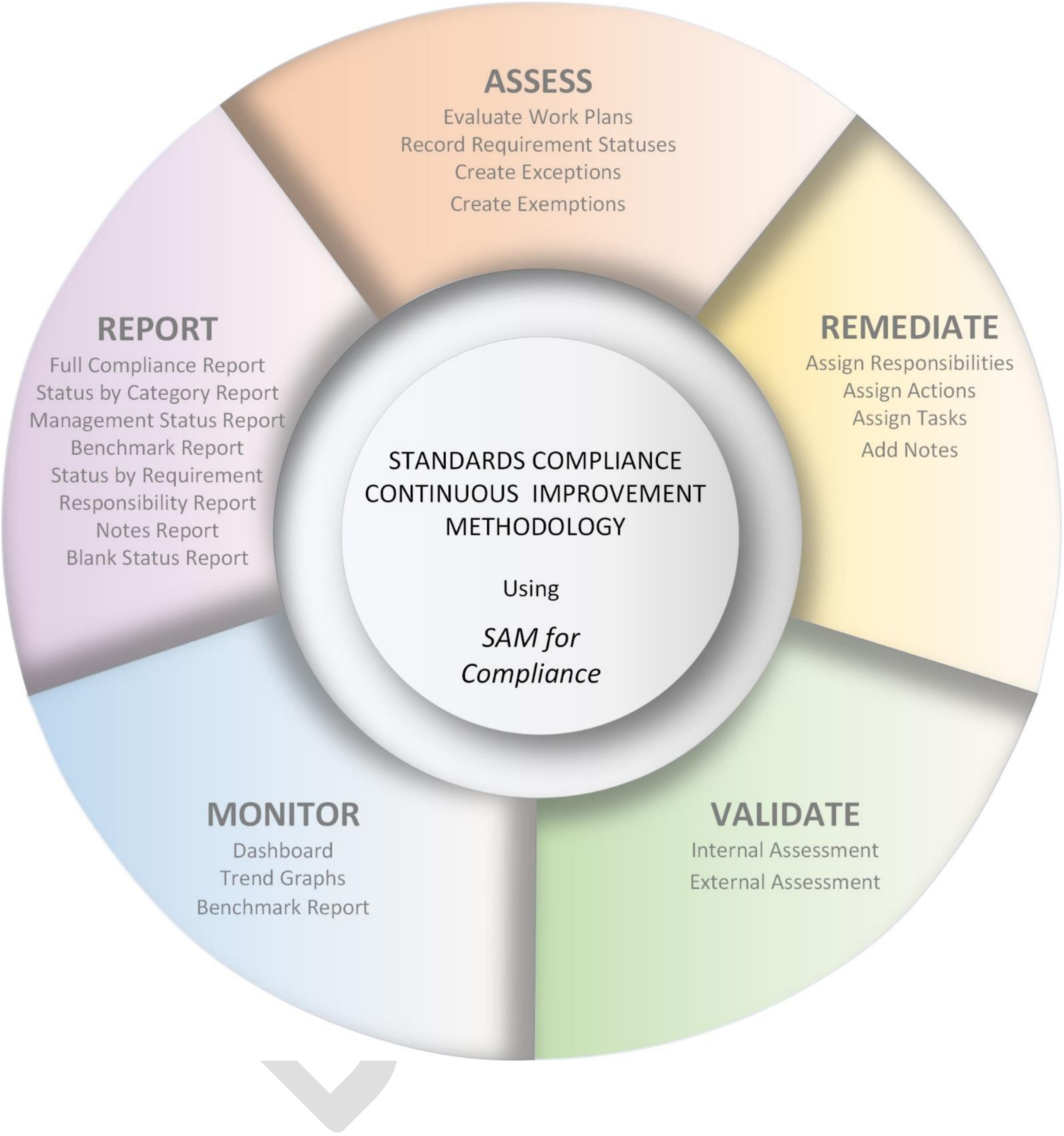
Level 1	59
Level 2	20
Level 3	14

© 2020 SAM for Compliance Ltd Terms and Conditions

SAM Management Methodology

The SAM for Compliance tool consists of functions that assist you to manage compliance to your chosen framework as demonstrated by the features on the colour wheel below:

- **ASSESS -** Evaluate and record your status against your chosen maturity model, including Exceptions and Exemptions
- **REMEDIATE -** Assign responsibilities for achieving compliance with controls, assign Actions and Tasks and add Notes to record specific details or links to other documents
- **VALIDATE** - Assessment function
- **MONITOR** - View your current Status from our dynamic, multi-chart Dashboard and Trend graphs. View benchmark comparisons against your Peer Group (where applicable)
- **REPORT** - Report your current Status


ASSESS
Evaluate Work Plans
Record Requirement Statuses
Create Exceptions
Create Exemptions
REMEDIATE
Assign Responsibilities
Assign Actions
Assign Tasks
Add Notes
VALIDATE
Internal Assessment
External Assessment
MONITOR
Dashboard
Trend Graphs
Benchmark Report
REPORT
Full Compliance Report
Status by Category Report
Management Status Report
Benchmark Report
Status by Requirement
Responsibility Report
Notes Report
Blank Status Report
STANDARDS COMPLIANCE
CONTINUOUS IMPROVEMENT
METHODOLOGY
Using
SAM for
Compliance

Page **24** of **25**

Reporting

Reporting on the progress of this plan will occur as follows:

Who	What	When
Audit and Risk Committee	An information report will be prepared, including the following topics: • **What is happening in New Zealand?** *Council utilise Computer Emergency Response Team (CERT) as a resource for cyber security support. CERT NZ works to support businesses, organisations and individuals who are affected (or may be affected) by cyber security incidents. CERT provide trusted and authoritative information and advice, while also collating a profile of the threat landscape in New Zealand.* • **What is happening at Central Otago District Council?** *The following outlines what Council protective technologies are doing for the x-to-x period.* • **ALGIM Cyber Security Programme update** *Association of Local Government Information Management (ALGIM) has defined a Cyber Security framework which is powered by SAM for Compliance giving councils the ability to manage and reduce organisational Cyber Security related risk. As part of the programme, councils that demonstrate defined levels of achievement and improvement will receive awards at the ALGIM annual conference.* *The latest Management Status Report is attached for your information (Appendix 1).* *The following details the current snapshot of how Council is preforming within this framework benchmarked against other Councils:* • **Cyber Security programme of work update by actions** *The following is a summary of the actions as agreed within the cyber security plan 2022-2024. The actions are grouped by the functions and categories of the ALGIM Cybersecurity Programme Framework.*	Quarterly
Executive Team		Quarterly

CENTRAL OTAGO
DISTRICT COUNCIL

1 Dunorling Street
PO Box 122, Alexandra 9340
New Zealand

03 440 0056

Info@codc.govt.nz
www.codc.govt.nz

Information and Records Management Plan 2022-2025

Department	Information Services
Final (PDF) Doc ID:	Insert CentralDocs Doc ID
Final Versions:	Insert CentralDocs version URL
Draft (Word) Doc ID:	558664
Draft Versions:	https://cdocs.codc.govt.nz//Versions.aspx?DocumentID=558664
Approved by:	Executive Team, Audit and Risk
Effective date:	Month 2022
Next review:	Month 2025

Table of Contents

Introduction

Purpose

The purpose of this information and records management plan is to assess how Council currently manages its information and records and what actions it needs to undertake to improve that management.

Information and records are key strategic assets of an organisation. These assets need to be actively managed to maintain and improve value. Information and records management assets take many forms, including data and business systems. Our digital and information strategy and this information and records management plan will guide Council to make its current operations more effective by managing information and records.

Scope

The Information and Records Management Plan is supported by Council's digital and information strategy, and information and records management policy, which covers:

- Council's responsibility for managing information and records
- Information and records support the business
- Management of information and records

This plan ensures Council is adhering to the requirements outlined in the Public Records Act 2005 Information and Records Management Standards 2016.

Our ability to respond to LGOIMA Requests efficiently and effectively is impacted by our information and records management practices, LGOIMA Requests actions have been included in this plan.

Privacy is an important consideration of information and records management practices; our Privacy Plan should be referred to for privacy-related actions.

Information Services (IS) are responsible for the management and implementation of this plan.

Key Concepts

Key concept	Definition
What are public, local authority and protected records?	Public records: • records or a class of records, created or received by a public office as it carries out its functions. Local authority records: • records or a class of records, created or received by a local authority as it carries out its functions. Protected records: • records created by local authorities that have been declared under section 40 of the PRA to be protected for the purposes of the Act. Protected records must not be disposed of without the prior approval of the Chief Archivist, or without notifying the Chief Archivist that you intend to dispose

Key concept	Definition
	of these records. You must identify the protected records and specify how they will be disposed of. The List of protected records for local authorities specifies classes of local authority records that may not be destroyed unless prior approval is given by the Chief Archivist.
Creating and maintaining record	Regulated organisations must create and maintain full and accurate records of their affairs, in line with normal business practice. Records must be maintained in an accessible form until their disposal is authorised by the Chief Archivist.
Disposing records	Information and records disposal refers to the range of processes associated with implementing retention, transfer, or destruction decisions. No one can dispose of, or authorise the disposal of, public or protected records unless they have the authority of the Chief Archivist, or where disposal is required by or under another Act.
Classifying records	All public records that have been in existence for 25 years, or are to be transferred to Archives New Zealand, must have their access status determined as either open or restricted. Similarly, when local authority records become local authority archives, these classifications must be applied. You can read more about determining access status in our **Access guide.**
Providing access to records	Unless the PRA states otherwise, an open access record must be made available to members of the public. This must be free-of-charge and happen as soon as practicable after the request is received. This applies to requests made to: • public offices, including Archives New Zealand • local authorities, and • approved repositories.

Key Outcomes

A clear governance, authorising and accountability environment for information and records.

- Information and records governance arrangements are in place
- Responsibility for managing information and records is assigned
- Information and records management is planned and integrates with Council business strategies and outcomes
- The environment meets the organisation’s information and records management legal, regulatory, and cultural responsibilities

Outcome 1: Improved information and records management capability and practice

- Proactive information and records management capability and practice help to improve the skills of staff

- Endorsed better practices are in place. Information and records systems collect and retrieve the information needed for Council business and work
- Better core business processes that embed effective information and records management practice have helped to reduce duplication of work and product

Outcome 2: Improved access to and use of Council's information and records

- The right information and records are available to the right person(s), at the right time, in the right format, at the right place, to enable open and accountable Council, a better-informed public, and improved business decisions
- The information and records needs of Councils and Community Boards are met
- Information and records are easier to find/retrieve
- The safe use and reuse of personal information and records is maximised

Outcome 3: Information and records treated as a valued asset

- Council's information and records requirements are defined
- Council can readily exchange information and records across government, and externally when appropriate.
- The value of information and records is unlocked by providing opportunities for reuse

Information and Records Management Culture

Information culture is a culture that is conducive to effective information and records management where "the value and utility of information in achieving operational and strategic goals is recognised, where information forms the basis of organisational decision making and information technology is readily exploited as an enabler for effective information systems".

Information and records management responsibility is part of the whole of Council culture.

Relevant Legislation

- Public Records Act 2005
- Information and Records Management Standard (Archives New Zealand) 2016
- Local Government Official Information and Meetings Act 1987
- Official Information Act 1982
- Privacy Act 2020
- Contract and Commercial Law Act 2017
- Evidence Act 2006
- Health and Safety at Work Act 2015

Related Documents

- Digital and Information Strategy
- Information and Records Management Policy
- Protection of Information and Information Systems (Cyber Security)
- Privacy Policy
- Privacy Plan
- Cyber Security Plan
- LGOIMA Request Policy

Council's Responsibility

The Public Records Act 2005 (PRA) establishes a regulatory framework for information and records management across the public sector. The purpose of the PRA is to promote the accountability of government through reliable information management, enhanced public confidence in the integrity of government information and records, and the protection of New Zealand's documentary heritage.

The PRA sets out obligations for regulated organisations in how information and records are created, maintained, transferred, and disposed of. The PRA also covers access to information and records.

Responsibilities of regulated organisations are to:

- Create and maintain information and records
- Dispose of information and records, as authorised by the Chief Archivist or otherwise by law
- Local authorities are responsible for managing information and records of archival value
- Classify the access status of all information and records
- Provide access to open access records as soon as practicable

The Information and Records Management Standard establishes how to manage information and records systematically. It sets out the minimum level of compliance that regulated organisations must meet. Compliance with the standard is mandatory.

Obligations under the Act

The Act sets out obligations of public offices and local authorities in how they create, maintain, transfer, and dispose of records. The Act also covers access to information and records.

Requirement to create and maintain records (section 17)
Every public office and local authority must create and maintain full and accurate records of its affairs, in line with normal prudent business practice. Records include the records of any task contracted to an independent contractor.
Every public office must maintain in an accessible form, to be able to use subsequent reference, all public records that are in its control, until their disposal is authorised.
Every local authority must maintain in an accessible form, to be able to use for subsequent reference, all protected records that are in its control, until their disposal is authorised.

Authority required to dispose of public records and protected records (section 18)
No person may dispose of, or authorise the disposal of, public records or protected records except with the authority of the Chief Archivist, unless disposal of a public record or protected records is required by or under another Act.

Mandatory transfer of public records (section 21)
Every public office must transfer from its possession and control public records that have been in existence for 25 years, unless the public records are to be destroyed, transferred before the expiry of 25 years, or transfer is to be deferred.

Transfer of public records and local authority records (section 23)
A public office that takes over responsibility for a function to which public records relate must give notice to the Chief Archivist of the transfer within 3 months. The same applies for local authority records.

Protected records of local authorities (section 40)

A local authority must provide for the adequate protection and preservation of a protected record it holds, in accordance with any applicable standards or instructions, and must not dispose of a protected record unless notice has been given to the Chief Archivist of the intention to do so.

Requirement to classify access status - (sections 43 and 44)
When public records have been in existence for 25 years or are about to be transferred to the control of the Chief Archivist, the records must be classified as open access records or restricted access records.
In classifying the access status of a public record, the administrative head of the controlling public office must consider whether there are good reasons to restrict public access, or whether another enactment requires the public record to be withheld from public access.

Requirement to classify the access status of local authority records (sections 45 and 46)
When a local authority record becomes a local authority archive, it must be classified as either an open access record or a restricted access record.
In classifying the access status of a local authority record, the administrative head of the controlling local authority must consider whether there are good reasons to restrict public access, or whether another enactment requires the local authority records to be withheld from public access.

Public inspection of open access records (section 47)
Unless the PRA provides otherwise, an open access record must be made available for inspection by members of the public free of charge as soon as is reasonably practicable after a request to inspect the record is made to the public office, the local authority, the approved repository, or Archives New Zealand, whichever has possession of the open access record.

Executive sponsor - Roles and responsibilities

Introduction

The Information and Records Management Standard requires a designated Executive Sponsor. That person has strategic and executive responsibility for overseeing information and records management in a public sector organisation.

An Executive Sponsor should:

- be a person reporting to the administrative head of the organisation – the Chief Executive
- have organisation-wide influence, particularly within the upper tiers of the organisation
- have appropriate strategic and managerial skills
- be able to liaise closely with information and accountability stakeholders
- understand how to promote and encourage information and records management in the organisation.

Key responsibilities

The Executive Sponsor champions the importance of information and records management among the organisation's leadership. The aim is for everyone in the organisation to see information and records management as an integral part of a business operating effectively.

The Executive Sponsor is responsible for:

- ensuring that the strategy and policy adopted by the organisation supports information and records management
- being involved in strategic and operational planning to align information and records management with the corporate objectives and business activities of the organisation

- liaising with business units to ensure that information and records management is integrated into work processes, systems, and services
- overseeing the budget for information and records management, and ensuring the resources needed to support information and records management are known and sought in funding decisions
- ensuring that staff with appropriate skills to implement information and records management strategies are employed, and regular upskilling is available
- monitoring and reviewing information and records management to ensure that it is implemented, transparent and meets business needs.

The Executive Sponsor's role extends beyond their organisation. They are responsible for cooperating and liaising with Archives New Zealand about monitoring and reporting on compliance. They should network with Executive Sponsors in other organisations to cooperate and align best practice processes.

How the Executive Sponsor can fulfil those responsibilities

When an organisation aligns its information and records management to its business objectives, it can add value to its organisation's products and services. Information and records management is an investment that an organisation can reuse and benefit from. The Executive Sponsor should champion effective information and records management strategies and policies to:

- encourage the organisation to value information and records management
- align information and records management to business objectives
- facilitate strategic partnerships
- increase efficiency.

When an information and records management strategy is planned and developed, this is an ideal time to align with the organisation's business and to ensure that information and records support business operations. The Executive Sponsor can oversee the incorporation of information and records management requirements into business processes and systems design. This will support business operations and service delivery.

The Executive Sponsor's position in the organisation means they can positively influence the organisation's attitudes to information and records management. They can help to develop a strong culture focused on managing information appropriately. They can act as a broker between business groups and the information and records management staff to ensure that business imperatives and effective information and records management work together.

The Executive Sponsor can change attitudes by leading by example. They can ensure that they understand and use organisational systems and encourage staff to do likewise.

The Executive Sponsor can use their strategic skills to ensure information and records management strategies are efficient and maximise the funds allocated to them. They can encourage effective information and records management practices to:

- generate savings across the organisation
- prevent information being kept longer than necessary
- ensure high value information is accessible and usable.

An organisation can experience costs from lost opportunities, lost collaborations, poor decision making, and strategic mistakes. These losses are sometimes due to a lack of information. Improved information flows can improve the quality of decision making, provide the basis to maintain products and services effectively, and drive collaboration and innovation. They can also improve transparency around government operations and increase the organisation’s public profile. This can help to increase business efficiency.

If you have any questions about the role or to send us notifications for new Executive Sponsors, please email us at rkexecutivesponsor@dia.govt.nz

Information and Records Management Standard

Introduction

Information and records are key strategic assets at the core of public sector business and government accountability. They help organisations plan for and achieve valuable and relevant short-term and long-term outcomes that benefit business, government, and the wider community.

Managing information and records appropriately is important because it:

- enables the public to hold the government accountable
- provides the foundation for sustainable and effective products and services
- supports decision making
- outlines responsibilities
- documents rights and entitlements
- drives collaboration and communication
- facilitates and enables creativity and growth
- preserves public knowledge for discovery and reuse
- makes up the corporate memory of an organisation.

Information and records should therefore be:

- trustworthy and managed accountably
- readily accessible, understandable, and usable
- valued as critical to business operations
- part of an organisation’s approach to risk management
- maintained to meet business, government, and community purposes.

Why we have an information and records management standard

This standard establishes how to manage information and records efficiently and systematically. It sets out the minimum level of compliance that organisations must meet.

This standard is designed to support organisations to meet their obligations under the Public Records Act 2005 (the Act). A major focus of the standard is to support effective information and records practices in complex business and government environments.

Records are any information, regardless of form and format, from documents through to data. Records serve both as evidence of business activity and as information assets. A record includes its metadata, which is also managed as a record. Meeting the standard enables organisations to manage their information assets in a holistic, integrated manner. The standard should be read in conjunction with instructions, directions, and any other standards or guidance under the Act.

Mandate

This standard is issued by the Chief Archivist under section 27 of the Act. It is mandatory for the following organisations, which must manage their information and records to the standard:

- public offices, including state and integrated schools
- local authorities, including council-controlled organisations

The Treaty of Waitangi / Te Tiriti o Waitangi

The standard supports the rights of Māori, under the Treaty of Waitangi/Te Tiriti o Waitangi to access, use and reuse information and records that are taonga. Organisations should ensure that information and records about Māori are accessible.

Principles

Principle 1: Organisations are responsible for managing information and records

To ensure information and records can support all business functions and operations, organisations must establish a governance framework. This framework will help an organisation to:

- develop strategies and policies to direct how information and records will be managed
- assign responsibilities and allocate resources
- establish provisions for information and records management in outsourcing and
- service delivery arrangements
- monitor information and records management activities, systems, and processes.

1.1 Information and records management must be directed by strategy and policy, and reviewed and monitored regularly

- Ensure senior executives adopt an organisation-wide strategy on information and records management.
- Ensure senior executives adopt an organisation-wide policy on information and records management.
- Monitor how people in the organisation are applying strategies and policies.

1.2 Information and records management must be the responsibility of senior management. Senior management must provide direction and support to meet business requirements as well as relevant laws and regulations.

- Ensure the policy lists the senior executive team as responsible for managing information and records.
- Ensure the policy reflects the legislative responsibilities of chief executives for example under the Public Service Act 2020 (section 32(1)), and the Local Government Act 2002 (section 42(2)).

1.3 Responsibility for the oversight of information and records management must be allocated to a designated role (the Executive Sponsor).

- Include the Executive Sponsor’s responsibility in all strategy and policy on information and records management.
- Include the Executive Sponsor’s responsibility in their performance plan.
- Advise Archives New Zealand of the organisation’s Executive Sponsor.

1.4 Organisations must have information and records management staff, or access to appropriate skills.

- Assign responsibility for information and records management to appropriate staff and record these responsibilities in all strategies and policies.
- Note the skills and capabilities in relevant role descriptions.
- Include responsibilities in performance plans and service agreements.

1.5 Business owners and business units must be responsible for ensuring that information and records management is integrated into business processes, systems, and services.

- Include and list all assigned responsibilities in the policy on information and records management.
- Include and list all assigned responsibilities in performance plans.
- Include in systems and processes details about responsibility for ensuring effective information and records management.
- Document the responsibility of the business owner.

1.6 Staff and contractors must understand the information and records management responsibilities of their role. They must understand relevant policies and procedures.

- Note the skills, capabilities and responsibilities in the relevant role descriptions and performance plans.
- Set out in all policies, business rules and procedures the requirements and responsibilities for all staff who create and manage information and records.

1.7 Information and records management responsibilities must be identified and addressed in all outsourced and service contracts, instruments, and arrangements.

- Note all responsibilities in the strategy and policy on information and records management.
- Specify and detail in outsourced and service contracts, instruments, and arrangements all aspects of information and records management.
- Assess portability and security of information and records in all outsourced and service contracts, instruments, and arrangements.

1.8 Information and records management must be monitored and reviewed to ensure that it is accurately performed and meets business needs.

- Document monitoring activities, systems, and processes; take corrective actions to address any problems.
- Ensure reviews of all processes and systems happen regularly.

Principle 2: Information and records management supports business

Information and records management ensures the creation, usability, maintenance, and sustainability of the information and records needed for business operations. It also ensures business operations meet government and community expectations.

By appraising business activities, organisations define their key information requirements. Appraisal is used to design and embed information and records management into business processes and systems. Taking a planned approach to information and records management means:

- considering all operating environments
- ensuring that all service and systems arrangements consider the creation and management of information and records needed to support business.

2.1 Information and records required to support and meet business needs must be identified.

- Document policies, business rules and procedures on what information and records are required to meet and support business needs.
- Current, comprehensive appraisal is documented.
- Decisions are documented or reflected in specifications for systems and metadata schemas.

2.2 High risk/high value areas of business, and the information and records needed to support them, must be identified, and regularly reviewed.

- Identify and document which parts of the organisation and which systems hold information and records that are high risk, high value, or both.
- Identify, manage, and mitigate all risks relating to the information and records.
- Protect with business continuity strategies and plans all business areas and systems which manage information and records that are high risk, high value, or both.

2.3 Information and records management must be design components of all systems and service environments where high risk/high value business is undertaken.

- Assess information and records management in system acquisition, maintenance, and decommissioning, and implement these practices where needed.
- Ensure that systems specifications for business that is high risk, high value, or both, include information and records management requirements.
- Ensure that systems specifications include minimum requirements for metadata needed to support information and records identification, usability, accessibility, and context.
- Document and maintain systems design and configuration.

2.4 Information and records must be managed across all operating environments.

- Identify and document where information and records are created and held, across all system environments and physical locations.
- Document the process for managing information and records in diverse system environments.

2.5 Information and records management must be designed to safeguard information and records with long-term value.

- Document which systems hold information and records of long-term value or archival value, and where they are located.
- Ensure that the decommissioning of systems follows the requirements for disposing of information and records.

2.6 Information and records must be maintained through systems and service transitions by strategies and processes specifically designed to support business continuity and accountability.

- Implement and review a migration strategy.
- Migrate information, records, and metadata from one system to another using a managed process that results in records that people can access easily and that have trustworthy information.
- Ensure the portability of information and records is addressed in outsourced or service arrangements.
- Maintain the systems documentation

Principle 3: Information and records are well managed

Effective management underpins trustworthy and reliable information and records that are accessible, usable, shareable, and maintained. This management extends to information and records in all:

- formats (and associated metadata)
- business environments
- types of systems
- locations.

3.1 Information and records must be routinely created and managed as part of normal business practice.

- Ensure all policies, business rules and procedures accurately document staff requirements and responsibilities for creating, capturing, and managing information and records of business processes.
- Ensure assessments or audits demonstrate that business rules, procedures and systems are operating.
- Identify, resolve, and document any exceptions to normal business processes that affect information integrity, usability, or accessibility.

3.2 Information and records must be reliable and trustworthy.

- Ensure appropriate minimum metadata is available so that the meaning and context are associated with the relevant information and records, and that it is correct.
- Ensure assessments or audits can test management controls, including information integrity.

3.3 Information and records must be identifiable, retrievable, accessible, and usable for as long as they are required.

- Ensure testing can verify that systems can locate and produce information and records that are viewable and understandable.
- Ensure appropriate minimum metadata is in place so that information and records are identifiable, accessible, and usable.

3.4 Information and records must be protected from unauthorised or unlawful access, alteration, loss, deletion and/or destruction.

- Ensure information security and protection mechanisms are in place.
- Protect information and records wherever they are located, including in transit and outside the workplace.
- Document and implement all permissions to access and use systems that manage information and records.
- Ensure that assessments or audits can test that access controls are implemented and maintained.

3.5 Access to, use of and sharing of information and records must be managed appropriately in line with legal and business requirements.

- Ensure policies, business rules and procedures identify how access, use and appropriate sharing of information and records are managed.
- Ensure assessments or audits confirm that access is in line with the organisation's policies, business rules and procedures.

3.6 Information and records must be kept for as long as needed for business, legal and accountability requirements.

- Ensure policies, business rules and procedures identify how the disposal of information and records is managed.
- Ensure information and records are sentenced (a decision is made about whether to keep, destroy or transfer them).
- Dispose of information and records regularly, and in line with authorised disposal authorities.
- Transfer information and records of archival value to Archives New Zealand, or to an approved repository, or to a local authority archive (when authorised).

3.7 Information and records must be systematically disposed of when authorised and legally appropriate to do so.

- Ensure policies, business rules and procedures set out how to manage the disposal of information and records (including metadata).
- Ensure disposal is in line with authorised disposal authorities.
- Document any disposal of information and records.

Information and Records Risk

Information Services manages it's risks as per the Risk Management Policy. Risk management forms of Information Services Activity Management Plan. For a detailed view of the Information Services Risk Register (Doc ID: 447956), please click here.
The following is an extract from the Information Services Risk Register:

Risk description	Risk driver	Risk consequence	Residual risk	Risk management plan/control
Cyber Security Risk are being reviewed by the external auditor. The risk register and plan will be updated following the review.				

Archives New Zealand Information Management Maturity Assessment

Council has chosen to undertake an independent information and records management review by an external party every 3 years. Council will utilise Association of Local Government Information Management (ALGIM) to undertake IM Audits to check our compliance with the Public Records Act 2005 and the Archives NZ Information and Records Management Standard 2016.

Purpose

The primary purpose of this Information Management Maturity Assessment (IM Maturity Assessment) is to help public offices and local authorities to assess the strengths and weaknesses of their information management (IM) programmes to determine where improvements are most needed.

A secondary purpose for the IM Maturity Assessment is to provide a consistent framework to support Archives New Zealand ‘s Audit Programme due to start in the 2020/21 financial year.

Other information-related models

Archives New Zealand acknowledge that there are a variety of excellent information-related maturity models and other guidelines available within New Zealand, each with their own purpose and scope.

Archives New Zealand also acknowledges the work completed by the Public Records Office of Victoria. Their Information Management Maturity Measurement tool (IM3) was used as a starting point for the development of Archives New Zealand’s IM Maturity Assessment.

What is the IM Maturity Assessment?

This IM Maturity Assessment is a high-level rating of the maturity of an organisation’s IM practice. It is a maturity model or analytical tool that provides a framework to assess a programme or practice based on a set of core principles and standards. The IM Maturity Assessment is based on the requirements outlined in the Public Records Act 2005 and Archives New Zealand’s Information and Records Management Standard 16/S1.

An assessment using a maturity model can highlight strengths and weaknesses in an organisation’s information management practices and assist the organisation to make decisions about priorities and improvement projects to improve IM maturity.
It can also identify areas of risk within an IM programme.

Scope and Structure

The IM Maturity Assessment consists of eight categories. Within each category there are one or more topics.

Each topic area has a question set drawn from the requirements of the Public Records Act 2005, the mandatory Information and Records Management Standard 16/S1 and other instructions and authorities released by the Chief Archivist.

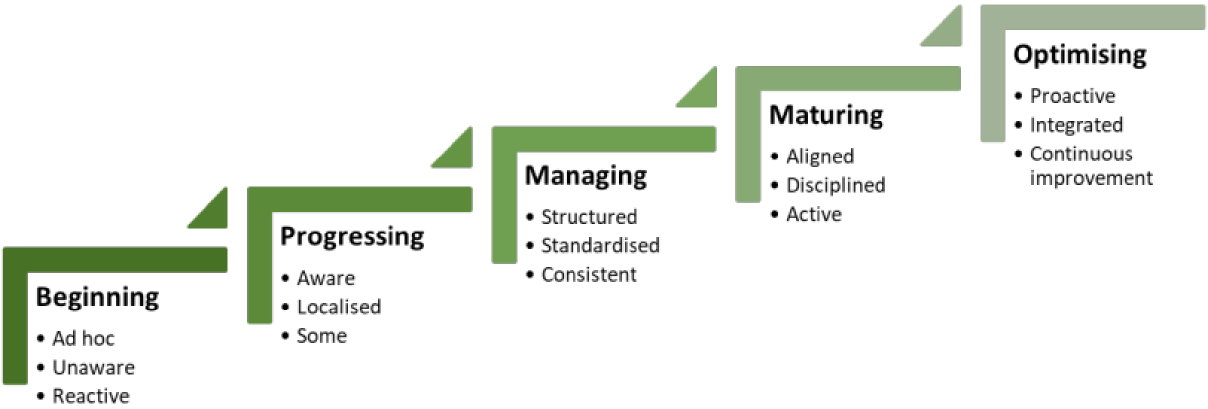
Archives New Zealand expects organisations that assess their maturity at:

- Beginning or progressing require greater focus and priority on the management of information

- Managing is broadly meeting the minimum requirements expected for all organisations covered by the mandatory Standard
- Maturing or Optimising are working towards increased organisation-wide consistency, alignment, and effectiveness
- Optimising understands the strategic importance of information to their organisation as well as for accountability and transparency of government

IM Maturity Levels

There are five levels of maturity. Each level builds on the previous level, showing progressive improvement in IM practices. Below are some of the words that have been used to describe IM maturity at each level of the assessment.



Current state by Categories

A snapshot of the current state of information and records management practices at Council will be represented here following the external audit.

Actions

Information and Records Management Actions

Action management and reporting on progress will occur within the SAM for Compliance - compliance management tool. Tasking of these actions will occur within the IS Portal.

The following is a summary of the actions at the time of preparing this plan, including recommendations from the ALGIM IM Audit. The actions are grouped by the categories and topics of the Archives New Zealand Information Management Maturity Assessment.

Status key: Not Started, Started, Partially Completed, Mostly Completed, Fully Completed
Priority key: Critical, Important, Normal, Low

Category	Topic	Actions	Priority	Responsibility	Due Month/Year	Status	Notes
Governance	1. IM Strategy	Actions will be populated following the external audit					
	2. IM Policy and Processes						
	3. Governance Arrangement and Executive Sponsor						
	4. IM Integration into Business Process						
	5. Outsourced Functions and Collaborative Arrangements						

Category	Topic	Actions	Priority	Responsibility	Due Month/Year	Status	Notes
	6. Te Tiriti O Waitangi						
Self-Monitoring	7. Self-Monitoring						
Capability	8. Capacity and Capability						
	9. Roles and Responsibilities						
Creation	10. Creation and Capture of Information						
	11. High Value/High Risk Information						
Management	12. IM Requirements Built into Technology Systems						
	13 Integrity of Information						
	14. Information Maintenance and Accessibility						
	15. Business Continuity and Recovery						
Storage							

Category	Topic	Actions	Priority	Responsibility	Due Month/Year	Status	Notes
	16. Appropriate Storage Arrangements						
	17. Local Authority Storage Arrangement for Protected Information and Local Authority Archives						
Access	18. Information Access, Use and Sharing						
	19. Local Authority Archives Access Classification						
Disposal	20. Current Organisation-Specific Disposal Authorities						
	21 Implementation of Disposal Decisions						

LGOIMA Request Actions

IRM team is responsible for LGOIMA Requests, the following is a summary of the actions at the time of preparing this plan.

These actions are broken down into the following categories which are based on the Ombudsman LGOIMA assessment framework for compliance and practice:

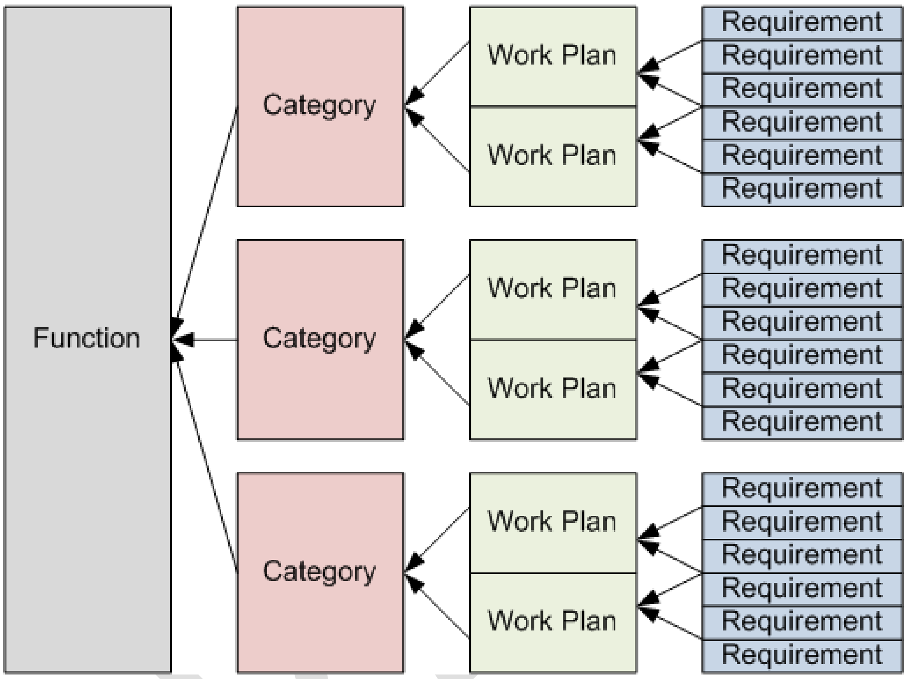
- Leadership and culture
- Organisation structure, staffing and capability
- Internal policies, procedures, resources, and systems
- Current practices
- Performance monitoring and learning

Status key: Not Started, Started, Partially Completed, Mostly Completed, Fully Completed

Category	Actions	Responsibility	Due Month/Year	Status	Notes
Leadership and culture	Actions will be populated following the external audit				
Organisation structure, staffing and capability					
Internal policies, procedures, resources, and systems					
Current practices					
Performance monitoring and learning					

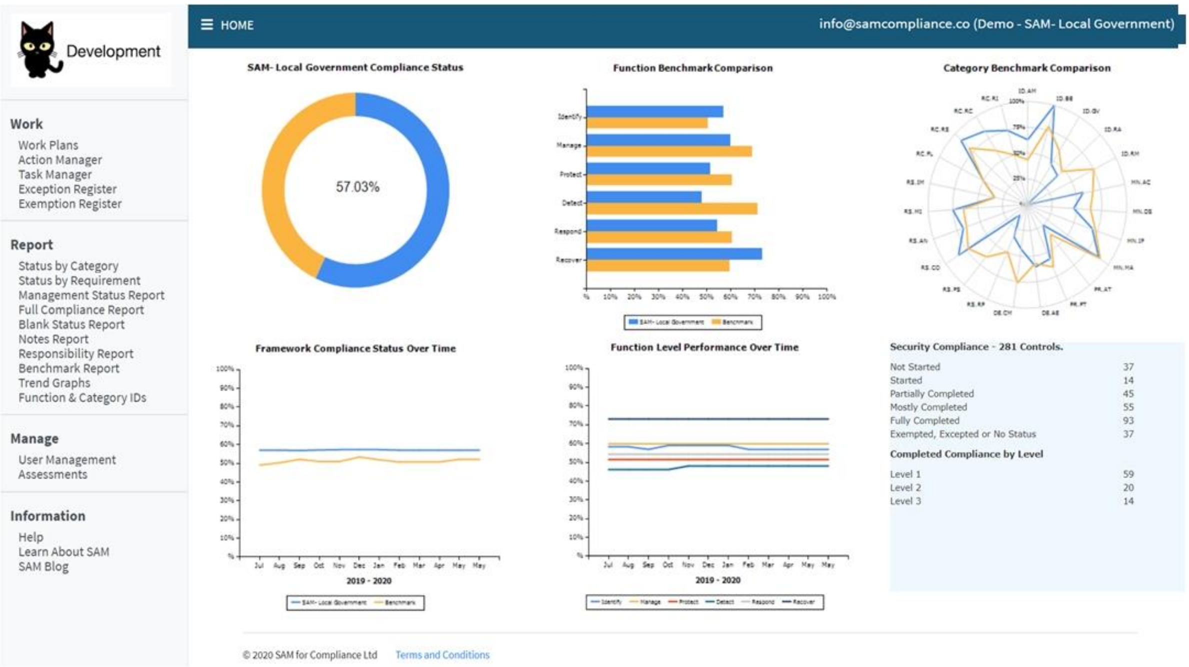
Compliance Management

Council has chosen to utilise SAM for Compliance. SAM for Compliance is a compliance management tool which can be applied to any standard or framework that is comprised of specific requirements or controls. SAM for Compliance contains frameworks which are broken down into key performance areas based on the NIST CSF model of Framework, Function, Category, Sub-Category and Controls.



SAM for Compliance relies on self-assessment to ascertain the current compliance status. The system simply calculates totals based on Council input.

The controls are assessed based on a pre-defined maturity model individual to each framework instance and dynamically update the dashboard view and all system reports.



Security Compliance - 281 Controls.

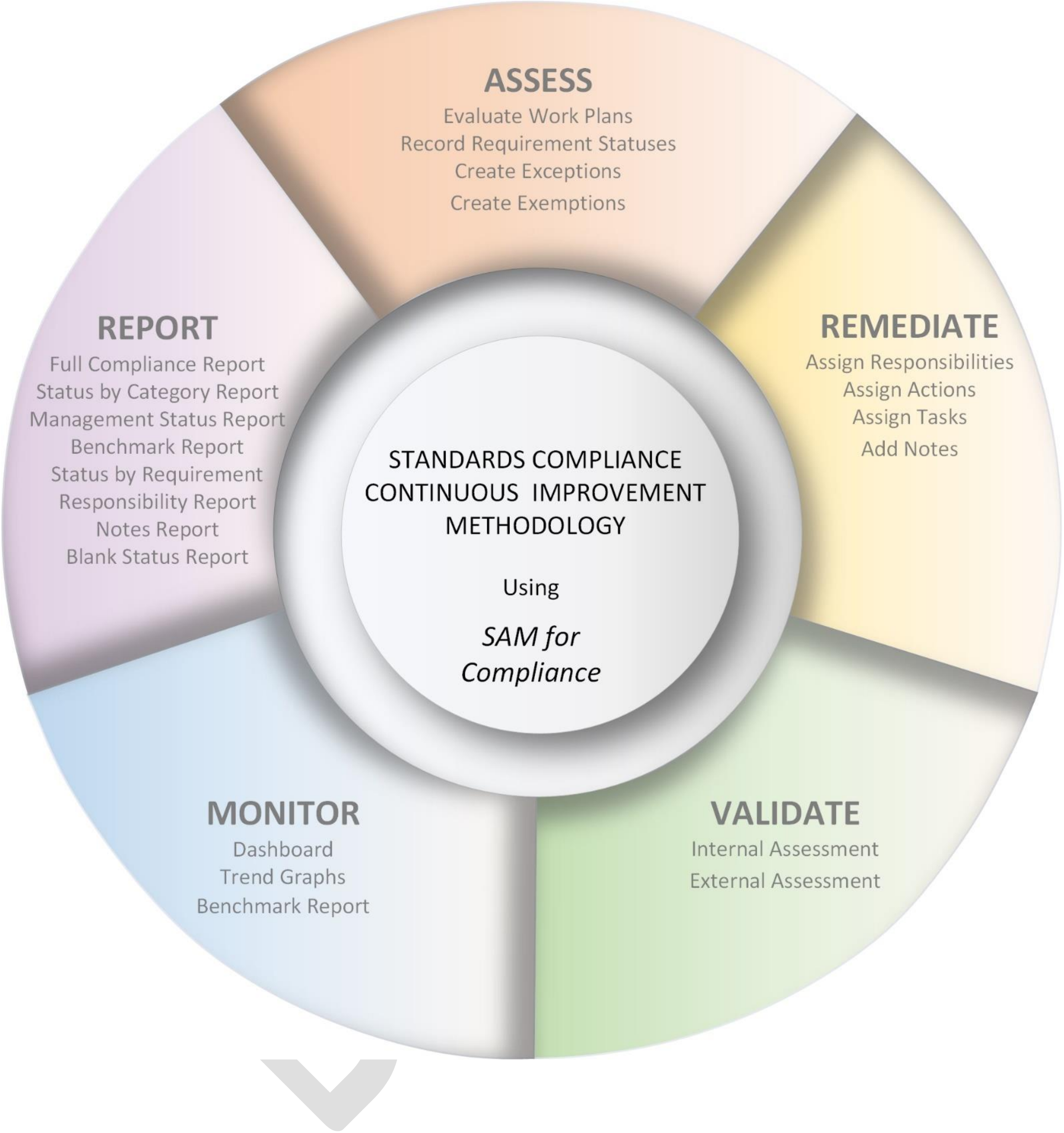
Not Started	37
Started	14
Partially Completed	45
Mostly Completed	55
Fully Completed	93
Exempted, Excepted or No Status	37

Completed Compliance by Level

Level 1	59
Level 2	20
Level 3	14

SAM Management Methodology
The SAM for Compliance tool consists of functions that assist you to manage compliance to your chosen framework as demonstrated by the features on the colour wheel below:

- **ASSESS -** Evaluate and record your status against your chosen maturity model, including Exceptions and Exemptions
- **REMEDIATE -** Assign responsibilities for achieving compliance with controls, assign Actions and Tasks and add Notes to record specific details or links to other documents
- **VALIDATE** - Assessment function
- **MONITOR** - View your current Status from our dynamic, multi-chart Dashboard and Trend graphs. View benchmark comparisons against your Peer Group (where applicable)
- **REPORT** - Report your current Status


ASSESS
Evaluate Work Plans
Record Requirement Statuses
Create Exceptions
Create Exemptions
REPORT
Full Compliance Report
Status by Category Report
Management Status Report
Benchmark Report
Status by Requirement
Responsibility Report
Notes Report
Blank Status Report
REMEDIATE
Assign Responsibilities
Assign Actions
Assign Tasks
Add Notes
STANDARDS COMPLIANCE
CONTINUOUS IMPROVEMENT
METHODOLOGY
Using
SAM for
Compliance
MONITOR
Dashboard
Trend Graphs
Benchmark Report
VALIDATE
Internal Assessment
External Assessment

Reporting

Reporting on the progress of this plan will occur as follows:

Who	What	When
Audit and Risk Committee	An information report will be prepared, including the following topics: • Archives New Zealand Information Management Maturity Assessment update • Information and Records Management programme of work by actions	Quarterly
Executive Team		Quarterly

CENTRAL OTAGO
DISTRICT COUNCIL

1 Dunorling Street
PO Box 122, Alexandra 9340
New Zealand

03 440 0056

Info@codc.govt.nz
www.codc.govt.nz

Privacy Plan

Department	**Information Services**
Final (PDF) Doc ID:	Insert CentralDocs Doc ID
Final Versions:	Insert CentralDocs version URL
Draft (Word) Doc ID:	558510
Draft Versions:	https://cdocs.codc.govt.nz//Versions.aspx?DocumentID=558510
Approved by:	Executive Team
Effective date:	TBC
Next review:	Every 12 months, add date

Table of Contents

Introduction

Purpose

Central Otago customers need to have trust and confidence in the way Central Otago District Council (Council) manages its personal information. This plan has a close relationship with Cyber Security Plan, and Information and Records Management Plan.

The purpose of this Privacy Plan is to assess how Council currently protects customer's personal information and what actions it needs to undertake to improve that protection.

Scope

The Privacy Plan is supported by Council's Digital and Information Strategy and Privacy Policy.

This plan ensures Council is adhering to the Information Privacy Principles (IPPs), surrounding the collection and dissemination of information (including personal information), managing privacy risks, breach notifications, privacy complaints and/or requests and protection of individuals.

The protection of personal information applies to all council staff, including temporary employees, and contractors. It also applies to anyone who is involved in council operations, including volunteers and those people with honorary status or unpaid staff status.

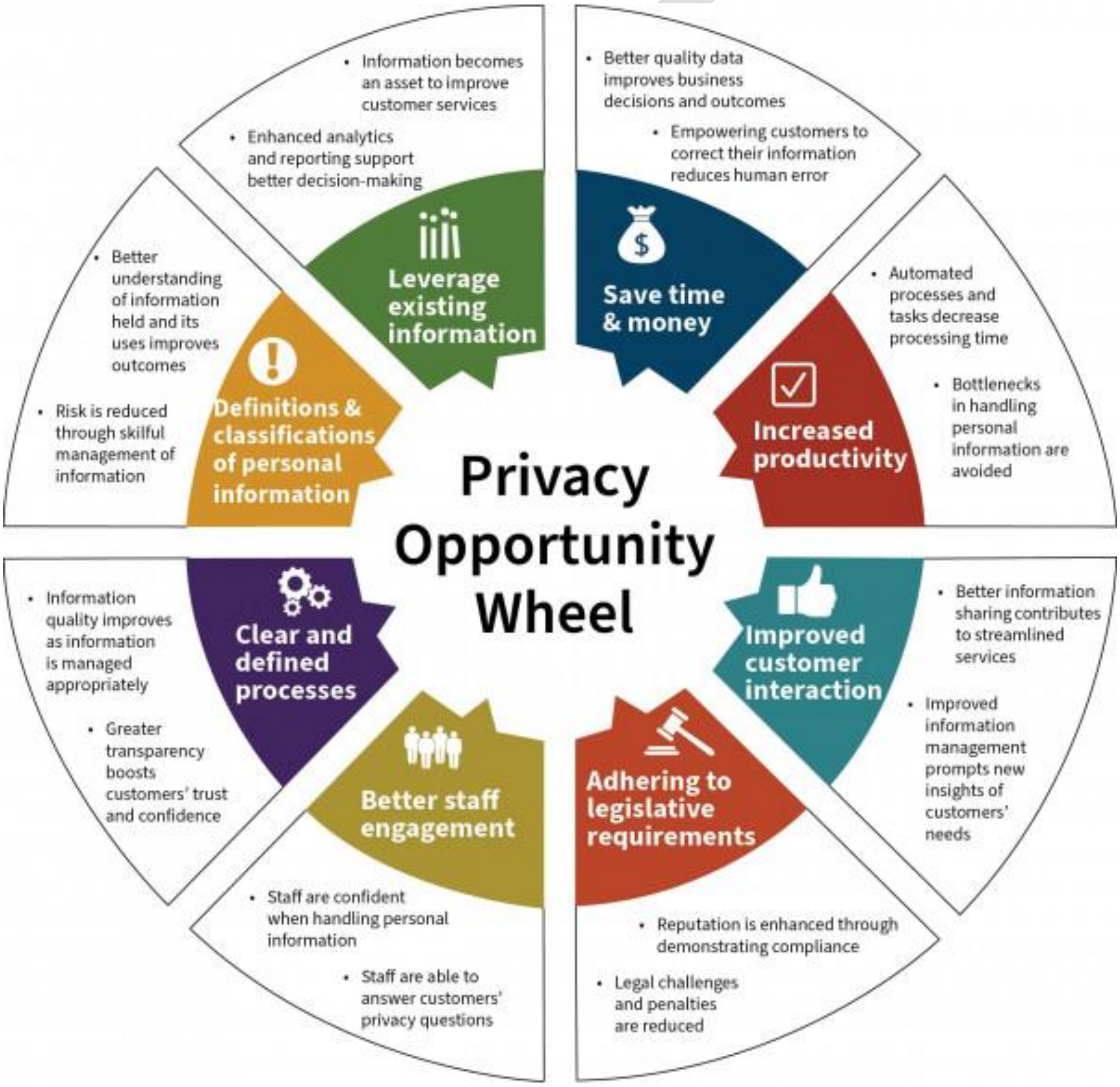
Information Services (IS) are responsible for the management and implementation of this plan.

Privacy Culture

Council wants to encourage a culture in which everyone views privacy as their responsibility and works to develop and promote a culture in which personal information is protected and respected.

Privacy means different things to different people. A right to privacy can mean a right to be left alone, a right to control who sees information about you, or a right to make decisions about your personal life without intervention.

The value of a right to privacy can also vary depending on circumstances, cultural context, time, and personal preference. Although privacy is important, it is not absolute. Other social interests can be more important than privacy in some instances, such as preventing crime, ensuring safety, and ensuring that courts get information to make their decisions.


Privacy Opportunity Wheel
Leverage existing information
• Information becomes an asset to improve customer services
• Enhanced analytics and reporting support better decision-making
Save time & money
• Better quality data improves business decisions and outcomes
• Empowering customers to correct their information reduces human error
Increased productivity
• Automated processes and tasks decrease processing time
• Bottlenecks in handling personal information are avoided
Improved customer interaction
• Better information sharing contributes to streamlined services
• Improved information management prompts new insights of customers' needs
Adhering to legislative requirements
• Reputation is enhanced through demonstrating compliance
• Legal challenges and penalties are reduced
Better staff engagement
• Staff are confident when handling personal information
• Staff are able to answer customers' privacy questions
Clear and defined processes
• Information quality improves as information is managed appropriately
• Greater transparency boosts customers' trust and confidence
Definitions & classifications of personal information
• Better understanding of information held and its uses improves outcomes
• Risk is reduced through skilful management of information

Relevant Legislation

The handling of personal information in New Zealand is governed by the Privacy Act 2020, Privacy Codes and other legislation.

Privacy Act 2020:

On 1 December 2020, the Privacy Act 2020 replaced the Privacy Act 1993. The reforms aim to encourage public and private sector agencies to identify risks and prevent incidents that could cause harm.

The major changes include:

- Notifiable privacy breaches
- Compliance notices
- Enforceable access directions
- Disclosing information overseas
- Extraterritorial effect
- New criminal offences
- Additional withholding grounds for access requests.

The purpose of the Privacy Act is to promote and protect individuals' privacy by establishing principles on the collection, use, and disclosure of personal information, and access by individuals to the personal information held about them. Personal information can relate to information about customers, clients, employees, and others.

Enforcement of the Act is through the Privacy Commissioner who has the power to investigate any action which appears to interfere with the privacy of an individual, either on a complaint made to the Commissioner or on the Commissioner's own initiative.

The Government Chief Privacy Officer provides guidance to help government agencies understand and meet their responsibilities under the Act.

More information:

- Privacy Act 2020
- Office of the Privacy Commissioner
- Government Chief Privacy Officer
- Office of the Privacy Commissioner — Key changes in the Privacy Act 2020
- Office of the Privacy Commissioner section-by-section comparison of the 2 Acts
- Office of the Privacy Commissioner — Reporting privacy breaches (NotifyUs)
- Office of the Privacy Commissioner — Privacy Act 2020 training module

Other legislation

- Public Records Act 2005
- Information and Records Management Standard (Archives New Zealand) 2016
- Local Government Official Information and Meetings Act 1987
- Official Information Act 1982
- Evidence Act 2006
- Contract and Commercial Law Act 2017
- Health and Safety at Work Act 2015
- Public Service Act 2020
- Human Rights Act 1993

Related Documents

- Digital and Information Strategy
- Privacy Policy
- Privacy Breach Notification Procedure
- Request for Personal Information Procedure
- Cyber Security Policy
- Protection of Information and Information Standards.
- Disposal Schedule

Information Privacy Principles

At the core of the Privacy Act are 13 Information Privacy Principles that set out how agencies are to:

- Collect personal information (IPPs 1 to 4)
- Store personal information (IPP 5)
- Provide access to (IPP 6) and correct (IPP 7) personal information
- Use (IPPs 8 to 10) and disclose (IPP 11 and 12) personal information
- Only keep personal information for as long as necessary (IPP 9)
- Use unique identifiers (IPP 13).

IPP 6 provides individuals with the right to access the personal information that an agency holds about them, unless 1 of the Privacy Act exceptions applies.

Principle 1 - Purpose for collection

Principle 1 states that organisations must only collect personal information if it is for a lawful purpose connected with their functions or activities, and the information is necessary for that purpose.

When asking people for their personal information, you should carefully consider why you are collecting it. If the personal information you are asking for isn't necessary to achieve something closely linked to your organisation's activities, you shouldn't collect it.

You can view Principle 1 in the Privacy Act 2020 here.

Principle 2 - Source of information

Principle 2 states that personal information should be collected directly from the person it is about. The best source of information about a person is usually the person themselves. Collecting information from the person concerned means they know what is going on and have some control over their information.

It won't always be possible to collect information directly from the person concerned, so organisations can collect it from other people in certain situations. For instance:

- If the person concerned authorises collection from someone else
- If it's necessary to uphold or enforce the law
- If the information is collected from a publicly available source
- If collecting information from the person directly would undermine the purpose of collection.

You can view Principle 2 in the Privacy Act 2020 here.

Principle 3 - What to tell an individual

Principle 3 states that organisations should be open about why they are collecting personal information and what they will do with it.

When an organisation collects personal information, it must take reasonable steps to make sure that the person knows:

- Why it's being collected
- Who will receive it?
- Whether giving it is compulsory or voluntary
- What will happen if the information isn't provided.

Sometimes there may be good reasons for not letting a person know about the collection – for example, if it would undermine the purpose of the collection, or it's just not possible to tell the person.

View Principle 3 in the Privacy Act 2020 here.

Principle 4 - Manner of collection

Principle 4 states that personal information must not be collected by unlawful, unfair, or unreasonably intrusive means. When an organisation collects information about a person, it has to do so in a way that is fair and legal.

What is fair depending a lot on the circumstances. Threatening, coercive, or misleading behaviour is likely to be considered unfair.

If you break a law when collecting information, then you have collected information unlawfully.

What is reasonable also depends on the circumstances, such as the purpose for collection, the degree to which the collection intrudes on privacy, and the time and place it was collected.

You need to take particular care when collecting information from children and young people. It may not be fair to collect information from children in the same manner as you would from an adult.

View Principle 4 in the Privacy Act 2020 here.

Principle 5 - Storage and security

Principle 5 states that organisations must ensure there are safeguards in place that are reasonable in the circumstances to prevent loss, misuse, or disclosure of personal information.

View Principle 5 in the Privacy Act 2020 here.

Principle 6 - Access

Principle 6 states that people have a right to ask for access to their own personal information.

Generally, an organisation must provide access to the personal information it holds about someone if the person in question asks to see it.

People can only ask for information about themselves. The Privacy Act does not allow you to request information about another person unless you are acting on that person's behalf and have written permission.

The provisions relating to access to personal information can be found in Part 4, Subpart 1 of the Privacy Act 2020 here.

Principle 6 in the Privacy Act 2020 here.

Refusing access:
In some situations, an organisation may have good reasons to refuse a request for access to personal information. For example, the information may involve an unwarranted breach of someone else's privacy or releasing it may pose a serious threat to someone's safety.

Principle 7 - Correction

Principle 7 states that a person has a right to ask an organisation or business to correct information about them if they think it is wrong.

If an organisation does not agree that the information needs correcting, an individual can ask that an agency attach a statement of correction to its records, and, if reasonable, the agency should do so.

The provisions relating to correction of personal information can be found in Part 4, Subpart 2 of the Privacy Act 2020.

View Principle 7 in the Privacy Act 2020 here.

Principle 8 - Accuracy

Principle 8 states that an organisation must check before using or disclosing personal information that it is accurate, up to date, complete, relevant, and not misleading.

View Principle 8 in the Privacy Act 2020 here.

Principle 9 - Retention

Principle 9 states that an organisation should not keep personal information for longer than it is required for the purpose it may lawfully be used.

View Principle 9 in the Privacy Act 2020 here.

Principle 10 - Use

Principle 10 states that organisations can generally only use personal information for the purpose it was collected.

Sometimes other uses will be allowed, such as if the new use is directly related to the original purpose, or if the person in question gives their permission for their information to be used in a different way.

View Principle 10 in the Privacy Act 2020 here.

Principle 11 - Disclosure

Principle 11 states that an organisation may only disclose personal information in limited circumstances. For instance, an organisation may disclose personal information when:

- Disclosure is one of the purposes for which the organisation got the information
- The person concerned authorises the disclosure
- The information is to be used in a way that does not identify the person concerned
- Disclosure is necessary to avoid endangering someone's health or safety
- Disclosure is necessary to uphold or enforce the law.

Principle 11 in the Privacy Act 2020 here.

Principle 12 - Disclosure outside New Zealand

Principle 12 sets rules around sending personal information to organisations or people outside New Zealand (cross-border disclosure).
A business or organisation may only disclose personal information to another organisation outside New Zealand if the receiving organisation:

- Is subject to the Privacy Act because they do business in New Zealand
- Is subject to privacy laws that provide comparable safeguards to the Privacy Act
- Agrees to adequately protect the information, e.g. by using model contract clauses
- Is covered by a binding scheme or is subject to the privacy laws of a country prescribed by the New Zealand Government.

If none of the above criteria apply, a business or organisation may only make a cross-border disclosure with the permission of the person concerned. The person must be expressly informed that their information may not be given the same protection as provided by the New Zealand Privacy Act.

View Principle 12 in the Privacy Act 2020 here.

Principle 13 - Unique identifiers

Principle 13 states that an organisation can only use unique identifiers when it is necessary.
An organisation cannot assign a unique identifier to a person if that unique identifier has already been given to that person by another organisation.

Organisations must take reasonable steps to protect unique identifiers from misuse.

Unique identifiers are individual numbers, references, or other forms of identification allocated to people by organisations, such as driver's licence numbers, passport numbers, or IRD numbers.

View Principle 13 in the Privacy Act 2020 here.

Privacy Act Requests

The Privacy Act provides that Council must respond to a Privacy Act request within 20 working days after receiving the request or transfer the request to another agency within 10 working days.

All Privacy Act requests, regardless of how they're made, trigger the same obligations under the Privacy Act.

- Council has:
  - Request for Personal Information Procedure
  - Privacy Breach Procedure
    - Privacy breaches will be treated as Critical Incidents as per the Incident and Problem Management Procedure
- The LGOIMA Request Training and Induction Guidelines cover the differences between a LGOIMA Request Procedure and Request for Personal Information Procedure under the Privacy Act.

More information:

- Office of the Privacy Commissioner — homepage
- Office of the Privacy Commissioner — Access to personal information (principle 6)

Council's Responsibility

Our customers need to have trust and confidence in the way government manages their personal information.

Privacy Officers

The Privacy Act requires all private and public sector agencies to have a Privacy Officer.

A Privacy Officer will:

- Be familiar with the privacy principles in the Privacy Act, relevant privacy codes and other legislation, and work to ensure compliance with them
- Deal with any privacy incidents and breaches, complaints about possible privacy breaches, and requests for access to personal information
- Act as the Councils liaison with the Office of the Privacy Commissioner
- Promote privacy awareness and training within Council
- Advise Council on the potential privacy impacts of changes to Council's business practices and how improving privacy practices might improve the business

To fulfil these responsibilities the Privacy Officer needs to develop, implement, and maintain a privacy programme. That programme is outlined within this Privacy Plan.

Core Expectations

The Government Chief Privacy Officer (GCPO) has issued core expectations that represent good practice for privacy management and governance. Meeting these core expectations will align Council's privacy practices with the Privacy Act's Information Privacy Principles.

The Privacy Maturity Assessment Framework (PMAF) has been developed to help agencies meet these core expectations.

Government Support

The Government Chief Privacy Officer (GCPO) supports agencies to implement these core expectations and provides advice on core expectations, PMAF and self-assessment.

- Government Chief Privacy Officer

Annual Privacy Self-assessments

The Privacy Maturity Assessment Framework (PMAF) forms the basis of the privacy self-assessment that the GCPO requires agencies to complete annually. The GCPO uses the completed self-assessment to report to the Minister of State Services on public sector-wide capability and maturity as required to by Cabinet.

Māori-Crown Relationship and Treaty Obligations

The inclusion of Māori perspectives and cultural values can improve Māori trust and confidence in the handling of their personal and collective information.

Effective engagement is key to producing better quality outcomes and realising Māori-Crown partnerships.

Benefits

Engaging with Māori contributes to:

- Improving agencies' understanding of Te Ao Māori (Māori world views) when handling personal and collective information
- Developing a partnership with Māori that supports the development of effective policy options through greater awareness and understanding of the issues and opportunities
- Help deliver improved outcomes and wellbeing for Māori.

Good engagement should complement other ways an agency collects personal information and data to deliver services to New Zealanders.

Engagement principles

Council has statutory obligations to engage with specific groups. Engagement should not be limited to achieving formal obligations. Processes that consider Māori participation and views are likely to be more effective.

Following Te Arawhiti's guidance: Te Arawhiti — values of engagement , throughout the development of an engagement process Council should be guided by the following principles:

- Engage early
- Be inclusive
- Think broadly.

Privacy by Design

Privacy by Design can help Council meet the Government Chief Privacy Officer's core expectations. Privacy by Design is a design methodology that includes privacy as an essential priority of any product, service, system, or process.

Privacy is embedded throughout the product or service lifecycle from design to disposal. The benefits of using Privacy by Design include:

- Increased awareness of privacy and handling of personal information across an agency's projects, products, services, systems, or processes
- Early identification and resolution of potential privacy risks and issues (when it's simpler and less costly to do so)
- Greater assurance of meeting the Information Privacy Principles of the Privacy Act

The 7 principles for Privacy by Design:
These principles and the philosophy and methodology they express can be applied to specific technologies, business operations, physical architectures, networked infrastructure, and entire information ecosystems.

The key to instilling Privacy by Design principles is to undertake ongoing communication and education with senior leadership, colleagues, and staff.

1. Proactive not reactive, preventative not remedial	•Privacy needs to be part of the planning of any new or updated product, service, system or process. Privacy considerations should help drive the design rather than being bolted on at the end to address a few privacy risks.
2. Privacy as the default	•The default setting of any design should protect the individual's personal information by understanding how the Information Privacy Principles apply in this context.
3. Privacy embedded into design	•Privacy should be so integral to the design of the product, service, system or process that it would not function without the privacy-preserving functionality.
4. Full functionality — positive-sum, not zero-sum	•Design requirements to protect personal information should be treated as an opportunity to design a better product, service, system or process, not as a trade-off with other functionality.
5. End-to-end security — lifecycle protection	•Protection and security of personal information should be considered for every stage of the information lifecycle: collection, storage and security, use, access and correction, disclosure, retention and disposal.
6. Visibility and transparency	•How the product, service, system or process will use the personal information needs to be clear to the individual providing the personal information. The accompanying privacy notice should be written in easy-to-understand, audience-appropriate language.
7. Respect for user privacy — keep it user-centric	•At the centre of any design for product, service, system or process is a person who will use that product, service, system or process. It's that person who will bear the harm and impact of any privacy breach or misuse of their personal information.

Privacy Risk

Information Services manages it’s risks as per the Risk Management Policy. Risk management forms of Information Services Activity Management Plan.
For a detailed view of the Information Services Risk Register (Doc ID: 447956), please click here.
The following is an extract from the Information Services Risk Register:

Risk description	Risk driver	Risk consequence	Residual risk	Risk management plan/control
The risk register and plan will be updated following the Executive Team review.				

Privacy Maturity Assessment Framework

The Government Chief Privacy Officer has developed the Privacy Maturity Assessment Framework (PMAF) to help Council assess their privacy capability and maturity.

The Government Chief Privacy Officer (GCPO) leads an All-Of-Government (AOG) approach to privacy to raise public sector privacy maturity and capability. The connection between good privacy practice, public trust and the quality of the services government delivers is critical to ensure that public services are trusted and accessible by those who need them.

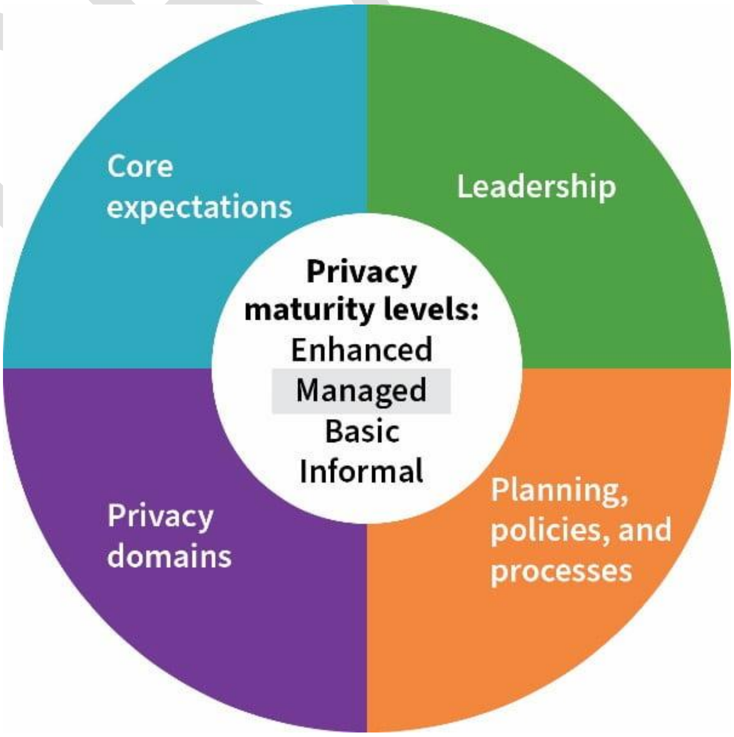
The GCPO developed the PMAF to help Council understand its current level of privacy capability, assess the maturity in managing personal information, and identify where Council can improve.

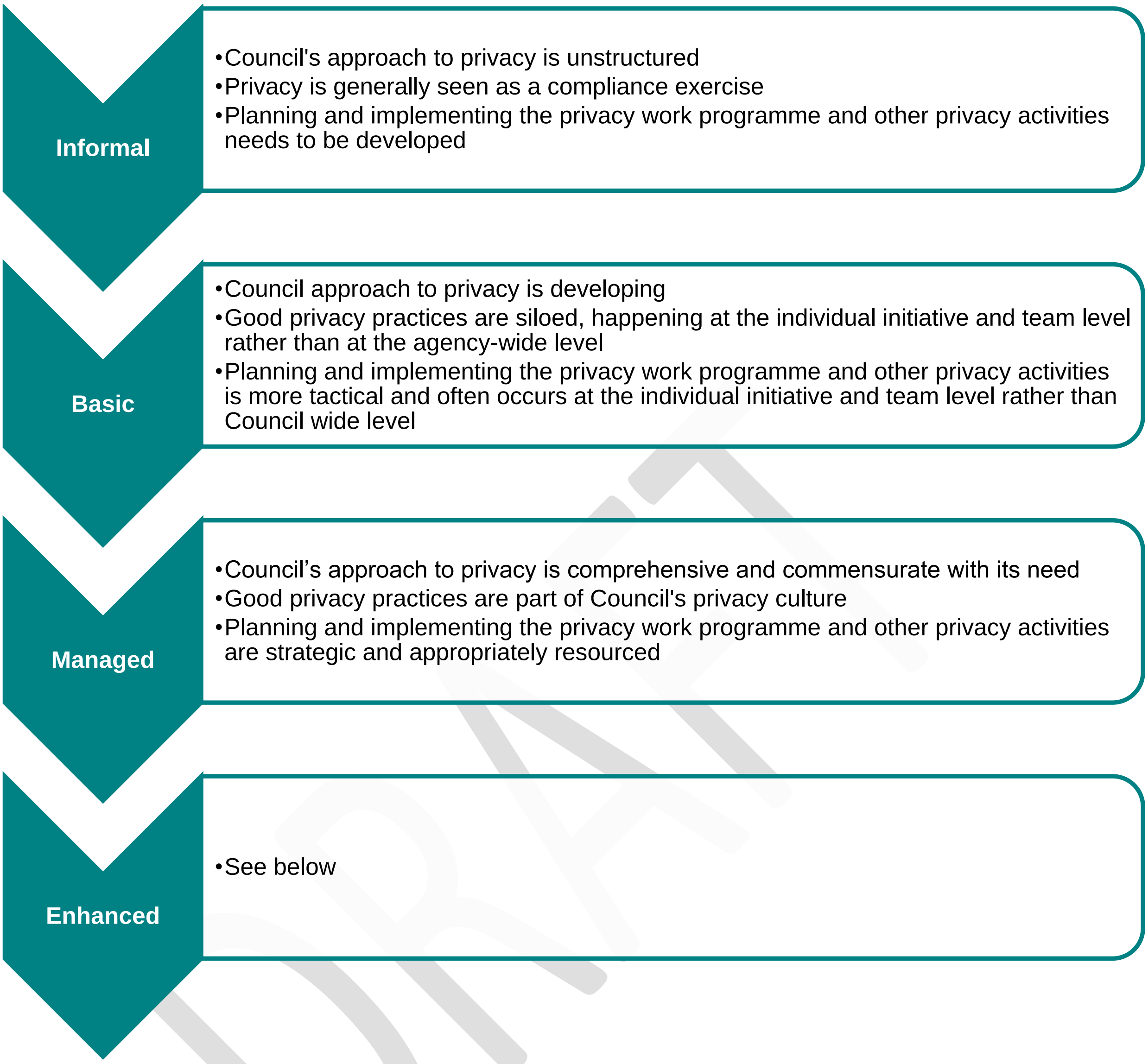
The PMAF also asks Council to think about the legitimate interests that communities have in data they consider 'personal' in a broader sense, often because it is derived from their personal information.

PMAF sections:
The PMAF is made up of 4 sections in which Council will assess its privacy capability and maturity. Each section is made up of elements and each element has 1 to 3 criteria:

- Core expectations (5 elements)
- Leadership (3 elements)
- Planning, policies, and practice (2 elements)
- Privacy domains (6 elements).

PMAF maturity levels
The PMAF has 4 maturity levels:





Informal

- Council's approach to privacy is unstructured
- Privacy is generally seen as a compliance exercise
- Planning and implementing the privacy work programme and other privacy activities needs to be developed

Basic

- Council approach to privacy is developing
- Good privacy practices are siloed, happening at the individual initiative and team level rather than at the agency-wide level
- Planning and implementing the privacy work programme and other privacy activities is more tactical and often occurs at the individual initiative and team level rather than Council wide level

Managed

- Council's approach to privacy is comprehensive and commensurate with its need
- Good privacy practices are part of Council's privacy culture
- Planning and implementing the privacy work programme and other privacy activities are strategic and appropriately resourced

Enhanced

- See below

The Government Chief Privacy Officer (GCPO): The managed maturity level is usually the appropriate maturity level for an agency to achieve and sustain.

The managed maturity level is usually the appropriate maturity level for an agency to achieve and sustain.

However, Council may determine that it needs to adopt and implement enhanced privacy measures for certain elements of the framework based on its assessment of a variety of factors.

Some factors to consider would be about the personal information Council collects, uses and shares:

- Scale or volume of the personal information: if a privacy incident occurs, the volume of people affected may be large
- Nature or class of personal information: if a privacy incident occurs, the potential or actual harm to people affected may be significant
- In-depth personal information about an individual(s): if a privacy incident occurs, the potential or actual harm to the individual(s) affected may be significant

- Volume of inter-agency transfer of personal information: if an agency, as part of its regular operations, shares or receives a significant volume of personal information with/from other agencies, the challenges of managing and protecting personal information may be greater
- Volume of cross-border transfer of personal information: if the agency has offices, staff and/or third-party suppliers around the world, the challenges of managing and protecting personal information may be greater.

Other factors to consider would be about what Council would like to achieve through its collection, use and sharing of personal information:

- To demonstrate trustworthiness more richly to stakeholders and clients/customers, especially a group of people or a community has lower level of trust in government's collection and use of their personal information by enhancing core expectation 1 - (take a people-centred approach)
- To be able to more confidently support opportunities to use personal information to improve outcomes by enhancing core expectation 3 - (build and maintain privacy capability) and privacy domain 6 - (enable personal information use, reuse and sharing)
- To do information sharing with several other agencies, NGOs, iwi, and third-party suppliers when required or asked to do so to meet government objectives by enhancing privacy domain 6 - (enable personal information use, reuse and sharing) and planning, policies, and practice 2 - (competent practice)
- To support business plans to utilise new or emergent technologies (for example, artificial intelligence, facial recognition software) by enhancing privacy domain 2 - (ensure the use and storage)
- To develop high-quality privacy practices that can be shared with other agencies and raise system capability and maturity.

Council will decide what enhanced privacy measures it will adopt and implement depending on the situation being addressed. Some possible measures could be:

- Embedding Privacy by Design by having the privacy team as part of project teams that meet the agency's criteria for enhanced privacy maturity
- Developing internal capability to do complex Privacy Impact Assessments which gives the agency greater connection to the design and implementation of a project or initiative
- Establishing data information governance group for personal information that may require enhanced privacy measures
- Establishing escalation procedures (which are tested regularly) that documents clearly how and to whom staff, contractors and third-party suppliers should raise privacy questions. Building expertise in the privacy team and key staff through certifications, extra training, etc.
- Building greater privacy expertise among staff, contractors, and third-party suppliers
- Developing the ability to rapidly address any increased need for privacy expertise through a responsive delivery of pre-packaged training materials
- Assessing proactively and periodically clients'/customers' understanding and perceptions of the transparency and trustworthiness of the agency's privacy practices.

Framework Sections, Elements and Criteria

The following table has been populated from: Complete a self-assessment | NZ Digital government

Section	Elements	Scope	Criteria	Informal	Basic	Managed
Core expectations	**1. Take a people-centred approach**	Take a people-centred approach to privacy that is respectful of those the information is about and provides the public with effective services. **Guidance note:** A people-centred approach is one that seeks to understand, invite, and act on the perspectives and interests of the people that the personal information is about when planning and undertaking activities and actions to collect, use, or share their personal information. Based on extensive engagement across the social sector, the principles of the Data Protection and Use Policy focus on how to develop a way of working that respects people, their personal information, and their stories.	**Criteria 1: Having a people-centred privacy programme**	Privacy policies and practices are compliance-centric and risk-centric with limited focus on the impact of decisions about use of personal information on the people that the information is about.	Privacy policies and practices include recommendations to consider the views of the people that the information is about. The privacy programme has no specific focus on instilling a people-centred perspective.	The Data Protection and Use Policy's principles are appropriately integrated with privacy policies and practices, and the privacy programme focuses on change initiatives to embed a people-centred approach.
			Criteria 2: Connecting with service users	Individual initiatives infrequently connect with service users to test new ideas with them about collection or use of their personal information.	Individual initiatives connect with service users or their representatives to include their views in decision-making processes about collection and use of their personal information. There is little guidance for initiatives about when and how to go about it.	There are established processes and easy-to-use methods for connecting with service users or their representatives, when appropriate, to include their views in decision-making processes about collection and use of their personal information.
			Criteria 3: Being transparent	Transparency is limited to general clauses in consent forms or privacy notices/statements used at the initiation of the relationship with service users.	Individual initiatives focus on transparency about why and how people's information is collected, used, or shared, and what choices they have.	The agency is transparent about: • what kinds of personal information it collects and uses? • why and how it's used

Section	Elements	Scope	Criteria	Informal	Basic	Managed
		Key features of such an approach are inclusion and participation in the development of new ideas, making it easy to understand what's happening and making it easy for people to access and request correction to their information. [Data Protection and Use Policy](#)		The approach to enabling people to access their information and request correction is ad-hoc or reactive.	Information about how people can access, and request correction of their information is available but is not easy for service users to understand or execute.	• choices people may have and how to access and request correction to their personal information. • This information is presented in easy-to-understand ways.
	2. Build and maintain a privacy culture	Build and maintain a privacy culture that embodies the public service values of being impartial, accountable, trustworthy, respectful, and responsive. **Guidance note:** It's not always clear or easy to understand how actions taken with personal information can support (or undermine) public service values. To build and maintain a privacy culture, leaders and managers can help by establishing and informing that	**Criteria 1: Creating a privacy culture**	Leadership has little involvement in the development of a privacy culture.	Leadership recognises the importance of building a privacy culture and focuses on specific areas of the agency or individual initiatives.	Leadership delivers consistent and positive messages about how privacy is everyone's responsibility and how privacy is an enabler of public trust and quality service delivery. Privacy culture is periodically assessed, possibly as part of a broader organisational culture survey.
			Criteria 2: Communicating privacy values and aspirations	Communication from senior leadership and privacy leaders is ad-hoc or reactive and focuses on specific events and incidents.	Senior leadership and privacy leaders communicate the agency's privacy values and aspirations as part of specific	Senior leadership and privacy leaders communicate the agency's clearly defined privacy values and aspirations in relevant terms throughout the

Section	Elements	Scope	Criteria	Informal	Basic	Managed
		understanding, so that people throughout the agency are better placed to appreciate this crucial linkage. Helping people to appreciate the nature of this connection and motivating them to act on that appreciation can encourage the implementation of privacy practices that express these values.			initiatives and/or work programme.	agency on a schedule that is proportionate to the agency's needs.
			Criteria 3: Developing privacy awareness	Privacy awareness is ad-hoc or reactive to specific events and incidents.	Privacy awareness is limited and is seen as the responsibility of a few managers and specialists.	Privacy awareness clearly communicates the agency's values, expectations and behaviours to staff and contractors, and promotes the use of Privacy by Design.
	3. Build and maintain privacy capability	Build and maintain privacy capability so that people have the knowledge and skills they need to contribute to good privacy practice. **Guidance note:** Privacy training is the foundation for building privacy capability and an effective privacy culture. Privacy training isn't about trying to make everyone experts in the letter of the law. It's to provide staff and managers with the knowledge and tools to adopt and apply the	**Criteria 1: Conducting privacy training**	Privacy training for staff and contractors is conducted on an ad-hoc basis.	At induction, staff, and sometimes contractors, receive privacy training on the agency's privacy values, policies, practices, and risks.	At induction and then on a regular basis, staff and contractors receive privacy training on the agency's privacy values, policies, practices and risks that is relevant to their roles and supports them to be effective and trusted custodians of personal information.
			Criteria 2: Monitoring and updating privacy training	Updates to privacy training content is ad-hoc.	Privacy training content is updated periodically.	Privacy training needs are monitored, and training content is reassessed to ensure that it remains fit for purpose.
			Criteria 3: Providing	There is little or no additional training for staff and contractors	Staff may have additional training before they are given	Staff and contractors know how to access appropriate advice that

Section	Elements	Scope	Criteria	Informal	Basic	Managed
		appropriate privacy concepts and principles to their work. People are more likely to retain the training they've been exposed to if it's relevant to what they see daily. People change roles or their current role may acquire additional responsibilities, so privacy training is an ongoing activity throughout their career at the agency.	**additional privacy training**	before they are given access to certain classes of personal information (for example, health information) that may fall under a Privacy Code and/or may require additional privacy knowledge to manage properly.	access to certain classes of personal information (for example, health information) that may fall under a Privacy Code and/or may require additional privacy knowledge to manage properly. Contractors generally do not have additional training.	they should understand before they are given access to certain classes of personal information (for example, health information) that may fall under a Privacy Code and/or may require additional privacy knowledge to manage properly.
	4. Establish a sense of collective responsibility	Establish a sense of collective accountability in which managers and staff understand their duty to ensure that personal information is collected and used appropriately. **Guidance note:** Sometimes privacy is seen as the specialised domain of a particular team.	**Criteria 1: Implementing privacy practices**	Adoption of privacy policies and practices by functional areas that collect or make use of personal information (for example, procurement, service design, contracting and funding, analysis, and research, etc) is ad-hoc, and tends to rely on the privacy officer/team involving themselves directly.	Some functional areas that collect or make use of personal information (for example, procurement, service design, contracting and funding, analysis, and research, etc) may reference, or integrate with, privacy policies and practices.	Functional areas that collect or make use of people's personal information (for example, procurement, service design, contracting and funding, analysis, and research, etc) include recognised good practice advice (for example, Data Protection and Use Policy (DPUP) in their core processes.
		However, all the following originate outside of privacy teams: designing a new service,	**Criteria 2: Linking privacy to**	There is no link between organisational value frameworks, such as	Organisational value frameworks, such as mission statements, include a focus on	Organisational value frameworks, such as mission statements, draw a direct line

Page **21** of **57**

Section	Elements	Scope	Criteria	Informal	Basic	Managed
		product, policy, or process, working with third party suppliers and providers, general custodianship of information and information systems, and using personal information to inform new actions. This expectation is about weaving a coherent and explicit understanding of that distributed network of activities and accountabilities, so good privacy practices can be a regular and normal feature of how the agency does its work.	**organisational values**	mission statements, and the importance of public trust in the use of personal information.	public trust, but the connection with respectful and transparent practice in the collection and use of personal information is not clear.	between delivering quality service and exercising a collective focus on respectful and transparent practices in the use of personal information.
			Criteria 3: Including privacy in employment	Letters of employment and job descriptions do not reference privacy obligations and responsibilities. There is no clear link made between privacy capability and its role in developing and retaining public trust.	Some letters of employment and job descriptions reference privacy obligations and responsibilities. There may be a link made between privacy capability and its role in developing and retaining public trust.	Letters of employment and job descriptions reference privacy obligations and responsibilities to develop and retain public trust in the collection and use of personal information.
	5. Be a capable Treaty partner	Be a capable Treaty partner by supporting the Crown to fulfil its stewardship responsibility and strengthen Crown's relationships with Māori. **Guidance note:** The Public Service Act 2020 highlights the responsibility of agencies to support the Crown in its Treaty obligations, and to	**Criteria 1: Identifying Māori privacy interests**	There is little awareness of the need to identify Māori interests when designing or updating a service or process that involves the collection, use or sharing of personal information.	When designing or updating a service or process that involves the collection, use or sharing of personal information, individual initiatives develop their own practices to identify Māori interests.	When designing or updating a service or process that involves the collection, use or sharing of personal information, the agency has policies and practices that can identify relevant Māori interests.
			Criteria 2: Partnering with Māori	The agency's identification of and response to Māori privacy interests is ad-hoc or reactive.	When Māori privacy interests have been identified, individual initiatives define their own approach for	When Māori privacy interests have been identified a partnership approach is used and provides for personal

Section	Elements	Scope	Criteria	Informal	Basic	Managed
		develop and maintain its capability to engage with Māori and understand Māori perspectives. Decisions to collect and use personal information can often involve material interests for Māori. This is increasingly so with the growth in interest and activities to use data, often originating from personal information, to improve how an agency thinks about and acts on public service imperatives. This expectation highlights the importance of considering these factors and developing enabling privacy practices such as advice as provided by Te Arawhiti and Statistics NZ: • Te Arawhiti — Guidelines for engagement with Māori			understanding and responding to those interests.	information to be interpreted with reference to Māori priorities, values, and worldviews.

Section	Elements	Scope	Criteria	Informal	Basic	Managed
		- Data.govt.nz — Ngā Tikanga Paihere				
Leadership	**1. Effective oversight**	Effective oversight for privacy practice through effective governance. **Guidance note:** The success of an agency's activities to build a privacy culture, develop privacy capability and implement its privacy programme requires governance and oversight by the senior leadership/executive team. Ensuring that the privacy officer provides regular updates and can discuss the agency's various privacy activities with the senior leadership/executive team, increases the likelihood of a successful, appropriate, and efficient implementation of these activities. An agency will have existing oversight structures and practices,	**Criteria 1: Privacy reporting**	Senior leadership/executive team has little awareness of, or pays little attention to, privacy and its management.	Privacy officer engages with the senior leadership/executive team, governance board and/or committees when there are specific issues and events that need to be addressed.	The privacy officer has regular updates and discussions with the senior leadership/executive team, governance board and/or committees on the agency's privacy culture and values, privacy strategy and programme, and privacy issues and risks.
			Criteria 2: Privacy and risk management	People have an idea of who is responsible for aspects of privacy. Day-to-day functional leadership responsibilities have not been clearly assigned and privacy is not integrated into the agency's risk management structure.	A senior leader has been assigned responsibility for functional oversight for privacy, though privacy is not integrated into the agency's risk management structure.	Functional oversight for privacy and its work programme is integrated into the risk management organisational structure and includes monitoring compliance.

Page **24** of **57**

Section	Elements	Scope	Criteria	Informal	Basic	Managed
		and these will be the natural starting point for designing and implementing effective oversight of privacy activities and the monitoring processes that support and enable effective oversight.				
	2. Delivery of objectives	Delivery of objectives through management structure, roles and responsibilities, and the capacity to achieve these objectives. **Guidance note:** The working structure of people, teams and accountabilities are what a privacy officer/team rely on to get suitable visibility into the progression of the privacy work programme to achieve the agency's privacy objectives. With this visibility, privacy advice, support and direction can be provided as needed.	**Criteria 1: Responsibility and accountability**	Responsibility and accountability for the implementation of the privacy strategy and work programme are unclear or absent.	The responsibility and accountability for the implementation of the privacy strategy and work programme is seen as the sole responsibility of the privacy officer/team and is not suitably distributed throughout the agency to ensure their implementation and the application of Privacy by Design principles.	Formal line management and governance includes responsibility and accountability for implementation of the privacy strategy and work programme. These responsibilities are suitably distributed throughout the agency to ensure their implementation and the application of Privacy by Design principles.
			Criteria 2: Resourcing	Resourcing for privacy staff and activities is ad-hoc and not commensurate with the agency's privacy profile and privacy work programme.	Resourcing for privacy staff and activities is planned at the individual initiative level.	Resourcing for privacy staff and activities is considered at a strategic level within the agency and is commensurate with the agency's privacy profile and privacy work programme.

Section	Elements	Scope	Criteria	Informal	Basic	Managed
		Project teams, new initiatives, planners, and resource managers need to understand what and how they contribute to these objectives and know that these objectives are linked to organisational priorities. For senior leadership/executive team to have confidence that privacy objectives will be met, having the right resourcing, both in number and capability, is essential.	**Criteria 3: Oversight and visibility**	Privacy activities are ad-hoc or reactive.	Because privacy objectives are planned at the individual initiative level, the privacy officer/team is not able to have sufficient visibility and oversight of the initiatives that need to deliver privacy objectives.	The privacy officer/team oversees the privacy work programme, maintains central oversight of privacy initiatives and activities on an agency-wide basis, communicates regularly with other related functions (for example, information management, security, risk management), and has clear alignment (where applicable) with their work programmes.
	3. Confidence in organisational progress	Confidence in organisational progress through appropriate monitoring and assurance practices. **Guidance note:** The integration of monitoring and assurance practices with the conduct of privacy activities is a key element of good practice for the same reasons that monitoring, and assurance are used in any other areas of an agency's business.	**Criteria 1: Privacy and assurance**	The agency adopts and implements the first of the 3 lines of defence: • First line: Business processes are designed to mitigate residual privacy risk to within the agency's risk tolerance.	The agency adopts and implements 2 of the 3 lines of defence: • First line: Business processes are designed to mitigate residual privacy risk to within the agency's risk tolerance. • Second line: Privacy and risk activities are integrated with the wider system of internal controls as part of the agency's	Privacy and assurance staff work together to adopt and implement the 3 lines of defence for privacy, as appropriate: • First line: Business processes are designed to mitigate residual privacy risk to within the agency's risk tolerance. • Second line: Privacy and risk activities are integrated with the wider system of internal controls as

Section	Elements	Scope	Criteria	Informal	Basic	Managed
					assurance framework.	part of the agency's assurance framework. - Third line: Internal audits or other equivalent independent assurance practices evaluate and improve the agency's privacy risk management, control, and governance processes.
Planning, policies, and practice	**1. Strategy and planning**	Formulate a privacy approach, a strategy for achieving it and a roadmap to bring it to life. **Guidance note:** An agency's privacy approach describes in simple terms 'how privacy gets done'. It's a high-level description of roles and responsibilities, core business processes that 'do the doing' and the owners of those processes, and an outline of how the approach is governed and monitored.	**Criteria 1: Planning**	Privacy planning is ad-hoc or reactive to specific events and incidents.	Privacy planning is seen as the domain of the privacy officer/team with little or no connection to the rest of the organisation.	Privacy planning includes all areas of the agency, comprehensively addresses the collection, use, storage, and security of personal information, and is flexible to accommodate changes either in the wider business environment or the result of assurance activity.
			Criteria 2: Planning documents	The agency does not have privacy planning documents (for example, strategy, roadmap, and work programme).	The agency has privacy planning documents (for example, strategy, roadmap, and work programme) which are reviewed regularly.	Privacy planning documents (for example, strategy, roadmap, and work programme) are easy to understand, communicated to those with relevant

Section	Elements	Scope	Criteria	Informal	Basic	Managed
		The privacy strategy sets coherent objectives for where the agency wishes to get to with its privacy practices and describes the key areas of activity that will achieve these objectives. These objectives will work well if they are targeted and make sense in the context of the agency's overall privacy stance and risk profile rather than being generic or overly broad. The strategy would specify its time horizon, scheduled updates, and the audiences who are expected to understand and support the subsequent roadmap of activities. If the strategy is an expression of the objectives, then the roadmap describes how to travel between the current state and the future state.				responsibilities, and reviewed regularly to ensure that they remain relevant and aligned with the agency's organisational and system context (nature, scale, and risk).
			Criteria 3: Reporting	Reporting is ad-hoc and is about specific events and incidents.	Progress towards privacy strategy, roadmap and work programme is reported to senior leadership and relevant governance bodies on an initiative basis.	Progress towards privacy strategy, roadmap and work programme is tracked and reported regularly to senior leadership and relevant governance bodies.

Section	Elements	Scope	Criteria	Informal	Basic	Managed
		A roadmap would include what set of activities to be undertaken; their dependency, timing, and duration; and accountabilities and resourcing to deliver the strategy's objectives. These planning documents 'carry the message' to others about where the agency is headed with privacy, why those are the objectives, and its intentions to deliver them. Making these documents easy to understand and engage with will allow the teams who contribute to those activities to achieve the agency's privacy objectives.				
	2. Competent practice	Have policies to equip managers and staff to play their part in achieving the core expectations. **Guidance note:** People can work with personal information	**Criteria 1: Policies**	Privacy policies are insufficient to meet the agency's privacy needs, are communicated on an ad-hoc or reactive basis and are not regularly reviewed.	Privacy policies meet the agency's privacy needs. They are used by individual initiatives or within a subset of core business processes (such as procurement,	Privacy policies are easy to understand, communicated and accessible throughout the agency, and reviewed regularly to ensure that they remain relevant and aligned with the agency's needs

Page **29** of **57**

Section	Elements	Scope	Criteria	Informal	Basic	Managed
		with greater confidence if they know what do to, when to do it and who to contact for support and advice. Project teams, policy teams, service designers and others can use privacy policies to help them think about their activities and tasks that involve personal information in the context of the work carried out by those various teams. Privacy policies also need to include and extend to contractors, partners and suppliers who may be involved in working with personal information. Their needs and requirements may be different than those of internal staff. Anyone who is expected to contribute towards good privacy practices should also be confident that, having understood the expectation, they can readily equip			policy/service design, front-line operations and management, analysis, and research) but are not explicitly aligned to agency needs, accounting for nature, scale, and risk.	— accounting for nature, scale, and risk.
			Criteria 2: Contracts	The inclusion of privacy policies in procurement contracts is ad-hoc or reactive.	The agency's procurement contracts sometimes include terms and conditions relating to privacy policies and practices, but this happens at the individual initiative level and is not a standard practice.	The agency's procurement contracts include standard terms and conditions relating to privacy, and privacy policies include advice on external suppliers and personal information.

Section	Elements	Scope	Criteria	Informal	Basic	Managed
		themselves to act on it through access to practical, documented descriptions of what contribution they need to make.				
Privacy domains	**1. Require a clear understanding of the purpose**	Require a clear understanding of the purpose and necessity of the collection, use and sharing of personal information. **Guidance note:** Clarity of purpose is vital to determining whether an agency needs to collect personal information and, if so, what personal information is needed to meet the purpose. It's also vital to determine whether the ways in which an agency intends to use and share the information are lawful, appropriate and supports public service values. Clarity of purpose is the anchor for many other things, such as consent forms, privacy	**Criteria 1: Defining the purpose Criteria**	The agency's advice on defining the purpose for the collection, use, or sharing of personal information is ad-hoc or reactive.	The agency's guidance on defining the purpose for the collection, use, or sharing of personal information is compliance-focused and risk-focused.	The agency has appropriately integrated the Data Protection and Use Policy's 'Purpose Matters' guideline to accurately define purposes for collection, use, or sharing of personal information for projects and business processes. • Data Protection and Use Policy — Purpose Matters Guideline • Data Protection and Use Policy — Understand why
			Criteria 2: Identifying choices	It's unusual to offer any choices to service users, and if it is done, it's ad-hoc or reactive.	Steps to identify practical choices that service users may be given regarding the collection or use of their personal information are taken by individual initiatives.	When purposes have been suitably well-defined, additional processes are explicitly applied to identify when and how choices may be offered or accommodated, in line with both the Data Protection and Use Policy's 'Purpose

Section	Elements	Scope	Criteria	Informal	Basic	Managed
		statements, privacy impact assessments, and more.				Matters' and 'Transparency and Choice' guidelines. • Data Protection and Use Policy — Purpose Matters Guideline • Data Protection and Use Policy — Transparency and Choice
			Criteria 3: Reducing personal information	Any steps to reduce or eliminate the need for collection or use of personal information are applied on an ad-hoc or reactive basis.	Steps to reduce or eliminate the need for the collection or use of personal information are taken by individual initiatives. Existing practice is rarely re-examined. It's generally assumed that if information is being collected, it's still reasonable to collect it.	When creating or updating a service or process, consideration is given to eliminating or reducing the need for personal information by ensuring that its collection, use, and sharing are needed to accomplish the stated outcomes. Existing practice is not used as a justification for continued collection and use.
	2. Ensure the use and storage of personal information	Ensure the use and storage of personal information protects against inappropriate access, use, and modification, whilst also ensuring effective and efficient support for its intended use.	**Criteria 1: Implementing Privacy by Design**	Privacy, ICT, information management and other responsible teams work in silos when building and updating processes, products, and services.	Privacy, ICT, information management and other responsible teams have limited engagement when building and updating processes, products, and services.	Privacy, ICT, information management and other responsible teams work together to incorporate Privacy by Design methodology and principles when building and updating

Section	Elements	Scope	Criteria	Informal	Basic	Managed
		Guidance note: Privacy by Design foundational principles serve as an overarching framework for inserting privacy and data protection early, effectively, and credibly into information technologies, organisational processes, networked architectures and entire systems of governance and oversight. Privacy by Design seeks to raise the bar for privacy by promoting enhanced accountability and user trust. If Privacy by Design provides the 'what' to do, then privacy engineering provides the 'how' to do it. Privacy engineering is the discipline of understanding how to include privacy as a non-functional requirement in systems engineering. While privacy may also appear as a functional requirement of a given system, for most				processes, products, and services.
			Criteria 2: Implementing privacy engineering	Privacy and ICT staff have no knowledge and understanding of using privacy engineering to address privacy considerations.	Privacy and/or ICT staff may have some knowledge and understanding of using privacy engineering to address privacy considerations. When building and updating processes, products and services, individual initiatives have privacy and ICT staff work together to incorporate the privacy engineering objectives of predictability, manageability and dis-sociability by using privacy design strategies (for example, minimise, hide, separate, aggregate, inform, control, enforce and demonstrate).	When building and updating processes, products and services, privacy and ICT staff work together to incorporate the privacy engineering objectives of predictability, manageability and dissociability by using privacy design strategies (for example, minimise, hide, separate, aggregate, inform, control, enforce and demonstrate).

Section	Elements	Scope	Criteria	Informal	Basic	Managed
		systems privacy is ancillary to the primary purpose of the system. • [IAPP — Privacy Engineering: Proactively Embedding Privacy, by Design]()				
	3. Make it easy for people to access	Make it easy for people to access and request correction to their information. **Guidance note:** People may not understand what rights they must see the personal information that has been collected about them, to ask for that information to be corrected, or to express a preference as to how they'd like to access their information. Ensuring that people understand these rights helps build public trust and confidence. Lack of this understanding may deter people from providing their personal information and receiving a service they need.	**Criteria 1: Having a process**	The approach to responding to access requests is ad-hoc or reactive, and it's not easy for clients to find or understand how to do this.	Customers and clients can find a process to make an access request, but it's not clear if they find it easy to use.	Customers and clients can easily find and understand the process to make an access request.
			Criteria 2: Monitoring the process	Access request responses are done on an ad-hoc basis with no systematic monitoring.	The agency has an access request process. The requesters and the agency have little visibility of whether the access requests responses are meeting the legislative requirements.	The agency has a customer-centred access request process that incorporates the Data Protection and Use Policy's 'Access to Information' guideline. The agency monitors and ensures that access request responses meet the legislative requirements and supports the agency's reputation as an effective and trusted custodian of New Zealanders' personal information. • [Data Protection and Use Policy — Access]()

Page **34** of **57**

Section	Elements	Scope	Criteria	Informal	Basic	Managed
		For people to act on these rights, the process to do so needs to be easy to understand and use. For an agency to respond to these requests, their systems and processes need to be able to support responding within the legislative timeframe.				to Information Guideline
			Criteria 3: Reviewing the process	Actions to improve the process for responding to access requests are ad-hoc or reactive.	Consideration of easy access and collation of personal information to enable timely responses to access requests rests with individual initiatives.	Information management and ICT system reviews explicitly include consideration of easy access and collation of personal information to enable timely responses to access requests.
	4. Understand and assess privacy risks	Understand and assess privacy risks and manage commensurately. **Guidance note:** An agency's work to develop, implement, and improve its privacy practices is best informed by a suitable understanding of its risk position, which in turn is dependent on a suitable understanding of the types of personal information it holds, why it's collected, and how it's used and shared. This understanding needs to be based on a holistic picture of the agency's holdings and	**Criteria 1: Knowing the agency's risks**	Privacy risks are not assessed or are assessed for specific events and incidents.	Privacy risks are assessed based on little understanding and knowledge of personal information holdings and the collection, uses, sharing activities, and storage of personal information.	Privacy risks are assessed based on an understanding and knowledge of personal information holdings, focusing on collection, uses, sharing activities, and storage.
			Criteria 2: Managing agency's risks	Agency privacy risk assessments, which provide a snapshot of an agency's current privacy risks, are not done.	Agency privacy risk assessments, which provide a snapshot of an agency's current privacy risks, are siloed within the privacy team and are not part of the agency's overall risk assessment.	Agency privacy risk assessments, which provide a snapshot of an agency's current privacy risks and how it will manage them as an organisation, are part of the agency's overall risk assessment, and are conducted and reviewed periodically.
			Criteria 3: Managing project risks	Project risk assessments, which are done to assess	Project risk assessments are done to assess the privacy	Project risk assessments are done to assess the privacy

Section	Elements	Scope	Criteria	Informal	Basic	Managed
		activities, not only about specific projects, and programmes of work. As privacy objectives are delivered and/or as the agency's holdings and activities change, updating and maintaining both the macro and micro risk pictures helps to draw a better line of sight between further actions taken to improve privacy practices.		the privacy risk of new or updated processes, products, or services, are done occasionally or not at all. The privacy team has little or no visibility of project privacy risks.	risk of new or updated processes, products, or services. Oversight by the privacy team and lines of ownership and accountability are not clear.	risk of new or updated processes, products, or services with the support of and oversight by the privacy team. They cover the whole information life cycle and have clear lines of ownership and accountability.
	5. Reduce the impact of privacy breaches	Reduce the impact of privacy breaches and incidents through good privacy practices. **Guidance note:** Managing privacy breaches begins with the 4 key steps of contain, assess, notify, and prevent. The effectiveness of these steps can be improved by: having clear roles and responsibilities in the incident management plan	**Criteria 1: Having a privacy incident register**	The agency may have a privacy incident register and/or a privacy incident response plan. Neither are reviewed regularly.	The agency has a privacy incident register and a privacy incident response plan. Learning from privacy incidents and breaches is done by individual initiatives.	The agency has: • a privacy incident register that is used by staff and/or privacy team • a tested privacy incident response plan (including partners and third parties) that is integrated into its business continuity planning • a process for learning from privacy incidents and breaches.
			Criteria 2: Minimising collection of	Consideration of whether personal information needs to	Consideration of whether personal information needs to	The agency collects only personal information that is

Page **36** of **57**

Section	Elements	Scope	Criteria	Informal	Basic	Managed
		regularly testing the plan, and integrating the plan into business continuity plans. Conducting tabletop exercises to test and validate the plan's activities will ensure that the plan will work as intended and familiarise the team with their role and responsibilities. The impact of breaches can be reduced by having practices that reduce the collection and retention of personal information.	**personal information**	be collected is based solely on compliance and risk assessments.	be collected and whether there are alternative ways to accomplish the desired outcome may be done by individual initiatives. Little or no review of the personal information already being collected is done when updating a process, product, or service.	clearly linked to the desired outcome and investigates alternative ways to accomplish the desired outcome that eliminates or reduces the need for personal information.
			Criteria 3: Retaining personal information	The retention and destruction of personal information is done on an ad-hoc basis.	The agency has information policy and practices that include the retention and destruction of personal information.	The agency has, maintains, and promotes information policy and practices that include the retention and destruction of personal information, and the destruction of personal information is authorised by the government's Chief Archivist.
	6. Enable personal information use, reuse and sharing	Enable personal information use, reuse and sharing to support a unified public service that provides the public with effective services. **Guidance note:** The Privacy Act 2020 and other related	**Criteria 1: Having policies**	Decisions to re-use or share personal information are made operationally and, on an ad-hoc or reactive basis.	Individual initiatives decide whether and how to re-use or share personal information, and this is primarily seen as a risk-based decision.	Information management and privacy policies include enabling advice on how to appropriately use and share personal information when individuals can be identified.

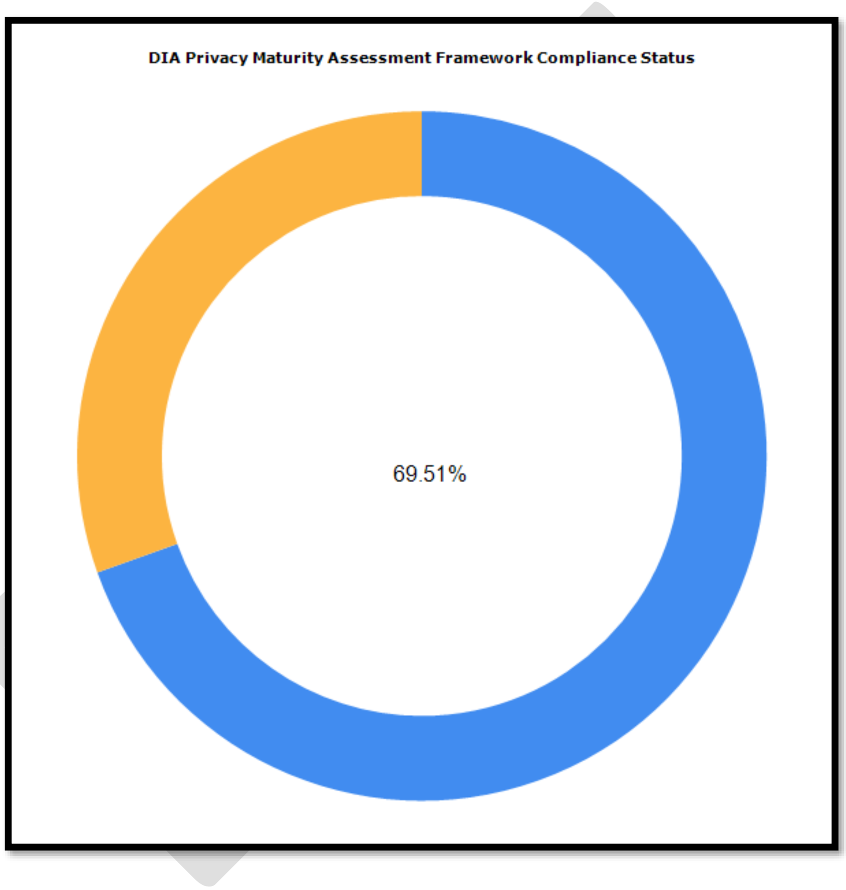
Section	Elements	Scope	Criteria	Informal	Basic	Managed
		legislation have provisions that enable the sharing of personal information to ensure that agencies and people with a legitimate purpose can access information they need.				These policies also refer to relevant external sources (for example, information to support tamariki wellbeing, information sharing under the Family Violence Act 2018).
		When building privacy awareness, culture, capability, and practices, it's important that a range of teams understand those enabling elements and are supported to act on them so that they can deliver services that meet public expectations. Even when it's not practical or possible to share personal information with the group or community from which it came, it remains important to share the value of information and insights that were developed using their personal information in some non-identifiable form. This may include data and	**Criteria 2: Understanding communities' interest**	Sharing of non-personal information is ad-hoc or reactive.	Individual initiatives take steps to share non-personal information that is of interest to communities. Privacy and other relevant policies may contain little or no guidance on this topic.	Privacy and other relevant policies incorporate advice for the appropriate reuse and sharing of non-personal information of interest to communities that does not identify individuals (for example, data and data sets, analysis, qualitative or quantitative information, statistics, research, reports, or studies) from: • Data Protection and Use Policy — Sharing Value • Office of the Privacy Commissioner • data.govt.nz — Manage data

Page **38** of **57**

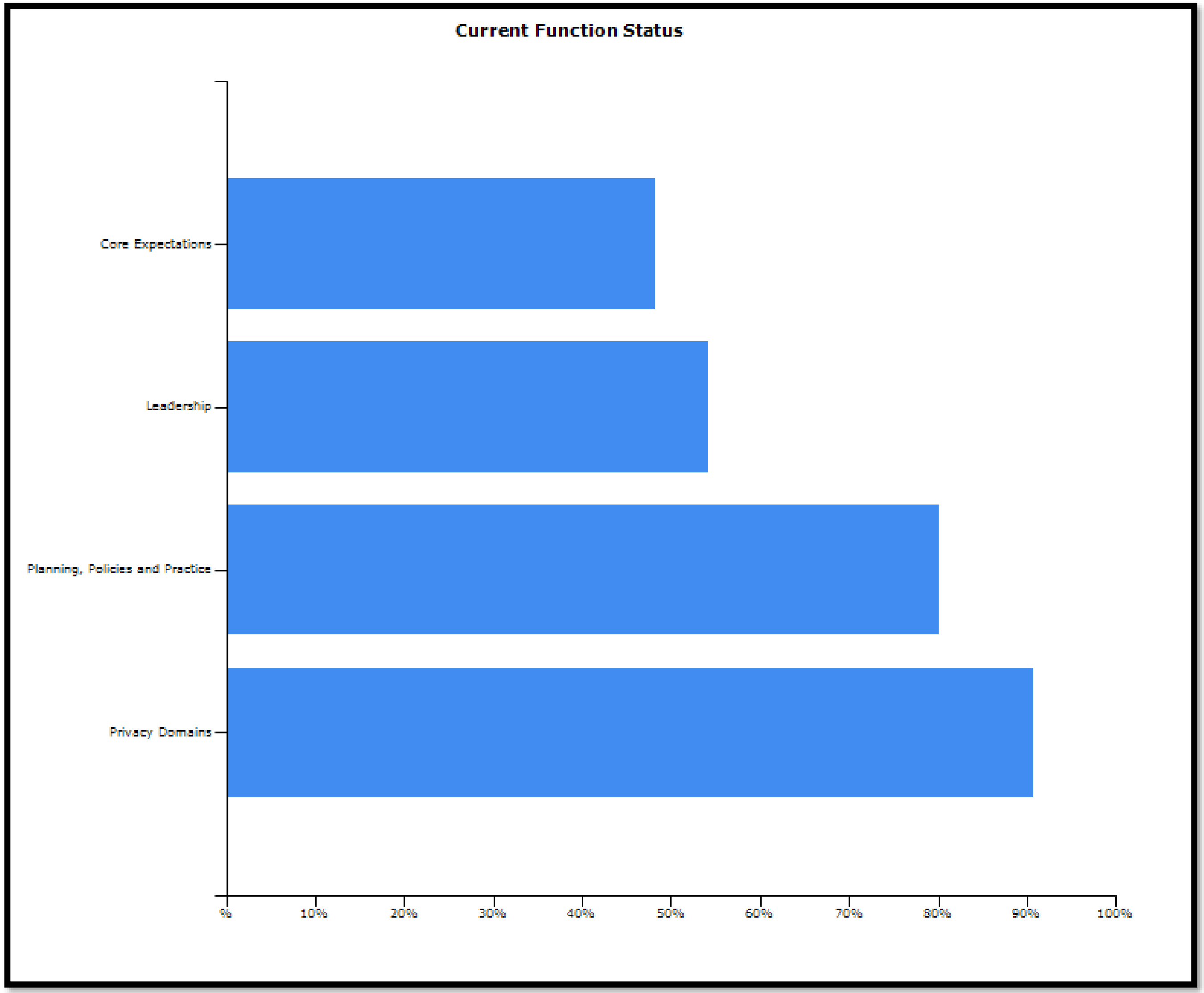
Section	Elements	Scope	Criteria	Informal	Basic	Managed
		data sets, analyses, qualitative or quantitative information, statistics, research, reports, or studies.				

Privacy Self-Assessment Current State

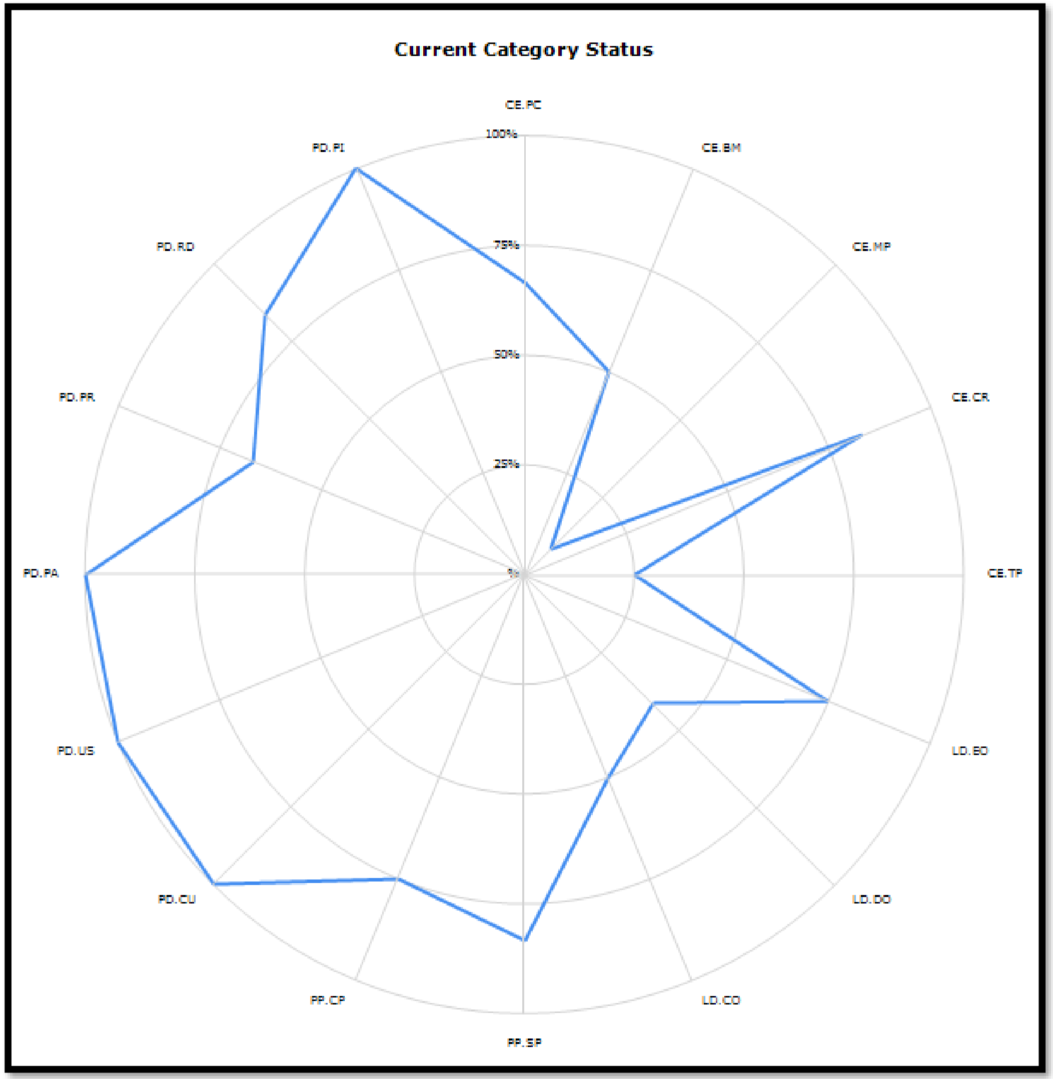
The following is the self-assessment carried out by Council showing the current state privacy at Council.



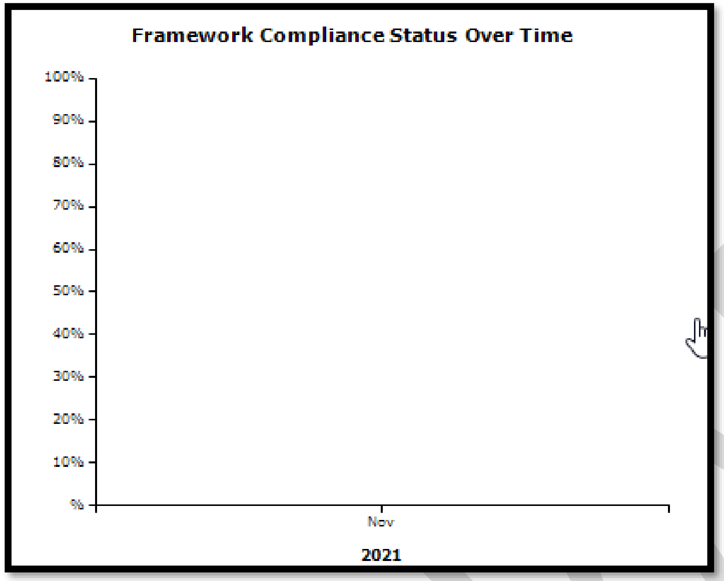
Page **40** of **57**

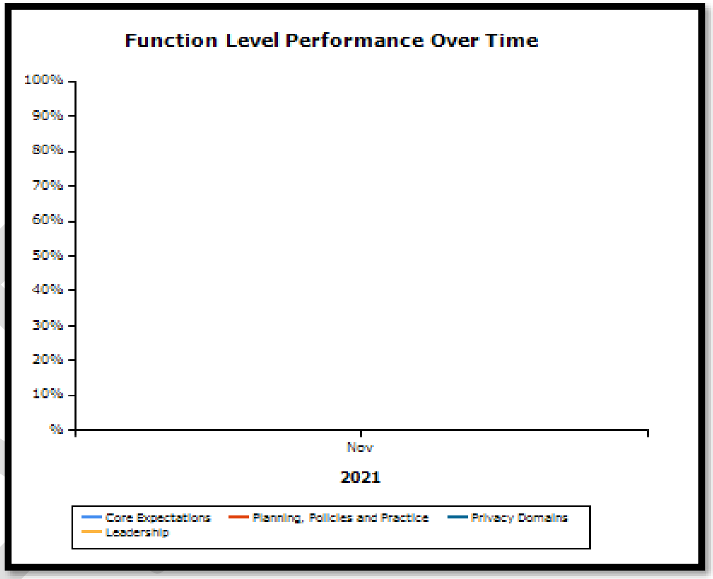

Current Function Status
Core Expectations
Leadership
Planning, Policies and Practice
Privacy Domains
%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

Page **41** of **57**

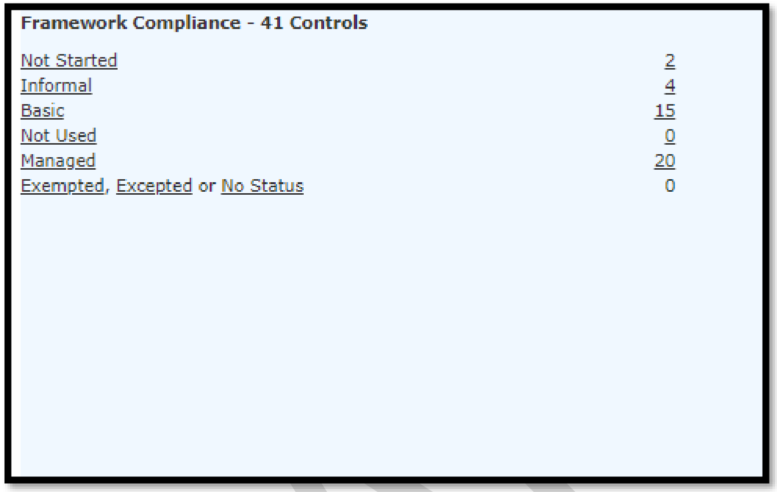


Current Category Status


Framework Compliance Status Over Time
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
%
Nov
2021

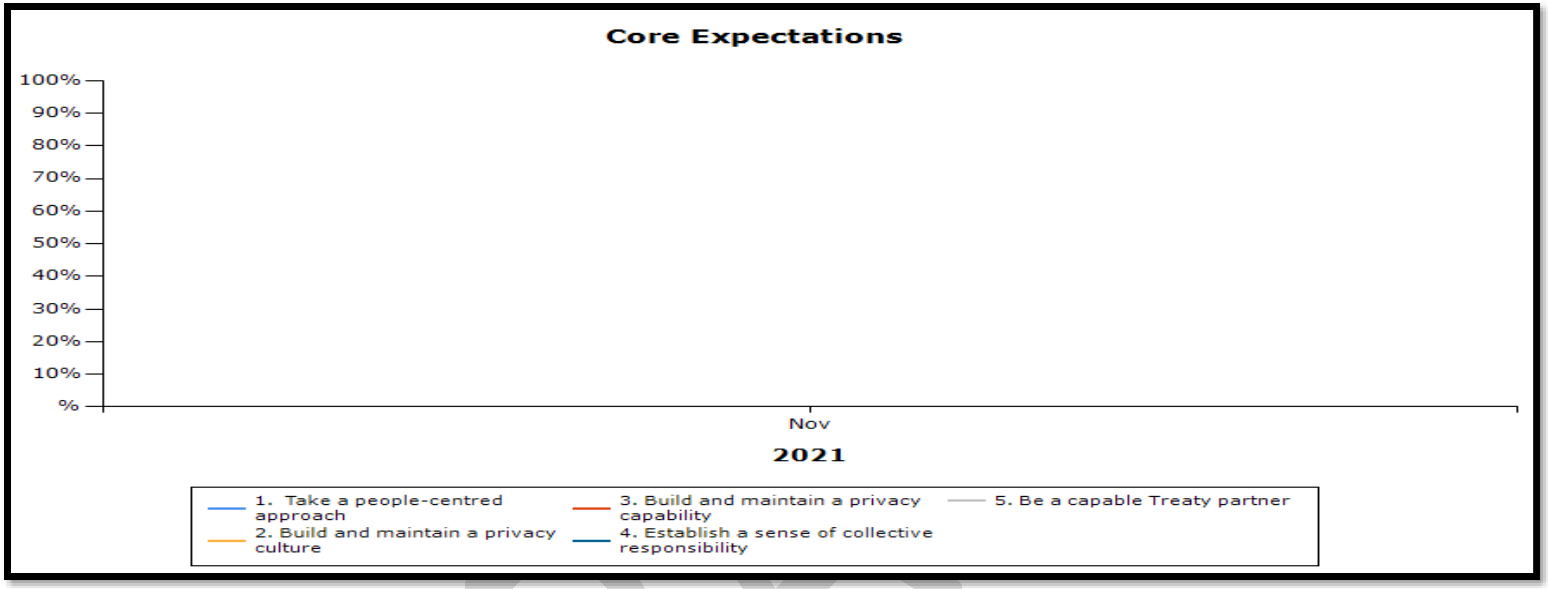

Function Level Performance Over Time
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
%
Nov
2021
Core Expectations
Planning, Policies and Practice
Privacy Domains
Leadership

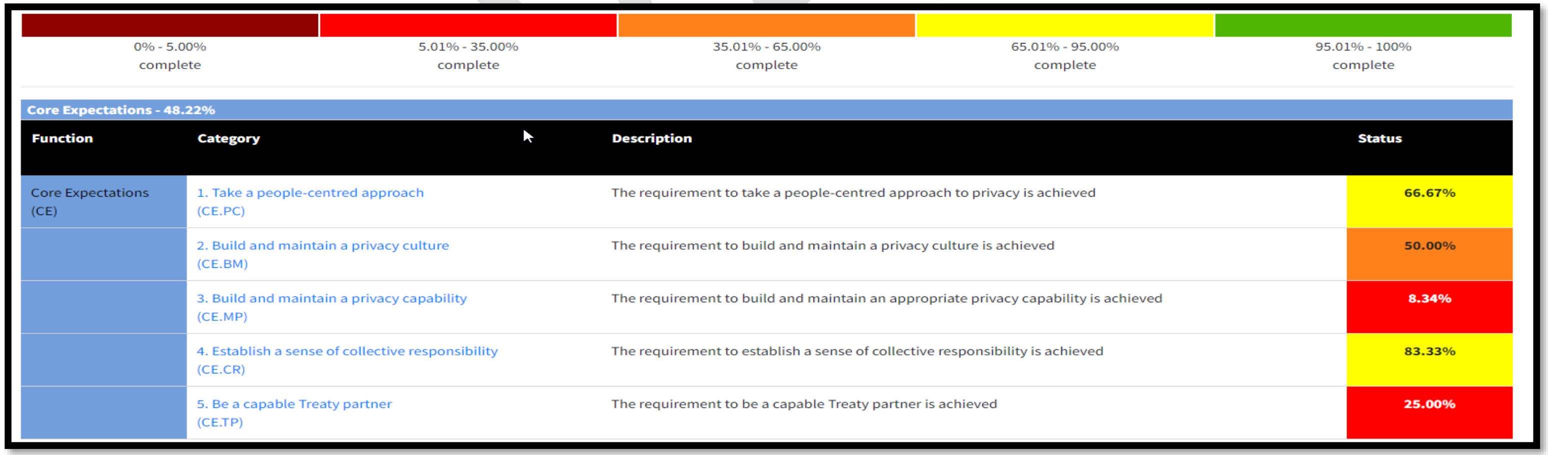
Page **43** of **57**



Framework Compliance - 41 Controls

Not Started	2
Informal	4
Basic	15
Not Used	0
Managed	20
Exempted, Excepted or No Status	0

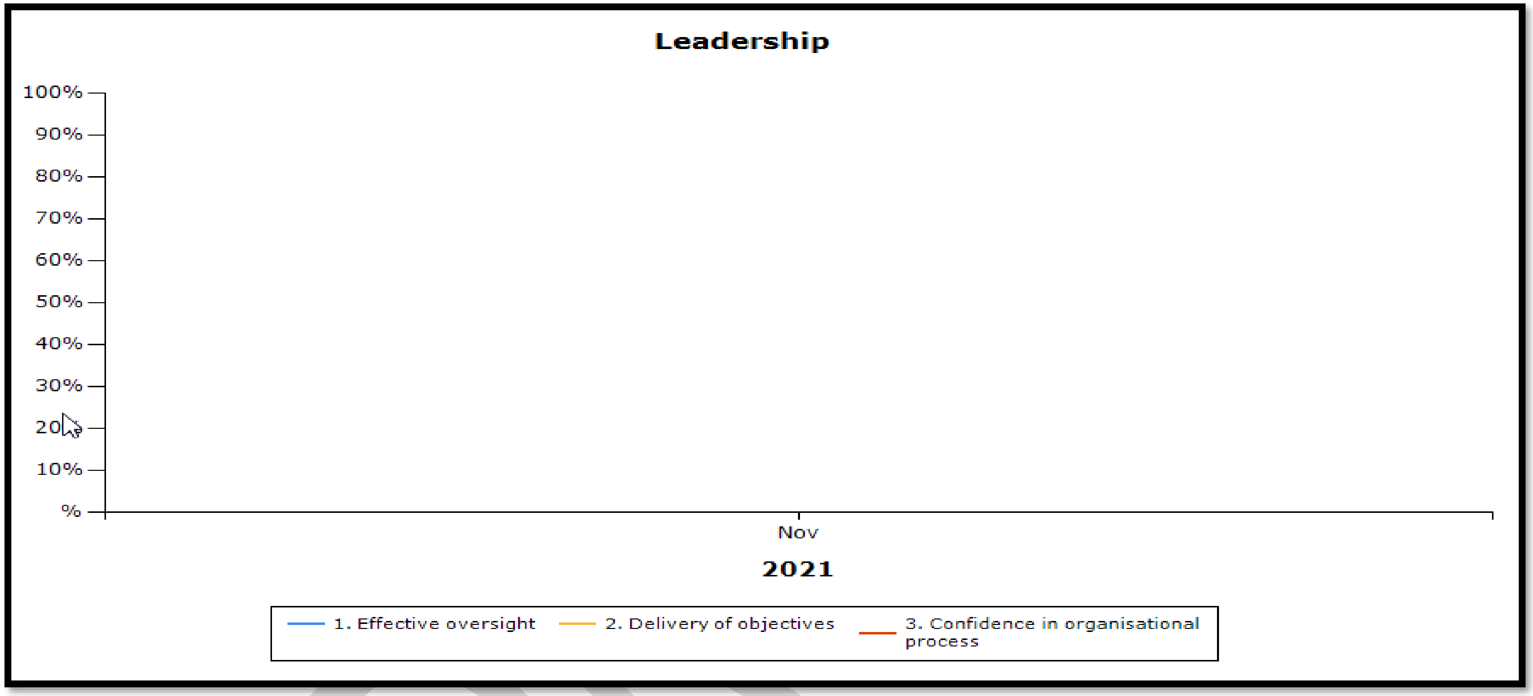


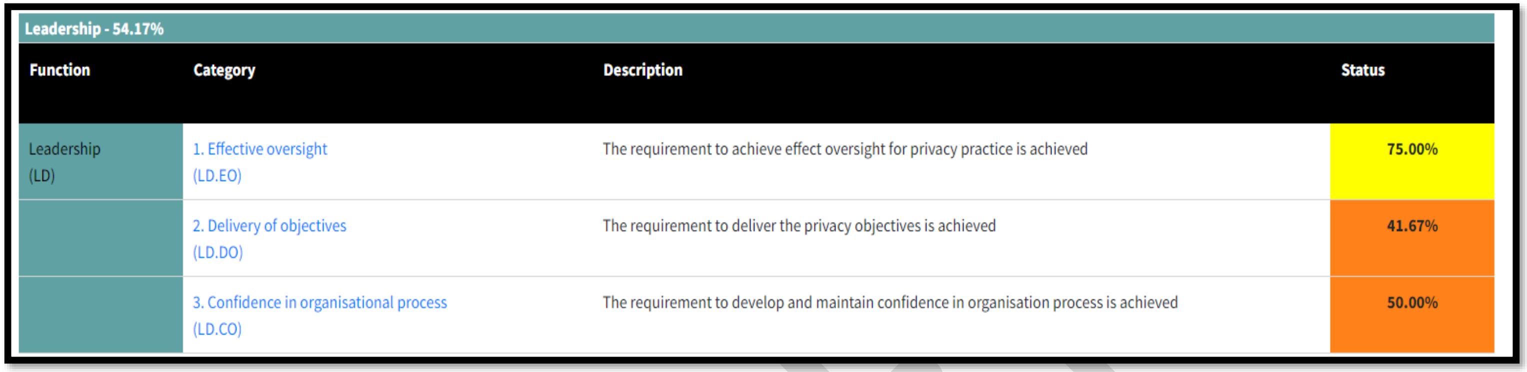


🟥	🟥	🟧	🟨	🟩
0% - 5.00% complete	5.01% - 35.00% complete	35.01% - 65.00% complete	65.01% - 95.00% complete	95.01% - 100% complete

Core Expectations - 48.22%

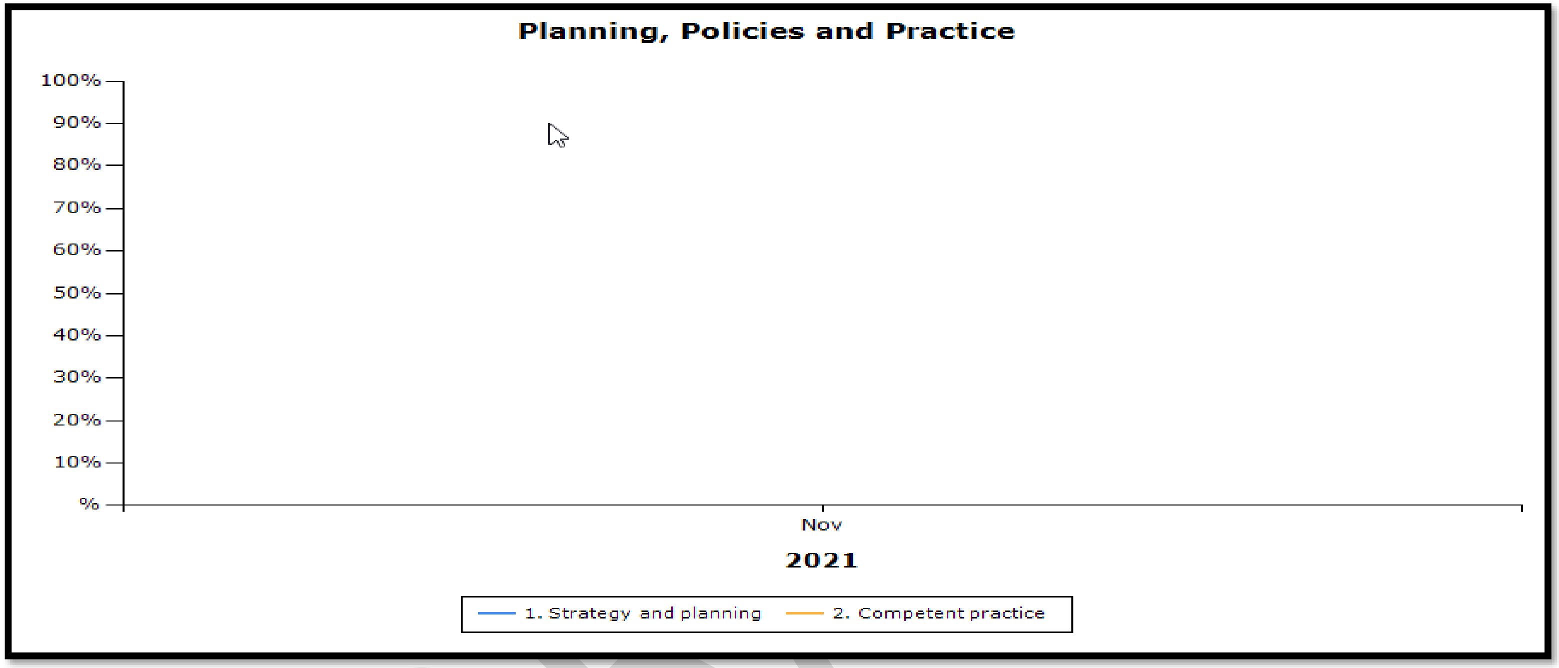
Function	Category	Description	Status
Core Expectations (CE)	1. Take a people-centred approach (CE.PC)	The requirement to take a people-centred approach to privacy is achieved	66.67%
	2. Build and maintain a privacy culture (CE.BM)	The requirement to build and maintain a privacy culture is achieved	50.00%
	3. Build and maintain a privacy capability (CE.MP)	The requirement to build and maintain an appropriate privacy capability is achieved	8.34%
	4. Establish a sense of collective responsibility (CE.CR)	The requirement to establish a sense of collective responsibility is achieved	83.33%
	5. Be a capable Treaty partner (CE.TP)	The requirement to be a capable Treaty partner is achieved	25.00%

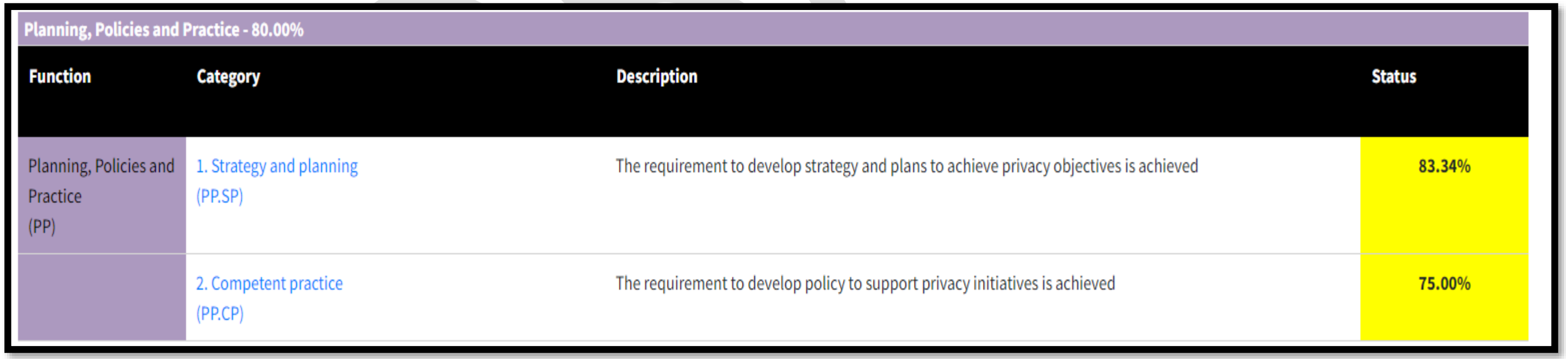

Leadership
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
%
Nov
2021
1. Effective oversight
2. Delivery of objectives
3. Confidence in organisational process



Leadership - 54.17%

Function	Category	Description	Status
Leadership (LD)	1. Effective oversight (LD.EO)	The requirement to achieve effect oversight for privacy practice is achieved	75.00%
	2. Delivery of objectives (LD.DO)	The requirement to deliver the privacy objectives is achieved	41.67%
	3. Confidence in organisational process (LD.CO)	The requirement to develop and maintain confidence in organisation process is achieved	50.00%

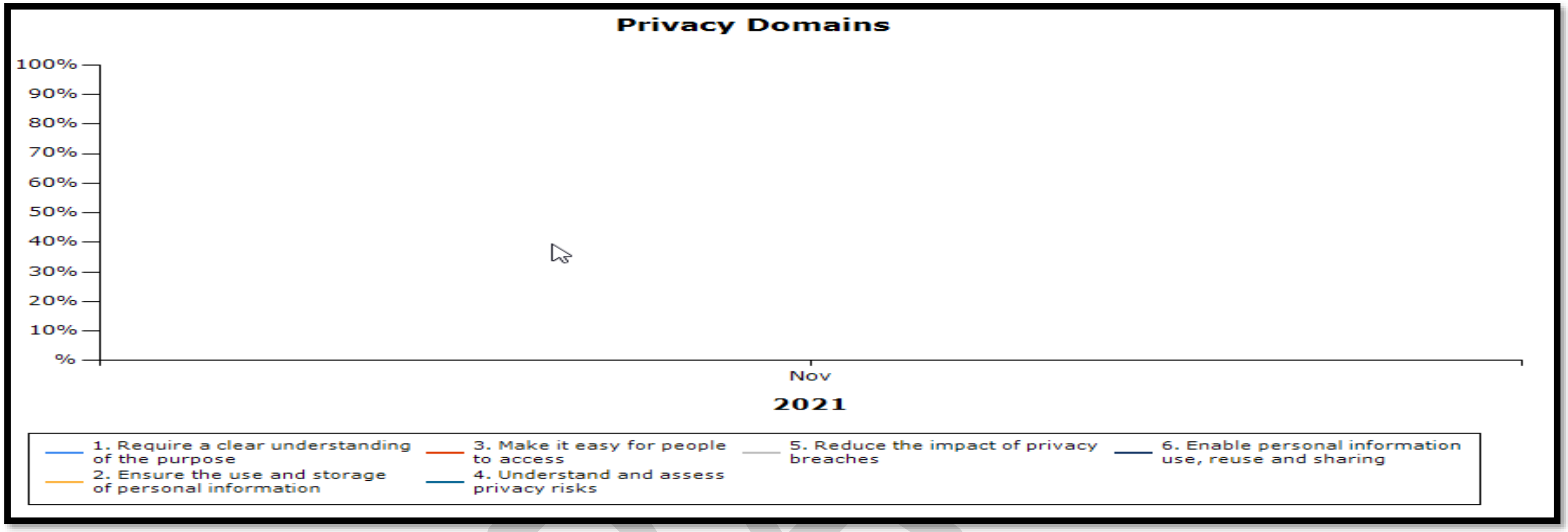


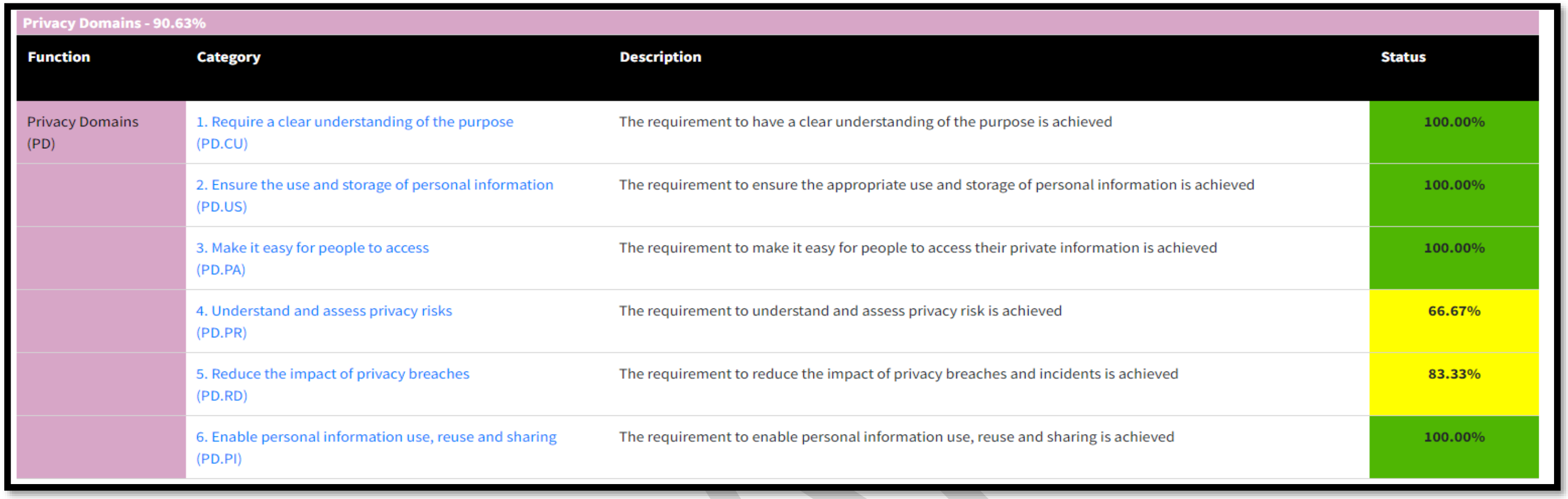


Planning, Policies and Practice - 80.00%

Function	Category	Description	Status
Planning, Policies and Practice (PP)	1. Strategy and planning (PP.SP)	The requirement to develop strategy and plans to achieve privacy objectives is achieved	83.34%
	2. Competent practice (PP.CP)	The requirement to develop policy to support privacy initiatives is achieved	75.00%

Page **48** of **57**


Privacy Domains
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
%
Nov
2021
1. Require a clear understanding of the purpose
2. Ensure the use and storage of personal information
3. Make it easy for people to access
4. Understand and assess privacy risks
5. Reduce the impact of privacy breaches
6. Enable personal information use, reuse and sharing



Privacy Domains - 90.63%

Function	Category	Description	Status
Privacy Domains (PD)	1. Require a clear understanding of the purpose (PD.CU)	The requirement to have a clear understanding of the purpose is achieved	100.00%
	2. Ensure the use and storage of personal information (PD.US)	The requirement to ensure the appropriate use and storage of personal information is achieved	100.00%
	3. Make it easy for people to access (PD.PA)	The requirement to make it easy for people to access their private information is achieved	100.00%
	4. Understand and assess privacy risks (PD.PR)	The requirement to understand and assess privacy risk is achieved	66.67%
	5. Reduce the impact of privacy breaches (PD.RD)	The requirement to reduce the impact of privacy breaches and incidents is achieved	83.33%
	6. Enable personal information use, reuse and sharing (PD.PI)	The requirement to enable personal information use, reuse and sharing is achieved	100.00%

Actions

Action management and reporting on progress will occur within the SAM for Compliance - compliance management tool. Tasking of these actions will occur within the IS Portal.

The following is a summary of the actions at the time of preparing this plan, including recommendations from the information security risk review. The actions will be grouped by the functions and categories of the Privacy Maturity Assessment Framework.

Status key: Not Started, Started, Partially Completed, Mostly Completed, Fully Completed

The following table has been populated from: Complete a self-assessment | NZ Digital government

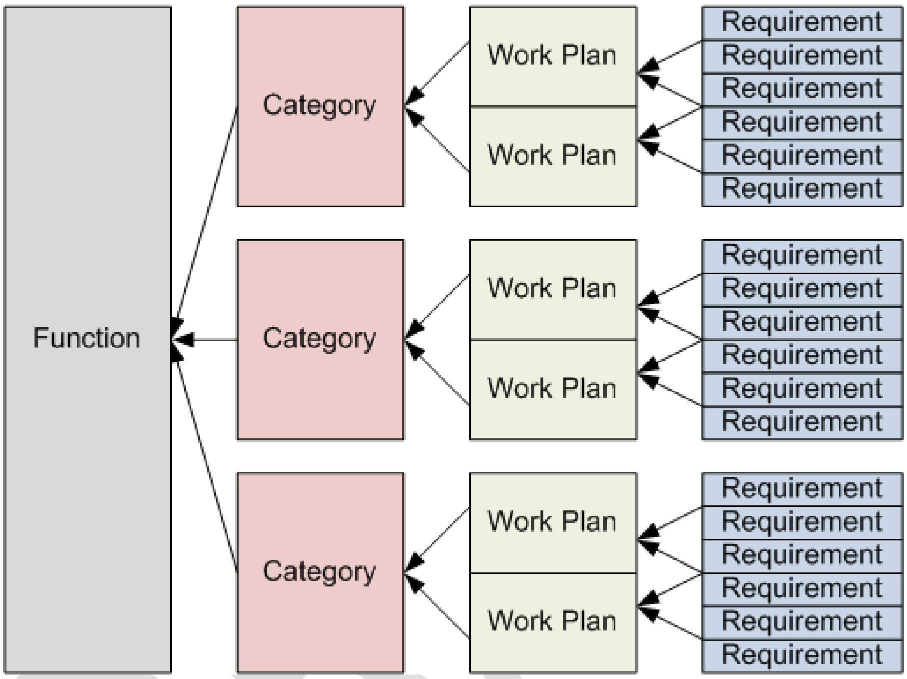
Section	Elements	Criteria	Actions	Responsibility	Due Month/Year	Status	Notes
Core Expectations	1. Take a people-centred approach	Criteria 1: Having a people-centred privacy programme	Actions will be populated following the review by the Executive Team.				
		Criteria 2: Connecting with service users					
		Criteria 3: Being transparent					
	2. Build and maintain a privacy culture	Criteria 1: Creating a privacy culture					
		Criteria 2: Communicating privacy values and aspirations					
		Criteria 3: Developing privacy awareness					
	3. Build and maintain privacy capability	Criteria 1: Conducting privacy training					

Section	Elements	Criteria	Actions	Responsibility	Due Month/Year	Status	Notes
		Criteria 2: Monitoring and updating privacy training					
		Criteria 3: Providing additional privacy training					
	4. Establish a sense of collective responsibility	Criteria 1: Implementing privacy practices					
		Criteria 2: Linking privacy to organisational values					
		Criteria 3: Including privacy in employment					
	5. Be a capable Treaty partner	Criteria 1: Identifying Māori privacy interests					
		Criteria 2: Partnering with Māori					
Leadership	1. Effective oversight	Criteria 1: Privacy reporting					
		Criteria 2: Privacy and risk management					
	2. Delivery of objectives	Criteria 1: Responsibility and accountability					
		Criteria 2: Resourcing					
		Criteria 3: Oversight and visibility					
	3. Confidence in organisational progress	Criteria 1: Privacy and assurance					
Planning, policies, and practice	1. Strategy and planning	Criteria 1: Planning					

Section	Elements	Criteria	Actions	Responsibility	Due Month/Year	Status	Notes
		Criteria 2: Planning documents					
		Criteria 3: Reporting					
	2. Competent practice	Criteria 1: Policies					
		Criteria 2: Contracts					
Privacy domains	1. Require a clear understanding of the purpose	Criteria 1: Defining the purpose Criteria					
		Criteria 2: Identifying choices					
		Criteria 3: Reducing personal information					
	2. Ensure the use and storage of personal information	Criteria 1: Implementing Privacy by Design					
		Criteria 2: Implementing privacy engineering					
	3. Make it easy for people to access	Criteria 1: Having a process					
		Criteria 2: Monitoring the process					
		Criteria 3: Reviewing the process					
	4. Understand and assess privacy risks	Criteria 1: Knowing the agency's risks					
		Criteria 2: Managing agency's risks					
		Criteria 3: Managing project risks					
	5. Reduce the impact of privacy breaches	Criteria 1: Having a privacy incident register					
		Criteria 2: Minimising collection of personal information					
		Criteria 3: Retaining personal information					
	6. Enable personal information use, reuse and sharing	Criteria 1: Having policies					
		Criteria 2: Understanding communities' interest					

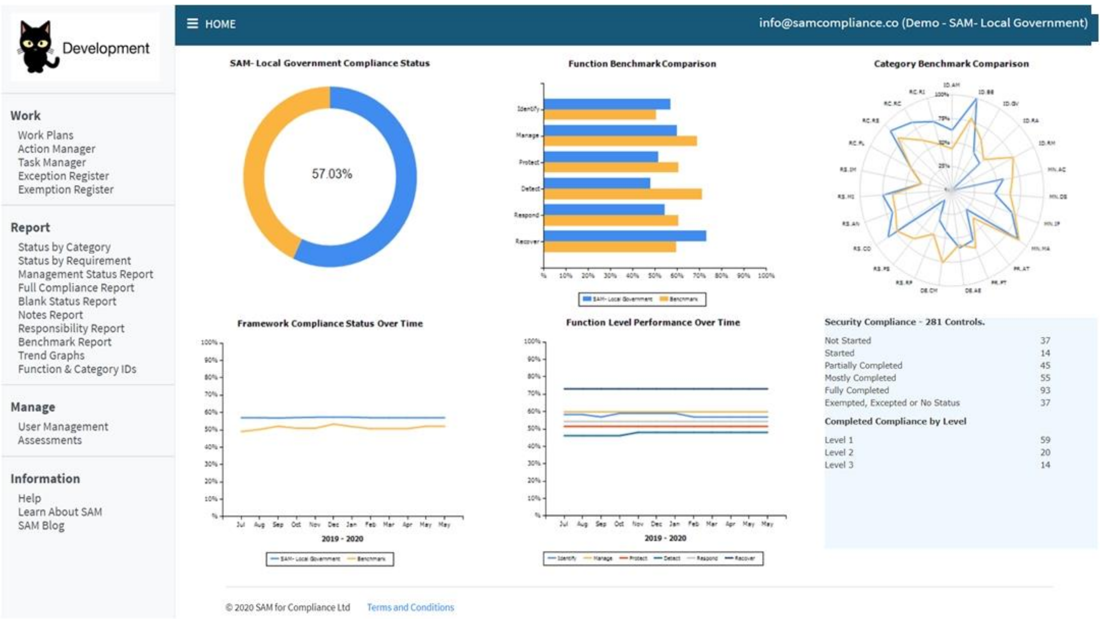
Compliance Management

Council has chosen to utilise SAM for Compliance. SAM for Compliance is a compliance management tool which can be applied to any standard or framework that is comprised of specific requirements or controls. SAM for Compliance contains frameworks which are broken down into key performance areas based on the NIST CSF model of Framework, Function, Category, Sub-Category and Controls.



SAM for Compliance relies on self-assessment to ascertain the current compliance status. The system simply calculates totals based on Council input.

The controls are assessed based on a pre-defined maturity model individual to each framework instance and dynamically update the dashboard view and all system reports.



Work
- Work Plans
- Action Manager
- Task Manager
- Exception Register
- Exemption Register

Report
- Status by Category
- Status by Requirement
- Management Status Report
- Full Compliance Report
- Blank Status Report
- Notes Report
- Responsibility Report
- Benchmark Report
- Trend Graphs
- Function & Category IDs

Manage
- User Management
- Assessments

Information
- Help
- Learn About SAM
- SAM Blog

SAM- Local Government Compliance Status

Function Benchmark Comparison

Category Benchmark Comparison

Framework Compliance Status Over Time

Function Level Performance Over Time

Security Compliance - 281 Controls.

Not Started	37
Started	14
Partially Completed	45
Mostly Completed	55
Fully Completed	93
Exempted, Excepted or No Status	37

Completed Compliance by Level

Level 1	59
Level 2	20
Level 3	14

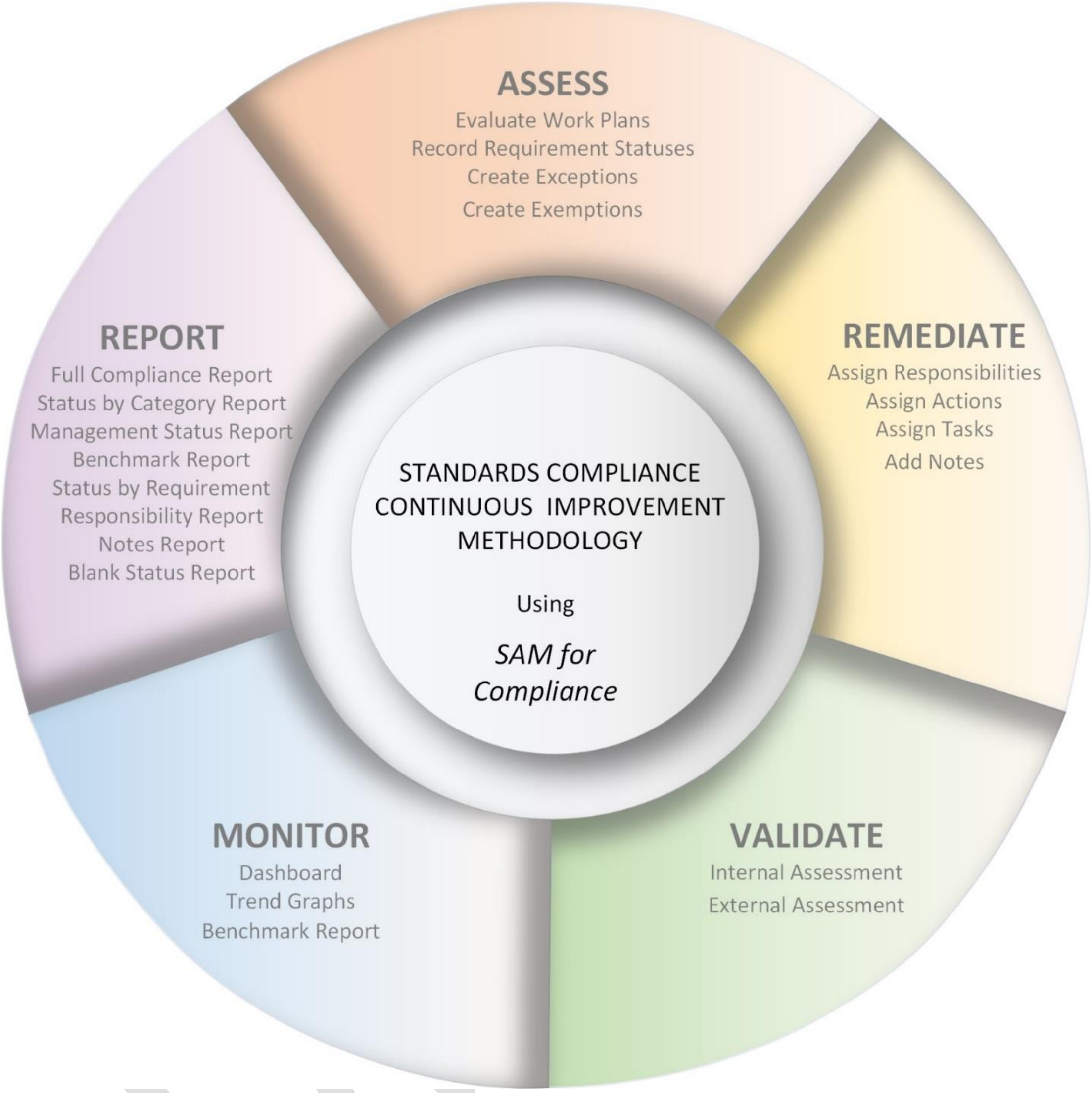
© 2020 SAM for Compliance Ltd   Terms and Conditions

SAM Management Methodology

The SAM for Compliance tool consists of functions that assist you to manage compliance to your chosen framework as demonstrated by the features on the colour wheel below:

- **ASSESS -** Evaluate and record your status against your chosen maturity model, including Exceptions and Exemptions
- **REMEDIATE -** Assign responsibilities for achieving compliance with controls, assign Actions and Tasks and add Notes to record specific details or links to other documents
- **VALIDATE** - Assessment function
- **MONITOR -** View your current Status from our dynamic, multi-chart Dashboard and Trend graphs. View benchmark comparisons against your Peer Group (where applicable)
- **REPORT -** Report your current Status

Page **55** of **57**



STANDARDS COMPLIANCE
CONTINUOUS IMPROVEMENT
METHODOLOGY

Using

SAM for Compliance

ASSESS
Evaluate Work Plans
Record Requirement Statuses
Create Exceptions
Create Exemptions

REMEDIATE
Assign Responsibilities
Assign Actions
Assign Tasks
Add Notes

VALIDATE
Internal Assessment
External Assessment

MONITOR
Dashboard
Trend Graphs
Benchmark Report

REPORT
Full Compliance Report
Status by Category Report
Management Status Report
Benchmark Report
Status by Requirement
Responsibility Report
Notes Report
Blank Status Report

Reporting

Reporting on the progress of this plan will occur as follows:

Who	What	When
Audit and Risk Committee	An information report will be prepared, including the following topics: • Department of Internal Affairs Privacy Maturity Assessment Framework update • Privacy programme of work by actions	Quarterly
Executive Team		Quarterly

22.2.6 PRIVACY AND LGOIMA REQUESTS POLICIES

Doc ID: 581151

1. Purpose

To note the Privacy Policy and Local Government Official Information and Meetings Act Request Policy are now finalised following incorporation of the recommended changes.

Recommendations

That the report be received.

2. Discussion

On 25 February 2022, the Audit and Risk Committee supported the Chief Executive approval of the Privacy Policy and Local Government Official Information and Meetings Act (LGOIMA) Request Policy, upon the following changes to be made:

- LGOIMA Request Policy changes included simplification of the charges tables and subject to Staff Delegation Manual in relation to release of information.
- Privacy Policy changes included: expanding the scope to include elected members, Council's obligations as an employer and staff consideration for personal information.

These changes have been made as per Appendix 1 and 2. Both policies have been approved by the Chief Executive and implemented, including being released on Council's website and staff intranet.

Further implementation tasks are ongoing for the Privacy Policy, including updating and standardising terms and conditions across all seven Council owned and managed websites.

3. Attachments

Appendix 1 - Privacy Policy ⇩
Appendix 2 - LGOIMA Request Policy ⇩

Report author:

Nathan McLeod
IS Manager
16/05/2022

Reviewed and authorised by:

Leanne Macdonald
Executive Manager - Corporate Services
17/05/2022

Privacy Policy

Department:	Information Services
Document ID:	574137
Approved by:	Chief Executive
Effective date:	March 2022
Next review:	March 2023

Purpose:

To outline the Central Otago District Council's ("Council") code of practice and legal obligations in accordance with the Privacy Act 2020.

Objectives:

The objectives of this policy are to:

- Create a framework to manage Council's legal obligations under the Privacy Act 2020 to achieve compliance.
- Provide external communication to the public via the Council website regarding the personal information Council collects, the purpose of the collection and how Council manages, protects, and respects that information including requests under the Privacy Act 2020.
- Provide clear guidance to staff regarding the management and release of personal information including requests under the Privacy Act 2020.
- Establish privacy breach prevention mechanisms and establish responsibilities for privacy breach detection.
- Maintain a positive "privacy culture" in which staff, contractors and appointees are supported and encouraged to adopt good privacy practices and adherence to the Information Privacy Principles (IPPs).

Scope:

Applies to all Elected Members, Council staff, including temporary employees, and contractors. It also applies to anyone who is involved in Council operations, including volunteers and those people with honorary status or unpaid staff status.

Staff may only access, use, or share information that Council holds for the express purposes of conducting the role for which they are employed by Council, or with the authorisation of the person which the information relates to, and in keeping with the conditions of the Code of Ethics.

Definitions:

Consent - Refers to authorisation from the individual concerned.
Personal Information - Any information about a specific individual. The information does not need to name the individual, as long as they are identifiable in other ways, like through their home address.
Privacy breach - Unauthorised access to or collection, use or disclosure of personal information.
Serious harm – Unwanted sharing, exposure or loss, damage, or disadvantage of access to people's personal information. Loss of a benefit or a right. May include physical harm or intimidation, financial fraud including unauthorised credit card transactions or credit fraud, family violence, psychological, or emotional harm, such as significant humiliation or loss of dignity.

Policy:

Information Privacy Principles

The Council is committed to the 13 Information Privacy Principles (IPPs) of the Privacy Act 2020 which govern the collection, holding, use and disclosure of individuals' personal information. The types of information collected for these purposes include:

- General contact details – address, telephone, email
- Identification details – name, address, date of birth
- Images from CCTV cameras and wearable cameras
- License plate numbers for parking matters
- Financial details for payments
- Medical information for recreation programmes or events.

Sharing personal information

Personal information will only be shared outside Council when:

- The reason for sharing matches the reason the information was collected; or
- A specific legal reason or obligation to share the information exists; or
- The persons concerned give permission for it to be shared; or
- When the persons concerned sign a consent form or voluntarily provide information to Council.

Other applicable legislation includes the Local Government (Rating) Act 2002, Resource Management Act 1991, Building Act 2004, Health and Safety at Work Act 2015

Building and resource consents

Documentation associated with consents such as resource and building consents are public record and will be available online for public access. This will include personal information on consenting documents and submissions.

Rating information

Section 28A of Local Government (Rating) Act 2002 requires the Council to maintain a rating information database and to make this available to the public. You have a right to request, in writing, that your name and/or postal address be withheld from this database. You do not need to provide reasons for this request, and you can revoke this request at any time.

Privacy Officer

Council has a designated Privacy Officer who is responsible for:

- Assisting elected members and staff in managing personal information requests
- Requests for information received
- Complaints made about Council's actions or procedures
- Privacy induction for new employees.

Procedures

Council staff will contain, assess, and notify all privacy breaches, near misses, trends, risks, and other relevant information to the appropriate levels of management in accordance with the Privacy Act 2020. Serious harm breaches that have caused "serious harm" to someone (or is likely to do so) must be reported to the Office of the Privacy Commissioner using the OPC online reporting tool - NotifyUs.

A series of procedures to support this policy will be maintained by Council staff.

Council staff will maintain up-to-date Privacy Information on its website.

Relevant legislation:

Privacy Act 2020
Public Service Act 2020
Human Rights Act 1993
Local Government Official Information and Meetings Act (LGOIMA) 1987
Official Information Act (OIA) 1982
Local Government Act (LGA) 2002
Local Government (Rating) Act 2002

Related documents:

Staff Delegations Manual (Internal use)
Privacy Breach Notification Procedure (Internal use)
Request for Personal Information Procedure (Internal use)
Office of the Privacy Commissioner Enquiry Form
Office of the Privacy Commissioner - AskUs
Office of the Privacy Commissioner AboutMe (Request my Info Tool)
Office of the Privacy Commissioner Privacy Statement Generator
LGOIMA Request Policy
LGOIMA Request Procedure (Internal use)
Redaction Guidelines (Internal use)

LGOIMA Request Policy

Department:	Information Services
Document ID:	576702
Approved by:	Chief Executive
Effective date:	March 2022
Next review:	March 2023

Purpose:

To provide the framework and formalise the Central Otago District Council's ("Council") legal obligation on granting requests for official information under the Local Government Official Information and Meetings Act (LGOIMA) 1987.

Principles and objectives:

The guiding principle under the legislation is that if the information is held by the Council, it must be available to the public unless good reason exists under the Act for withholding it.

The objectives of this policy are:

- To ensure all council staff are aware of their responsibilities under the LGOIMA Act 1987.
- To provide clear guidance to requesters of information on the Council approach to LGOIMA Requests
- To provide clear guidance on what information may be charged for.

Scope:

This policy applies to the decision-making process for requests for official information held by the Council and its contractors. Requests for official information may be made by any person.

Any LGOIMA Request received by Council is subject to the Privacy Act 2020. Requesting personal information about other people from the Council is prohibited.

Out of Scope:

If the request is for personal information about the requester, the Privacy Act 2020 will apply, and the request will be managed under the provisions of the Privacy Act 2020.

Definitions:

The Act: The Local Government Official Information and Meetings Act (LGOIMA) 1987
LGOIMA Requests: Requests for any official information held by Council as defined in the Act
Official Information: Any information held by the Council as defined by of the section 2 of the LGOIMA.
Personal information requests: Requests managed under the Privacy Act 2020.

Policy:

Request:

A request can be made in various forms including:

- Verbal or written directly from individuals
- Verbal or written directly from groups
- From other public bodies
- From individuals or groups referred by other public bodies
- From an individual's agent (e.g., a lawyer acting on behalf of a client).

Even when a request is not specified as a LGOIMA Request, it may be processed under this policy.

Decision to release and charges (if any):

Council must decide as soon as reasonably practicable after receiving the request:

- Whether a request for official information will be granted
- In what manner
- If any charges will apply.

In making this decision, Council officers as per the Staff Delegation Manual will consider all aspects of the LGOIMA Act 1987. Council shall adopt the principle that the material is available it shall be released, unless there are grounds to withhold it under the Act.

If a request is estimated to take over one hour of staff time, Council may charge for searching for relevant material, abstracting, collating, copying, and transcribing to fulfil the request, consistent with the Ombudsman Charging Guidelines.

First hour	No Charge
Initial charge for the first chargeable half hour, additional half hour or part thereof	$38.00

Charges related to photocopying and printing can be found in Councils fees and charges.
If the request is likely to incur a charge, the Council will discuss this with the requester to refine the request and accordingly reduce or remove costs. Work will not commence until an estimate of charges has been provided to the requester, and the requester has accepted and paid these charges.

Timeframes:

Council will ensure that requests are responded to within 20 working days unless the requester is notified within 5 working days of the request that the Council requires the period to be extended.

Council will make any official information available it has decided to release without undue delay.

Release of the information:

Information may be made available by the Council in several different ways and every effort will be made to make it available in accordance with the requester's preferred format. If the requester's preference is not possible, Council will provide the requester with reasons for this.

Council may decide to release information under certain conditions, with additional context, or with appropriate redactions as detailed in the Act.

Relevant legislation:

Local Government Official Information and Meetings Act (LGOIMA) 1987
Official Information Act 1982
Privacy Act 2020
Local Government Act 2002

Related documents:

LGOIMA Request Procedure (Internal use)
Staff Delegations Manual (Internal use)
LGOIMA Request Training and Induction Guidelines
Privacy Policy
Privacy Breach Notification Procedure (Internal use)
Request for Personal Information Procedure (Internal use)
Redaction Guidelines (Internal use)

22.2.7 HEALTH, SAFETY AND WELLBEING REPORT

Doc ID: 580825

1. Purpose

To provide an update on the health, safety and wellbeing performance at Central Otago District Council.

Recommendations

That the report be received.

2. Discussion

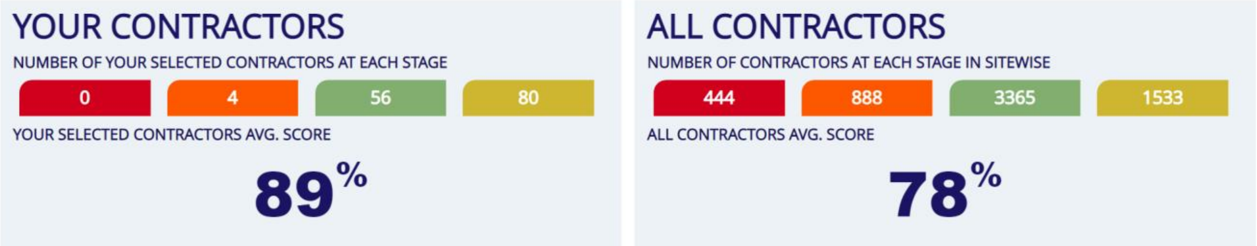
2.1 COVID-19 Management update
Council continues to review its COVID-19 management risk assessments and make any required operational changes.

On April 5, 2022, council lifted the My Vaccine Pass requirement from pools, libraries and i-Sites.

Following the national move to the orange traffic light setting, Council offices returned to operating 50% staff capacity.

2.2 Contractor management

Council has 140 contractors on its Sitewise pre-qualification list. The average score of 89% is consistent with last quarter.



YOUR CONTRACTORS

NUMBER OF YOUR SELECTED CONTRACTORS AT EACH STAGE

🟥	🟧	🟩	🟨
0	4	56	80

YOUR SELECTED CONTRACTORS AVG. SCORE

89%

ALL CONTRACTORS

NUMBER OF CONTRACTORS AT EACH STAGE IN SITEWISE

🟥	🟧	🟩	🟨
444	888	3365	1533

ALL CONTRACTORS AVG. SCORE

78%

Figure 1. Sitewise contractor scores (retrieved May 10, 2022)

Council continues to improve its contractor monitoring processes. In March 2022, the Capital Projects team trialled a new site observation reporting process. This process will build a record of contractor health and safety performance on Council projects. 12 reports have been submitted through this process to date. The process will be introduced to other areas of the business in June 2022.

Contractors raised seven incidents to Council during the reporting period.

2.3 Incident and injury reports

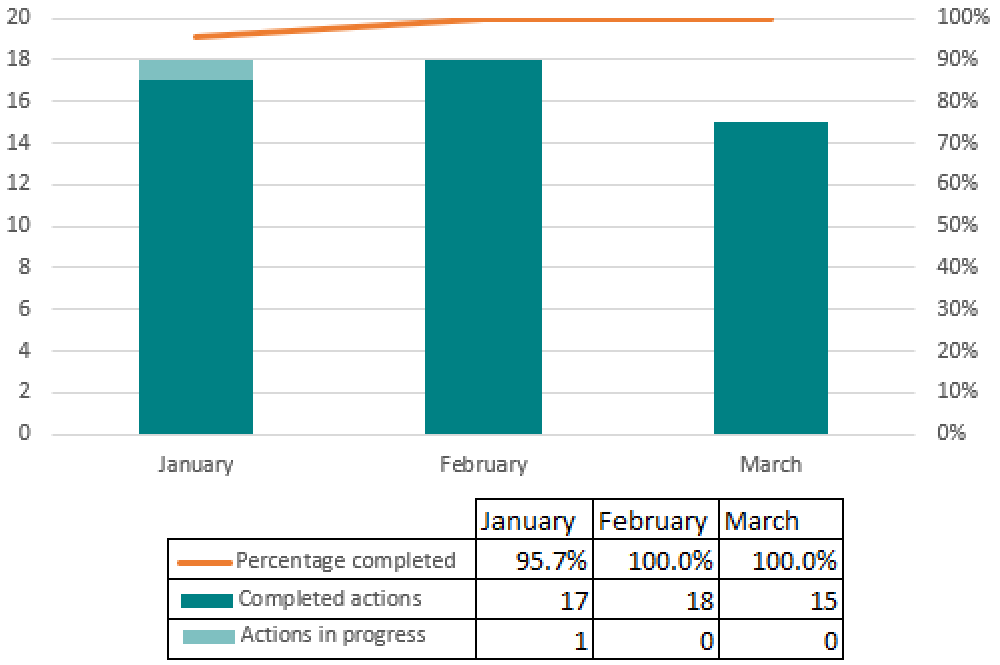
There were 51 reports made between January-March 2022. These reports include safety observations, near misses, and incidents.

Council’s Risk Management Policy has a five-level risk consequence rating system. This system is used to determine incident severity. A rating of 1 or 2 is considered business as usual. All reports submitted this period were within business as usual.

Risk consequence category	Negligible	Minor	Moderate	Major	Extreme
	1	2	3	4	5

Figure 2. Council risk consequence ratings (Source: Risk Management Policy)

Graph 1 shows the percentage of completed corrective actions. One action remains in progress this quarter.



	January	February	March
Percentage completed	95.7%	100.0%	100.0%
Completed actions	17	18	15
Actions in progress	1	0	0

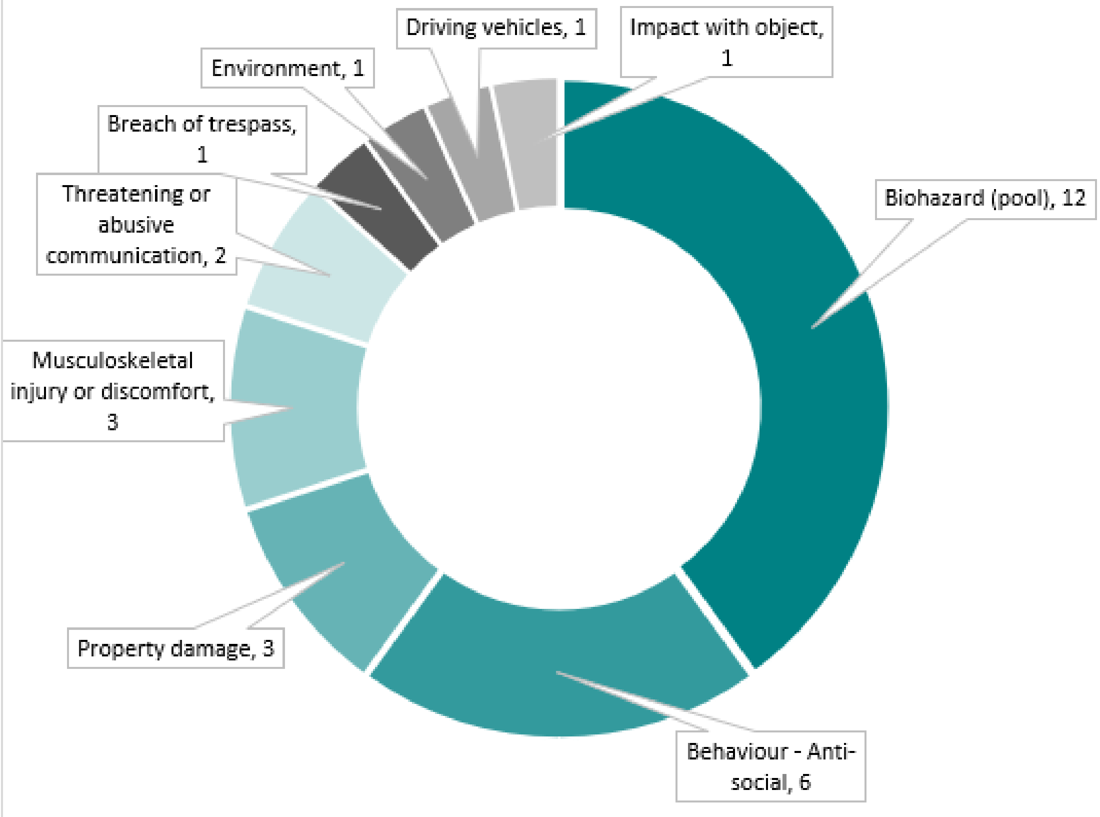
Graph 1: Status of corrective actions

2.3.1 Employee incidents

Of the 52 reports submitted, 30 incidents affected employees.

Employees continue to raise health and safety concerns proactively. 70% of employee reports submitted this quarter were proactive.

Graph 2 shows the areas of concern employees are reporting in.



Graph 2: Employee reports by area of concern

2.3.1a Recordable injuries

Recordable injuries include fatalities, lost time injuries (LTI), medical treatment injuries (MTI), first aid injuries (FAI) and non-treatment injuries.

There was one recordable injury during the reporting period January-March 2022.

Reporting period	Non-treatment injury	FAI	LTI	MTI	Fatality	Total recordable injuries
July-Sept 21	2	1	0	0	0	**3**
Oct-Dec 21	5	1	2	0	0	**8**
Jan-Mar 22	1	0	0	0	0	**1**

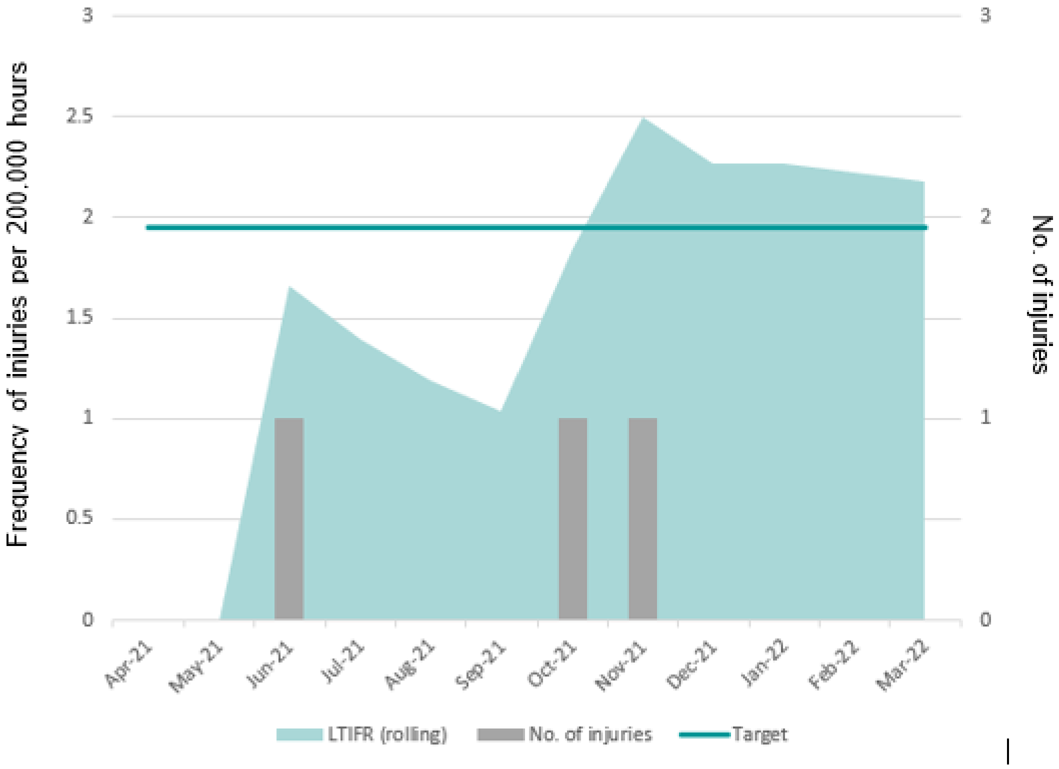
Table 2: Recordable injuries (employees)

2.3.1b Lost time injury frequency rate

Council has set the national benchmark for Lost time injury frequency rate (LTIFR) (1.99) as its target. LTIFR measures the number of lost time injuries per 200,000 hours worked.

During the reporting period, Council’s LTIFR has decreased from 2.27 to 2.18.

There were no lost time injuries during the reporting period.



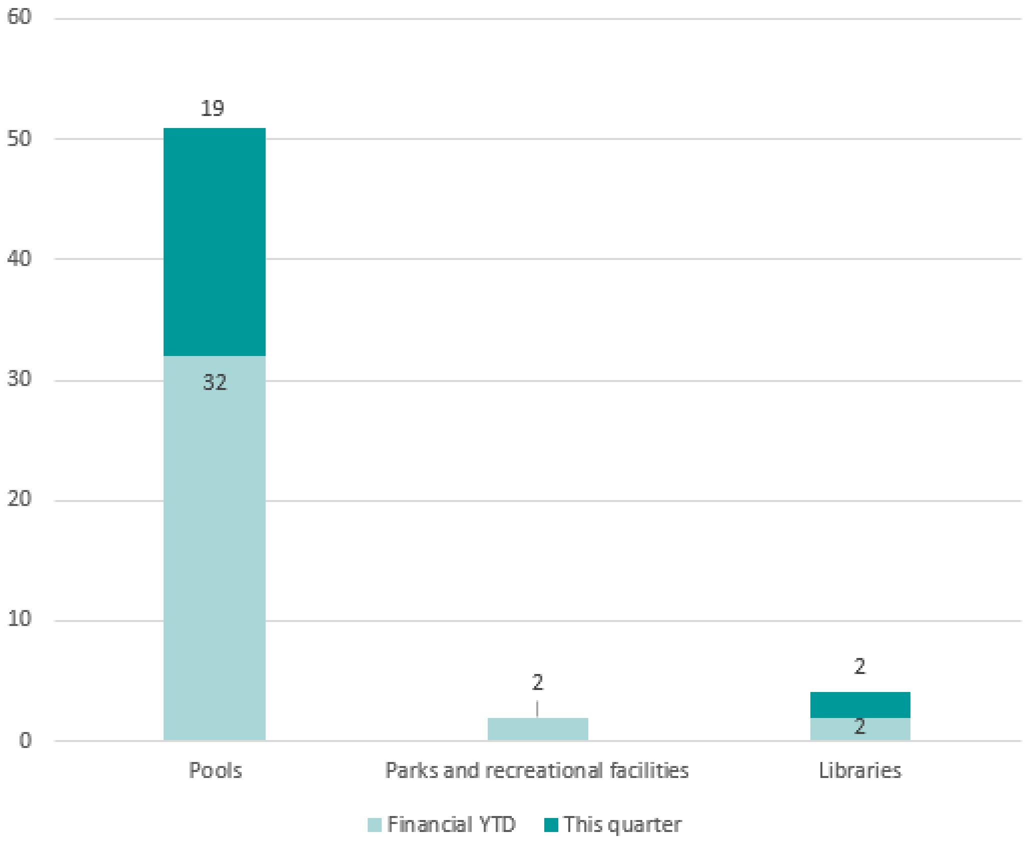
Graph 3: Trend information for LTIFR (lost time injury frequency rate)

Month	Average LTIFR (YTD)	No. of injuries
April 2021	0	0
May 2021	0	0
June 2021	1.66	1
July 2021	1.39	0
August 2021	1.19	0
September 2021	1.04	0
October 2021	1.85	1
November 2021	2.50	1
December 2021	2.27	0
January 2022	2.26	0
February 2022	2.22	0
March 2022	2.18	0

Table 3: Lost time injury frequency rate data

2.3.2 Public incidents

There were 21 incidents involving members of the public during the period January-March 2022. Most incidents occurred at council pools. 19 of those incidents involved injury and are further explained in the public injuries section (2.3.2a) below.



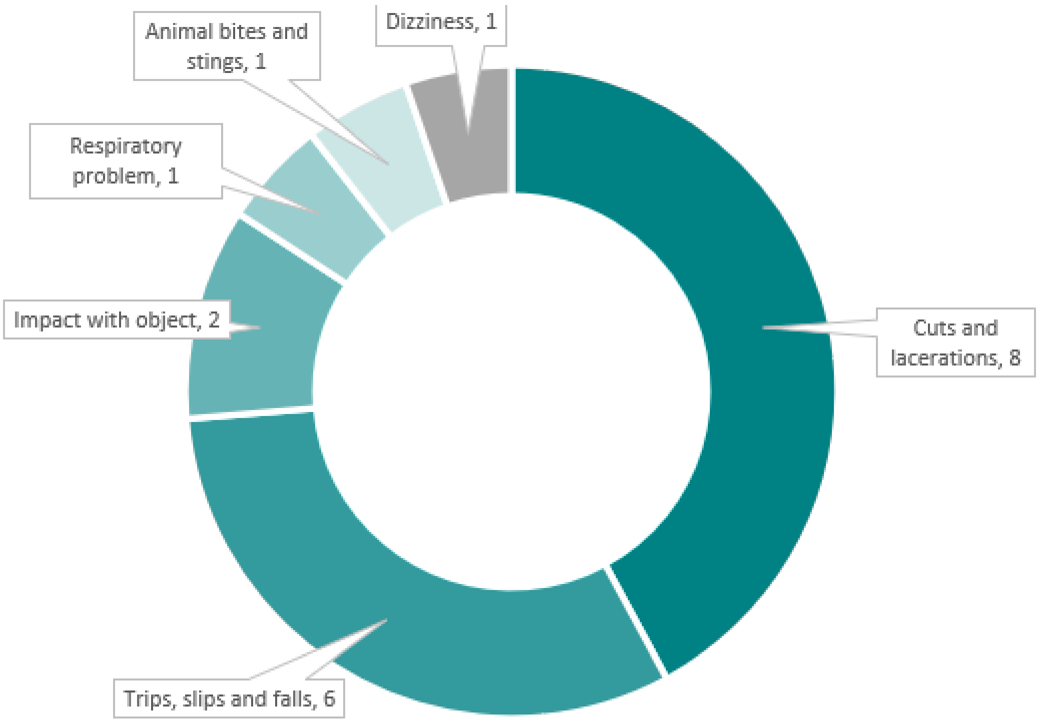
Graph 4: Public incidents by business activity

2.3.2a Public injuries

During the reporting period, there were 19 injuries to members of the public. Graph 5 shows the types of injuries that are occurring.

Reporting period	Non-treatment injury	FAI	MTI	Fatality	Total recordable injuries
July-Sept 21	2	7	0	0	**9**
Oct-Dec 21	0	11	0	0	**11**
Jan-Mar 22	2	17	0	0	**19**

Table 4. Recordable injuries (public)



Graph 5: Public incidents by injury type

2.4 Critical risk

Incidents were reported in all critical risk areas during this reporting period.

Psychosocial hazards (including anti-social behaviour and threatening communications) were the focus area this quarter. Customer Services staff have undertaken de-escalation training. Council continues to support employees to report hazards and incidents related to psychosocial hazards.

Critical risk	Existing controls	New or upcoming controls	Related incident reports
Driving and vehicles	• Vehicle User Policy • E-Roads installed in fleet vehicles • 5-Star ANCAP rated vehicles • Licenced drivers • Fleet inductions for new starters • Annual snow chain fitting training	• Vehicle User and Safe Driving policy review (including a review of driver training) • The health and safety committee is using E-road reports to recognise safe drivers • Snow chain fitting was held in May 2022	1
Remote or isolated working	• Working from Home Policy • Panic buttons • Work plans and risk assessments • Pair or buddy work systems	• Procurement project for a lone worker app • Work from home risk assessments	1

Psychosocial hazards	• Employee Assistance Programme (EAP) • Wellbeing programme • Regular 1:1s • Flexible working • Equal Employment Opportunity (EEO), Discrimination, Harassment and Bullying Policy • Performance Management Policy • Fit for Work Programme	• De-escalation training completed by new customer services team members • De-escalation training planned for aquatics teams	9
Biological hazards	• High-risk vaccinations programme • Barriers and fences • PPE is provided	• Reviewed our risk assessments for COVID-19 • Promoted annual flu vaccines	12
Hazardous chemicals	• Chemical register • Display safety data sheets • Appropriate storage • Quantities stored is kept at a minimum • Ventilation and circulation of air is monitored • PPE is provided for handling or working with chemicals • Records of training are maintained • Fire schemes updated with FENZ (chemical registers) • Qualified contractors	• A third-party health and safety contractor is supporting aquatics to audit hazardous chemicals procedures and handling practices	1

Table 5. Critical risk and controls

2.5 Training and initiatives

- Health and Safety Representatives will attend Stage 1 and Stage 2 training in May and June 2022.
- Fire warden training will return in the new financial year.
- Flu vaccinations were offered on-site at Alexandra Service Centre in May 2022.
- 43 staff participated in Move it March 2022. This is the first time this initiative has been run remotely.
- Financial wellbeing seminars will run from March-November 2022 in partnership with BNZ.
- Staff supported Pink Shirt Day on May 20, 2022
- New starters in the Customer Services team have completed de-escalation training

The following regular training was completed:

Training	Jan-Mar 2022	Financial YTD
New staff inductions	10	45
First aid	17	42
Fire warden	0	25
Chain fitting	13	NA

Table 6. Training register excerpt

3. Attachments

Appendix 1 - Risk Management Policy 2020-2021.pdf ⇩

Report author:

Rachel Ennis
Health, Safety and Wellbeing Officer
19/05/2022

Reviewed and authorised by:

Louise Fleck
Executive Manager - People and Culture
19/05/2022

Risk management policy

CENTRAL OTAGO DISTRICT COUNCIL

1 Dunorling Street
PO Box 122, Alexandra 9340
New Zealand

03 440 0056

Info@codc.govt.nz
www.codc.govt.nz

Department:	Risk and Procurement
Document ID:	500614
Approved by:	Council – 26 August 2020
Effective date:	26 August 2020
Next review:	26 August 2021

Purpose

Risk management is an integral aspect of Central Otago District Council operations.

Effective risk management ensures an integrated, structured and coordinated approach to operational risk management throughout all business functions and activities across the organisation. Risk cannot be eliminated entirely; however, it must be clearly understood, ensuring that any risks taken are appropriate for both the business activity and the business level.

This policy aims to support Council's objectives, providing assurance to both Council and the Audit and Risk Committee that risks are being managed appropriately and in line with objectives and the Council's risk appetite.

This policy is in line with the standards of best practice established by the AS/NZS *ISO31000:2009 Risk Management – Principles and Guidelines.* This shall be achieved through the continual implementation of risk management throughout processes within the organisation and creating a strong organisational risk aware culture.

Principles and objectives

Central Otago District Council's risk management processes will be applied in accordance with the following objectives.

- Embed a consistent risk management process with the implementation of a common approach to the identification, assessment, treating and monitoring of risks;
- Provide protection and continuity of core business activities;
- Promote a risk aware culture whereby all employees assume responsibility and proactively manage risk through sound decision making in their day to day activities;

- Define and establish clear responsibilities and structures to ensure risk management practices are incorporated into strategic, operational and project planning and review processes;
- Establish a consistent, clear framework to provide assurance that material risks are identified, regularly reviewed, monitored and managed to an acceptable level, in an open and transparent manner.

Scope

This policy shall apply to all business, service or activity conducted by Council and all employees of Council.

For the avoidance of any doubt, any reference to employees or staff in this policy shall include:

- the organisation's employees
- volunteers
- persons seconded to council
- contractors.

Specific risk management policies, procedures and/or guidelines relating to specialised areas will remain consistent with the broad directions in this policy.

Definitions

Word or phrase	Definition
Risk	The effect of uncertainty on objectives (adopted from the AS/NZS ISO 31000-2009 Risk Management Standard). Risk may be something unexpectedly occurring which impacts negatively upon council's strategic objectives. Risk is assessed in terms of likelihood and consequence.
Risk Assessment	The overall process of risk identification, risk analysis and risk evaluation.
Risk Management	An enabling function which adds value to the organisation, increasing the probability of success in achieving strategic objectives. Risk management aims to decrease the potential for legal liability and managing uncertainty; creating an organisation wide environment where the unexpected is

Word or phrase	Definition
	minimal and, should it occur, the consequences may be managed effectively.
Risk Management Framework	The set of components which provide foundations for designing, implementing, monitoring, reviewing and continually improving risk management within the organisation. Components include the Risk Management Policy, Process, Risk Registers.
Risk Management Process	The systematic and consistent application of policies, processes and practices of establishing the context, identifying, analysing, evaluating, communicating, treating, monitoring and reviewing risk.
Risk Register	A documented record of risks identified. This includes a description of risk, controls, risk levels and treatment plans.
Risk Appetite	The level of risk that council is willing to accept in pursuit of its strategic objectives.
Risk Tolerance	A measure of the level of risk an organization is willing to accept, used as a key criterion when making risk-based decisions.
Risk Owner	The position with authority and accountability for managing a specific risk and any associated risk controls.

Roles and responsibilities

All staff

Risk Management is the responsibility of all Central Otago District Council staff. The process of identifying and managing risk should underpin all council functions to insure transparency, authority and accountability. To remain effective, both the Risk Management Policy and Framework must be supported by an organisation-wide risk aware culture which will better enable council to achieve strategic goals.

Specific duties by role

To support the Risk Management Framework and ensure an appropriate degree of oversight, transparency and accountability in risk management practices around the organisation, the roles and responsibilities have been outlined in *Appendix One: Risk Management Roles and Responsibilities*.

Policy

Central Otago District Council shall maintain an effective and relevant Risk Management Framework, ensuring a structured, consistent and systematic approach to risk management across the organisation. Risk management documents shall remain relevant to the organisational culture, business objectives and organisational strategies, remaining applicable to all areas and in keeping with Council's risk appetite.

Core Principles

Central Otago District Council will establish, implement, maintain and monitor effective risk management processes aligned with the principles and processes described within AS/NZS *ISO31000:2009 Risk Management – Principles and Guidelines*. The following core principles are the foundation for Council Risk Management Processes.

- Facilitation of a risk-aware culture which is integrated into all critical planning and decision-making activities;
- Systematic, structured, transparent, informed and inclusive processes with the engagement of all relevant stakeholders, both internal and external where appropriate, contributing to risk discussions;
- Identify, assess, treat and monitor risks throughout the organisation;
- Recognise and integrate strategic, operational, human and cultural factors into processes;
- Maintaining dynamic and customisable yet resilient risk management processes which are responsive, adapting to a changing environment and Councils risk appetite in a timely manner;
- Reduce the likelihood of negative impacts on Council's strategic directives/objectives by obtaining the best possible information to base decisions from;
- Recognise, respect and support human and cultural factors which may influence risk management decisions.
- The Central Otago District Council Risk Management Framework shall include but is not limited to the following:
- Central Otago District Council Risk Management Policy – provides guidance and a foundation for the management of risk.

- Central Otago District Council Risk Management Process – provides guidance on identification of potential threats to an organisation and defines the strategy for eliminating, mitigating and/or minimising the impact of these risks, as well as processes to effectively monitor and evaluate this strategy.
- Central Otago District Council Strategic Risk Register – register of the organisations strategic and operational risk, with the inclusion of risk ratings and management/treatment plans.
- Central Otago District Council Group Risk Register – risk Register for each business area with the inclusion of risk ratings and management/treatment plans.
- Audit and Risk Committee – the overarching governance body assisting and advising Council in meeting the responsibility and ownership of governance, risk management and internal controls to achieve strategic objectives.
- Relevant information, training and educational activities for the ongoing improvement of risk management processes.
- Informed decisions are to be made based on a comprehensive understanding of the risks involved; It is acknowledged that some risks must be accepted in the achievement of strategic objectives.

Risk Reporting

Reporting of risk is an integral aspect of effective risk management, aiming to support the understanding of risk at all levels - to improve decision making, day to day operations and the achievement of objectives. Risk reporting is a fluid and constantly evolving process.

Risk reporting should focus on the change to the risk profile, outlining any emerging or potential risks which may require escalation.

Risk reports are to be prepared annually for the Executive Team and bi-annually for the Audit and Risk Committee. Risk management includes continual communications with both internal and external stakeholders.

Risk reporting shall detail the following.

- Risks which stand outside accepted tolerance levels
- Escalating risks
- Emerging risks
- Significant project risks.

Comprehensive reporting on significant risks contributes to effective governance.

Relevant legislation

AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines

Reporting and Monitoring

The policy shall be reviewed every three years or as required.

Related documents

- Staff Interest Policy
- Fraud, Bribery and Corruption Policy
- Fraud, Bribery and Corruption Process
- Protected Disclosure (Whistle blower) Policy
- Delegations Policy
- Register of Interest

Document Management Control:

Prepared by: Business Risk and Procurement Manager

File Location Reference: 500614

Date Issued: 26 August 2020

Attachments

Appendix One:	Risk Management Roles and Responsibilities
Appendix Two:	Risk Likelihood Table
Appendix Three:	Risk Consequence Table
Appendix Four:	Risk Matrix

Appendix One

Risk Management Roles and Responsibilities

Position	Roles and Responsibilities
Audit and Risk Committee	• The Audit and Risk Committee provides governance and oversight in the areas of audit and risk to ensure appropriate systems and best practices are delivered throughout the organisation and its activities. • Ensure that strategic planning and business operations are achieved within an effective Risk Management Framework. • Review and recommend approval of risk management frameworks, risk-related policies, the Risk-Register and review risk treatment options for critical risks. • Supervise Corporate Risk Registers • Monitor and review the risk management practices, systems and processes adopted by Council to ensure these remain relevant and appropriate. • Monitor Council's risk appetite and exposure and recommend to Council any pre-emptive or corrective actions in respect of risk management frameworks, the Risk Register and risk-related policies. • Approve and monitor the internal auditor's annual workplan, ensuring an adequate response to corrective actions are assumed and implemented.
Council	• Nominate members for the Audit and Risk Committee. • Confirm appropriate risk governance and management frameworks are in place, ensuring risks are appropriately managed, aiding in the achievement of Council’s strategic objectives. • Receive and evaluate reports from the Audit and Risk Committee.
Chief Executive Officer	• Lead and promote a risk-aware culture across the organisation. • Ensure overall accountability, authority and resources for managing risks within management and operational areas. • Champion a strong risk management culture across the organisation. • Report critical risks to Council with treatment options.
Executive Manager – Corporate Services	• Oversee the development and implementation of the Risk Management Policy and Risk Management Framework. • Ensure that the Risk Framework and Corporate Risk Register are regularly reviewed and maintained and inform the development and effectiveness of risk controls and management plans implemented.

	• Ensure appropriate reporting to the Audit and Risk Subcommittee and Council. • Receive disclosures from all members of staff relating to risk concerns or issues. • Review tracking of risks against the Risk Appetite tolerance limits.
Executive Team	• Champion a strong risk management culture across all of Council. • Maintain situational awareness of council-wide risk exposure, priorities and risk management activities. • Ensure the effective implementation of the organisation-wide Risk Management Framework and promote a risk-aware culture across the organisation. • Develop and maintain an effective Risk Management Policy. • Facilitate the identification, management and monitoring of the organisations Strategic and Operational Risks. • Undertake (at a minimum) a six-monthly review of the Corporate Risk Register, and the appropriateness of all Strategic Risk ratings, priorities, controls and management plans. • Monitor relevant Group Risk Register/s and ensure the appropriateness of all associated risk ratings, priorities, controls and management plans. • To facilitate the management of organisation-wide risks and risk management training.
Business Risk and Procurement Manager	• Responsible for the maintenance of the Risk Management Framework. • Support the development and provision of risk training and awareness-raising activities across the organisation. • Facilitate (at a minimum) a six-monthly review of the Corporate Risk Register, and inform associated risk ratings, priorities, controls and management plans. • Support the development of relevant business (BAU, project, contract) risk registers and appropriate risk management plans, activities and priorities, including providing specialist advice in relation to new or existing risks, appropriate management strategies and the escalation of risks. • Provide reports to, the Executive Team and the Audit and Risk Committee on Council's Strategic and Operational Risk exposure, to ensure effective oversight and assurance of all business risk management activities. • Alongside the Audit and Risk Committee, develop and manage the delivery of Council's annual internal audit plan and activities. • Support the activities of Council's Audit and Risk Committee. • In conjunction with the Executive Team, develop and review the Risk Management Policy and Risk Management Framework.

	• Receive disclosures from all members of staff relating to risk concerns or issues.
Managers	• Champion a risk-aware culture across the organisation and their group and drive implementation of the Risk Management Framework. • Develop and maintain relevant business (BAU, project, contract) risk registers and appropriate risk management plans, activities and priorities. • Implement risk management practices within relevant business areas. This includes ensuring that all operational risks are effectively identified, managed, reviewed and updated regularly. • Report all risks with a residual risk rating of high and critical to the Group Manager and/or Business Risk and Procurement Manager for review. • Prioritise resources, time and budget to those risks rated high and very high; and implement appropriate risk controls or business improvement activities. • Facilitate the identification, management and monitoring of Council's Strategic and Operational Risks, ensuring Risk Management is incorporated into the planning and delivery of the Council's core strategic and business activities. • Undertake (at a minimum) a six-monthly review of the Corporate Risk Register, and the appropriateness of all Operational Risk ratings, priorities, controls and management plans. • Develop and monitor respective Group Risk Register/s and ensure the appropriateness of all associated risk ratings, priorities, controls and management plans. • Alongside the Business Risk and Procurement Manager, facilitate the delivery of the annual internal audit plan and activities, and appropriate corrective or business improvement activities within their group.
All Staff	• To maintain awareness of risks, risk management and processes associated with risk management. • Ensure compliance with the Risk Management Policy. • Apply risk management practices in all day-to-day business activities. This involves systematically identifying, assessing and treating risks in accordance with the Risk Management Framework. • Ensure that risk management reporting is appropriately undertaken and advise their Manager, or the Business Risk and Procurement Manager of any risks residually rated as high or critical or that they believe require attention. • Maintain an awareness of current and potential/emerging risks that relate to their area of responsibility. • Support the implementation of risk mitigation.

Appendix two

Risk Likelihood Table

Score	Rating	Probability	Frequency	Likelihood Criteria
5	Almost Certain	>90%	Frequency of more than once a year	• Is expected to occur • Definite probability
4	Likely	60% - 90%	Frequency of occurring once a year	• Will probably occur
3	Moderate	20% - 60%	Frequency of occurring once every 5 years	• Could occur
2	Unlikely	5 – 20%	Frequency of occurring once in 5 -10 years	• Not generally expected to occur • The event hasn't occurred, but could
1	Rare	<5%	Once every 20 – 50 years.	• Exceptional circumstances • Improbable • Small chance of the event occurring • Caused by events and/or conditions previously unseen

Appendix three

Risk Consequence Table

Risk consequence category	Negligible	Minor	Moderate	Major	Extreme
	1	2	3	4	5
People and Health and Safety	No injury/harm. A possible near miss.	Minor injury or harm. Medical treatment required	Moderate injury or harm. One or more persons require medical treatment.	Serious injury or harm.	One or more fatalities or permanent disability or injury.
Compliance and legal/statutory and regulatory	Negligible compliance breach. Able to be remedied without penalty or notification.	Minor compliance breaches resulting in corrective actions.	Moderate statutory or regulatory breaches resulting in formal investigation by regulatory body, Council liability and fines may be provided.	Major statutory or regulatory breaches and litigation. External investigation, litigation, fines and implications for Executive Team.	Very serious statutory or regulatory breaches and litigation Serious court enforcement, prosecution or judicial review.
Environmental	Brief, non-hazardous and short-term impact on localised natural environment or ecosystem. Minor short-term reversible damage to landscapes	Minor damage including temporary pollution or contamination of localised natural environment or ecosystem. Minor reversible damage to landscapes. Temporary reduction of one or more of species.	Widespread damage to local natural environment and ecosystems taking several years to recover and extensive restoration work. Localised reversible damage to landscapes. Moderate reduction of one or more species.	Long-term and significant damage to natural environment and ecosystems taking >5 years to recover and significant restorative work. Localised irreversible damage to landscapes. Significant reduction in one or more species.	Irreversible and extensive damage to significant natural environments and ecosystems. Widespread irreversible damage to landscapes. Permanent loss of one or more species.
Reputation and stakeholder relationship	External Reputation not affected. No effort or expense required to recover.	Adverse attention from community groups and district media – no more than 1 day.	Regional and district media attention short term (1-3 days). Partial loss of stakeholder confidence. Negative association with CODC brand. little effort or	Nationwide media attention, more than 3 days. Significant reduction in stakeholder confidence. Negative association with CODC brand. Requires effort or expense to	Prolonged adverse national media attention. Significant long-term reduction in stakeholder confidence. Potential statutory management intervention. Significant

Risk consequence category	Negligible	Minor	Moderate	Major	Extreme
	1	2	3	4	5
			expense required to recover.	recover and mitigate.	damage to CODC brand requiring urgent effort and expense to recover. Involves unplanned council time to address.
Financial	Less than 10% loss of revenue, increase in expense or liability.	Between 10% and 19% loss of revenue, increase in expense or liability.	Between 20% and 29% loss of revenue, increase in expense or liability.	Between 30% and 49% loss of revenue, increase in expense or liability.	Greater than 50% loss of revenue, increase in expense or liability.
Performance and Capability	A disruption to any service or activity that causes an inconvenience for less than 4 hours. (half a workday) Negligible performance impact.	Minor impact on the quality or delivery of services offered. Disruption to any service or activity lasting less than one day	Some impact on the quality or delivery of services offered. 1 critical service or numerous non-critical service activities which are undeliverable for a minimum of one week.	Considerable impact on the quality or delivery of services offered. Impedes the achievement of objectives. One or a number of critical activities are undeliverable for a period between 2-4 weeks.	Major impact on the quality or delivery of services or operation. Sustained inability to deliver core services. One or a number of critical services or activities are unavailable for a period of more than one month.
Assets and Infrastructure	Impairment of a non-critical asset which causes an inconvenience for less than 4 hours. Minor damage to an asset	Impairment of a non-critical asset which interrupts service delivery for less than 1 day. Damage to an asset	Damage to one or more critical assets which interrupts service delivery for at least 1 week. Damage to multiple assets	Extensive damage to one or more critical assets which interrupts service delivery for a month. Loss of an asset	Damage to multiple critical assets which interrupts service delivery for more than 1 month. Loss of multiple assets
IS Systems and Data	Non-critical systems or data interrupted for less than 4 hours.	Loss of access to non-critical systems or data for less than 1 day.	Loss of access to critical systems and/or data for at least 1 week.	Loss of access to critical systems and data for between 2 to 4 weeks.	Loss of access to critical systems and data for more than 1 month.

Appendix four

Risk Matrix

Likelihood rating		Consequence rating				
		Negligible	Minor	Moderate	Major	Extreme
		1	2	3	4	5
Almost certain	5	Medium	Medium	High	Critical	Critical
Likely	4	Low	Medium	High	High	Critical
Moderate	3	Low	Medium	Medium	High	Critical
Unlikely	2	Low	Low	Medium	High	High
Rare	1	Low	Low	Low	Medium	High

6 CHAIR'S REPORT

22.2.8 CHAIR'S REPORT

Doc ID: 582660

1. Purpose

To consider the Chair's report.

Recommendations

That the report be received.

---

2. Attachments

Nil

7 MEMBERS' REPORTS

22.2.9 MEMBERS' REPORTS

Doc ID: 582662

1. Purpose

To consider the members’ reports.

Recommendations

That the reports be received.

2. Attachments

Nil

8 STATUS REPORTS

22.2.10 JUNE 2022 GOVERNANCE REPORT

Doc ID: 581855

1. Purpose

To report on items of general interest, consider the Audit and Risk Committee's forward work programme and the current status report updates.

Recommendations

That the report be received.

2. Discussion

Forward Work Programme
The Audit and Risk Committee's forward work programme has been included for information (appendix 1).

Status Report
The status report has been updated with actions undertaken since the last meeting (appendix 2).

3. Attachments

Appendix 1 - Audit and Risk Forward Work Plan ⇩
Appendix 2 - Audit and Risk Status Update ⇩

Report author:	Reviewed and authorised by:
W McEnteer	Sanchia Jacobs
Wayne McEnteer Governance Manager 24/05/2022	Sanchia Jacobs Chief Executive Officer 30/05/2022

Updated 24 May 2022

Audit and Risk
Forward Work Programme 2022 - 2023

Area of work and Lead Department	Reason for work	Committee's role (decision and/or direction)	Expected timeframes Highlight the month(s) this is expected to come to Audit and Risk in 2022/23											
			Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun
Long-term Plan 2021/31														
Long-term Plan Chief Advisor/Executive Manager - Corporate Services	Oversight of the preparation of the Long-term Plan.	**Direction required:** Direction on timeline and progress. To make recommendations to Council on matters and proposals relevant to risk management and internal review practices.	Not applicable until 2024/34 LTP is being prepared											
Annual Report														
Annual Report Executive Manager - Corporate Services	Oversight of the preparation of the Annual Report.	**Direction required:** For the Committee to recommend to Council that they adopt the 2020-2021 Annual Report subject to any changes the Committee may identify.			R									
Governance Reports														
Audit Management Reports Executive Manager - Corporate Services	Oversight of management reports post external audits	**Direction required:** Overseeing the progress of key recommendations arising from the audits.			R			R		R				R
Internal Audits														
Internal Audits Executive Managers / Business Risk and Procurement Advisor	Reviewing the internal audit programme of work (3 yearly) and the actions arising from those audits.	**Direction required:** Direction on timeline and progress. Identifying the key risks and actions arising from the audits.			R			R		R				R
Policy Reviews														
Policy Reviews Senior Strategy Advisor	Oversight of Council's policy renewal schedule and reviewing relevant updated and new policies.	**Direction required:** Provide feedback on policies and recommend for approval and implementation. Review policy schedule to ensure timelines are being achieved.			R			R		R				R
2022 Annual Plan														
2022 Annual Plan Executive Manager - Corporate Services	Oversight of the preparation of the Annual Plan (may include verbal update).	**Direction required:** Direction on timeline and progress. To make recommendations to Council on matters and proposals relevant to risk management and internal review practices.						V		V				

Updated 24 May 2022

Area of work and Lead Department	Reason for work	Committee's role (decision and/or direction)	Expected timeframes Highlight the month(s) this is expected to come to Audit and Risk in 2022/23											
			Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun
Litigation Update														
Litigation Updates Business Risk and Procurement Advisor	Oversight of Council's litigation register.	**Direction required:** Keeping an oversight of litigation that the Council is either involved in, or potentially involved in, to understand any risk.			R			R		R				R
Legislative Compliance Update														
Legislative Compliance Update Senior Strategy Advisor	Annual oversight of Central Otago District Council's compliance against relevant legislative requirements.	**Direction required:** Keeping an oversight that Council is meeting its legislative requirements.			R									

Key – R = recommendation , U = update, V = verbal update

Status Updates	**Committee**:	Audit and Risk Committee

Meeting	Report Title	Resolution No	Resolution	Officer	Status
25/02/2022	Audit and Risk Committee Terms of Reference	22.1.3	That the Audit and Risk Committee A. Receives the report and accepts the level of significance. B. Recommends to Council that they accept the proposed amendments to the Audit and Risk Committee's terms of reference as detailed in appendix 2 of the report. C. Recommends to Council that the reference to the Deputy Chair is removed from the delegation and that the term of the appointment of the Chair is clarified to include the words "each triennium following the year of election or as required."	Community Development Advisor	**02 Mar 2022** Action memo sent to report writer. **02 Mar 2022** Draft delegations updated for recommendation to the new Council in October 2022. MATTER CLOSED
25/02/2022	Local Government Official Information and Meetings Act 1987 (LGOIMA) Request Policy	22.1.7	That the Audit and Risk Committee A. Receives the report and accepts the level of significance. B. Supports the Chief Executive approval of this policy and issues to staff for implementation.	IS Manager	**02 Mar 2022** Action memo sent to report writer. **24 May 2022** CEO has approved the policy. MATTER CLOSED
25/02/2022	Privacy Policy	22.1.8	That the Audit and Risk Committee A. Receives the report and accepts the level of significance. B. Supports the Chief Executive approval of the policy and suggests its scope is expanded to include internal privacy relating to staff prior to implementation.	IS Manager	**02 Mar 2022** Action memo sent to report writer. **24 May 2022** CEO has approved the policy. Implementation tasks are ongoing for the Privacy Policy, including updating and standardising terms and conditions across all seven Council owned and managed websites. MATTER CLOSED

9 DATE OF THE NEXT MEETING

The date of the next scheduled meeting is 30 September 2022.

10 RESOLUTION TO EXCLUDE THE PUBLIC

Recommendations

That the public be excluded from the following parts of the proceedings of this meeting.

The general subject matter 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 of the Local Government Official Information and Meetings Act 1987 for the passing of this resolution are as follows:

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
Confidential Minutes of Ordinary Committee Meeting	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)(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 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 s7(2)(g) - the withholding of the information is necessary to maintain legal professional privilege s7(2)(i) - the withholding of the information is necessary to enable Council to carry on, without prejudice or disadvantage, negotiations (including commercial and industrial negotiations)	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
22.2.11 - Water Services Update on Compliance Status	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
22.2.12 - Strategic Risk Register	s7(2)(i) - the withholding of the information is necessary to enable Council to carry on, without prejudice or disadvantage, negotiations (including commercial and industrial negotiations)	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
22.2.13 - Litigation Register	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
22.2.14 - June 2022 Confidential Governance Report	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 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