



RANGITIKEI
DISTRICT COUNCIL

Making this place home.

Audit/Risk Committee Meeting

Order Paper

**Thursday, 29 November 2018
9.00am**

**Council Chamber, Rangitikei District Council
46 High Street, Marton**

Website: www.rangitikei.govt.nz
Telephone: 06 327-0099

Email: info@rangitikei.govt.nz
Facsimile: 06 327-6970

Chair

Mr Craig O'Connell

Membership

Councillors Nigel Belsham (deputy), Angus Gordon and Dean McManaway
His Worship the Mayor, Andy Watson (ex-officio)

Please Note: Items in this agenda may be subject to amendments or withdrawal at the meeting. It is recommended therefore that items not be reported upon until after adoption by the Council. Reporters who do not attend the meeting are requested to seek confirmation of the agenda material or proceedings of the meeting from the Chief Executive prior to any media reports being filed.



Rangitikei District Council

Audit and Risk Committee Meeting

Agenda – Thursday 29 November 2018 – 9:00 a.m.

Contents

1	Welcome	2	
2	Council prayer	2	
3	Apologies.....	2	
4	Members' conflict of interest	2	
5	Confirmation of order of business	2	
6	Confirmation of minutes	2	Attachment 1, pages 7 - 14
7	Chair's report	2	<i>To be tabled</i>
8	Work Programme matrix – progress update	2	Attachment 2, pages 15 - 19
9	Riskpool – call on members, July 2019	3	Attachment 3, pages 20 - 25
10	Internal Audit programme – audit focus risk analysis	3	Attachment 4, pages 26 – 29
11	Actions to reduce risk – half year update, November 2018	3	Attachment 5, pages 30- 36
12	Final Audit management report 2017/18	3	<i>Verbal</i>
13	Strategic risks for the Council	3	Attachment 6, pages 37 - 60
14	Update on the Government's review of the 3 waters infrastructure	4	<i>Agenda note</i>
15	Late items.....	5	
16	Future items for the agenda	5	
17	Next meeting.....	5	
18	Meeting closed.....	5	

The quorum for the Audit and Risk Committee is 3.

Council's Standing Orders (adopted 3 November 2016) 10.2 provide: The quorum for Council committees and sub-committees is as for Council, i.e. half the number of members if the number of members (including vacancies) is even or a majority if the number of members is odd.

1 Welcome

2 Council prayer

3 Apologies

4 Members' conflict of interest

Members are reminded of their obligation to declare any conflicts of interest they might have in respect of items on this agenda.

5 Confirmation of order of business

That, taking into account the explanation provided why the item is not on the meeting agenda and why the discussion of the item cannot be delayed until a subsequent meeting, be dealt with as a late item at this meeting.

6 Confirmation of minutes

The Minutes of the Audit/Risk Committee meeting held on 30 August 2018 are attached.

File ref: 3-CT-17-2

Recommendation:

That the Minutes of the Audit/Risk Committee meeting held on 30 August 2018 be taken as read and verified as an accurate and correct record of the meeting.

7 Chair's report

A report will be provided at the meeting.

Recommendation:

That the Chair's report to the Audit/Risk Committee meeting held on 29 November 2018 be received.

8 Work Programme matrix – progress update

An update is attached.

File ref: 3-CT-17-5

Recommendation:

That the Work programme matrix – progress update as at 20 November 2018 be received.

9 Riskpool – call on members, July 2019

A memorandum is attached.

File ref: 5-FM-6-1

Recommendation:

That the memorandum 'Riskpool – call on members, July 2019' be received.

10 Internal Audit programme – audit focus risk analysis

A letter and report from Cotton Kelly is attached.

File ref: 5-EX-2-6

Recommendation:

That the report 'Internal Audit programme – audit focus risk analysis' be received.

11 Actions to reduce risk – half year update, November 2018

An updated schedule is attached (together with the risk matrix).

File ref: 5-PY1-3

Recommendation:

That the updated schedule of 'Actions to reduce risk, November 2018', be received.

12 Final Audit management report 2017/18

A verbal update will be provided to the meeting.

13 Strategic risks for the Council

One of the areas of improvement for the Council identified in last year's report from the Independent Assessment Board was for councillors to be actively engaged in, and have a detailed understanding of, strategic risk issues. These are 'risks that affect or are created by an organisation's business strategy and strategic objectives'¹ Strategic risks are different from operational risk, financial risks, technology risks or compliance risks; they result from adverse business decisions, improper implementation of decisions or lack of responsiveness to changes in the business environment. This amounts to a refinement of the present risk management framework.

Suggested strategic risks for consideration by the Committee are:

¹ Deloitte, 'Exploring strategic risk', 2013, page 4.

- Reputation – driven by the speed and reach of social media;
- Human capital – organisation depth and values
- Financial stability
- Cyber-security
- Legal and political environment
- Climate change

Assuming there is time in the meeting to discuss these suggestions, it is intended to develop a more formal statement for the Committee's February 2019 meeting on Council's strategic risks. Once agreed to, this would be provided to Council.

Attached is the current strategic risk register for the Yorke Peninsula Council, a rural local authority in South Australia comprising 11,000 people and nearly 6,000km² in extent.

Also attached is the Government Communications Security Bureau's benchmark assessment of cyber security resilience across New Zealand's nationally significant organisations (released 31 October 2018).

14 Update on the Government's review of the 3 waters infrastructure

In September 2018, the Minister of Internal Affairs reiterated her intention to have options for changes to three waters before Cabinet later in the year with decisions on a regulator taken in 2019 as the first priority. She has been specific that the Government cannot separate out solutions by territorial authority: "we need to lift up, lead out and envision solution that will deliver gains across the country".

On 13 November 2018, Local Government New Zealand released its position statement, based on four principles:

- Fix drinking water first
- Let existing regulations run their course
- Take mandatory aggregation off the table
- Incentives matters.

On 20 November 2018, the Minister released two Cabinet papers. The first, from 29 October 2018, formally starts the process of rethinking the role of local government in achieving intergenerational wellbeing, with a report to the relevant Cabinet Committee in April 2019 (and an increased funding to Internal Affairs to meet the costs of the work programme, estimated at \$2.7 million. The second, from 5 November 2018, sets out a roadmap for future decisions on three waters reform. The initial focus (for report to the Cabinet Economic Development Committee in June) is developing detailed policy proposals for (i) drinking water and (ii) environmental regulation of the three waters sufficient to enable legislation to be drafted. The next stage is developing detailed policy proposals (for report to the Cabinet

Economic Development Committee late 2019) on service delivery arrangements following analysis of three high-level options – regulatory reforms only, a three waters fund to support voluntary sector-led improvements, and an aggregated system of dedicated, publicly-owned drinking water and wastewater providers. That work is to include ongoing engagement with stakeholders, iwi and Māori.

15 Late items

16 Future items for the agenda

17 Next meeting

28 February 2019, 9.00 am.

18 Meeting closed

Attachment 1



Rangitikei District Council

Audit and Risk Committee Meeting

Minutes – Thursday 30 August 2018 – 9:00 am

Contents

1	Welcome	3
2	Council prayer	3
3	Apologies.....	3
4	Members' conflict of interest	3
5	Confirmation of order of business	3
6	Confirmation of minutes	3
7	Chair's report	3
8	Questions put at previous meeting for advice or action.....	4
9	Review of terms of reference and objectives for the committee.....	4
10	Draft Annual Report for 2017/18.....	5
11	Update on the Government's review of the 3 waters infrastructure	5
12	Informing members about material matters between meetings	5
13	Management report from Audit New Zealand on the 2018-28 Long Term Plan	5
14	Work Programme Matrix – Progress update	6
15	Internal Audit programme – status report	6
16	Late items.....	6
17	Future items for the agenda	6
18	Next meeting.....	6
19	Meeting closed.....	7

The quorum for the Audit and Risk Committee is 3.

Council's Standing Orders (adopted 3 November 2016) 10.2 provide: The quorum for Council committees and sub-committees is as for Council, i.e. half the number of members if the number of members (including vacancies) is even or a majority if the number of members is odd.

Present: Mr Craig O'Connell (Chair)
His Worship the Mayor, Andy Watson
Cr Nigel Belsham
Cr Angus Gordon
Cr Dean McManaway

Also Present: Cr David Wilson

In attendance: Mr Ross McNeil, Chief Executive
Mr Michael Hodder, Community & Regulatory Services Group Manager
Ms Debbie Perera, Audit Director
Ms Nardia Gower, Governance Administrator
Ms Selena Anderson, Governance Administrator
Mr David Kelly, Cotton Kelly
Mr Michael Smit, Cotton Kelly

Tabled Documents Nil

1 Welcome

The meeting started at 9.04am. The Chair welcomed everyone to the meeting including Debbie Perera, Michael Smit and David Kelly.

2 Council prayer

The Chair read the Council prayer.

3 Apologies

That the apology for the late arrival of Cr McManaway was received.

4 Members' conflict of interest

Members were reminded of their obligation to declare any conflicts of interest they might have in respect of items on this agenda.

There were no declared conflicts of interest.

5 Confirmation of order of business

That, taking into account the explanation provided why the item is not on the meeting agenda and why the discussion of the item cannot be delayed until a subsequent meeting,

37 Kensington Rd, Marton

be dealt with as a late item at this meeting.

There was no scheduled change to the order of business.

6 Confirmation of minutes

Resolved minute number

18/ARK/013

File Ref

3-CT-17-2

That the Minutes of the Audit/Risk Committee meeting held on 11 June 2018 be taken as read and verified as an accurate and correct record of the meeting.

Cr Belsham / His Worship the Mayor. Carried

7 Chair's report

The Chair did not provide a report.

8 Questions put at previous meeting for advice or action

Addressed in items 9, 11 and 12.

9 Review of terms of reference and objectives for the Committee

The Chair led the Committee's discussion.

Cr McManaway arrived at 9.13am. The Chair checked that Cr McManaway had no conflicts of interest to declare

The following points were raised:

- The Committee's role is to ensure the process and monitoring of the framework that supports and service/project delivery is sound and mitigates risk. This includes information received by Council for projects, and what learnings are gained during and post service and project delivery.
- The Committee's role is to ensure the process and system of deciding to outsource or insource work is sound and the decision appropriate.
- Other Council committees should consider the Audit/Risk Committee as an avenue to provide a level of scrutiny should Council have concerns over a project or service.
- Council management should consider the Audit Risk Committee as an avenue to act as a sounding board on technical issues or as a support for potential disagreements between external audit and council that have escalated to a governing body level either prior or post an Audit Report.

The following amendments to draft were noted:

- | | |
|--------|--|
| Item 2 | Appetite for Risk (words from page 28 – LGNZ, <i>Audit and risk management</i> , page 2: 'Areas of focus...') |
| Item 5 | Oversight of Shared Services – revised wording to be drafted by the Chief Executive from a risk perspective, likewise business cases |
| Item 6 | The Committee to act as a sounding board for relevant issues that arise between management and External Audit. |

Resolved minute number

18/ARK/014

File Ref

3-OR-3-4

That the memorandum 'Review of the terms of reference for the Audit/Risk Committee' be received.

and

That the Audit/Risk Committee recommends to Council that it adopts the 'Audit Risk Committee terms of reference', as amended.

Cr Belsham / Cr McManaway. Carried

Cr Wilson arrived at 9.45am

10 Draft Annual Report for 2017/18

The Committee noted the commentary in the agenda.

11 Update on the Government's review of the 3 waters infrastructure

Mr McNeil gave a verbal update with the following key points:

Central Government has been clear about their desire to review the Three Waters. This has been driven in part by the Havelock North drinking water incident. Central government are considering whether the country will be divided on to a five entity framework or by regional council boundaries. The first report is due before Cabinet in October 2018, following which will be the establishment of a regulatory agency and detail on the new frame work.

Resolved minute number	18/ARK/015	File Ref	3-OR-3
-------------------------------	-------------------	-----------------	---------------

That the verbal update on the Government's review of the 3 waters infrastructure is received.

Cr Gordon / Chair. Carried

12 Informing members about material matters between meetings

The Chair noted that he will ensure raised issues and conversation occurring between meetings will be shared with committee members.

13 Management report from Audit New Zealand on the 2018-28 Long Term Plan

Ms Perera spoke to the report noting that the Audit NZ issued an unmodified audit opinion. This meant the LTP meets the statutory purpose and provides a reasonable basis for long-term integrated decision-making and co-ordination of the Council's resources and accountability of the Council to the community.

The misstatements were not derived from a system or process point of view and were explained by Ms Perera not material to adjust but are obliged to be reported.

Resolved minute number	18/ARK/016	File Ref	1-LTP-4-1
-------------------------------	-------------------	-----------------	------------------

That the Management report from Audit New Zealand on the 2018-28 Long Term Plan be received.

HWTM / MM. Carried

14 Work Programme Matrix – Progress update

Mr Hodder took the matrix as read. It was noted that Central Government has currently halted the Risk Agency, who would have been helpful in guiding the committee.

The committee discussed the risks associated with natural disasters and council continue to work alongside the regional council on gaining information on liquefaction prone areas of the district. It was noted that the insurance underwriter at Lloyd's states information in New Zealand is second to none.

Resolved minute number	18/ARK/017	File Ref	3-CT-17-5
-------------------------------	-------------------	-----------------	------------------

That the Audit/Risk Committee's work programme matrix (outlining progress to 20 August 2018) report be received.

MM / NB. Carried

15 Internal Audit programme – status report

David Kelly and Michael Smit (from Cotton Kelly) were in attendance and explained their current process of identifying key projects and getting synergy between councils, preparing a matrix for three member councils. They listed the top 6 elements as:

- 1 Procurement procedure
- 2 Cyber Security
- 3 Cash handling
- 4 Payroll process control
- 5 Conflicts of interest
- 6 Fraud

16 Late items

The Committee discussed the matter of 37 Kensington Road, Marton in the upcoming Council meeting later that day.

17 Future items for the agenda

Update from Cotton Kelly on internal audit matrix.

Revised Terms of reference

18 Next meeting

To be determined.

19 Meeting closed

10.32am

Confirmed/Chair: _____

Date:

Unconfirmed

Attachment 2

Topic	What	Why	Who/How	Priority	Committee decision/action	Progress to 20 November 2018
Annual Audit review	Interim management report (2017/18)	Ensure Council operating procedures and policies are appropriate and managed	Council management and Audit Director	Very high	Review Audit comment and Council response; recommendation to Council	Complete. The planned interim audit (second part) for 2017/18 in the first week of July was deferred (and shortened) because of the death of George McIrvine. Agreed no interim management report to be provided. Main audit commenced on 10 September. Adoption occurred on 11 October.
	Final management report (2017/18)	Ensure Council operating procedures and policies are appropriate and managed	Council management and Audit Director	High	Review Audit comment and Council response; recommendation to Council	Pending
Other reviews of Council operations		Ensure recommendations are well-founded and there is a robust plan of action	Chief Executive	Medium	As required. Consideration of interest-free loan to Edale was flagged once relevant information is received, but was not needed because of its purchase by the Masonic Villages Trust.	Complete. The Audit management report on the Consultation Document for the 2018-28 Long Term Plan was considered at the Committee's June meeting; the Audit management report on the final adopted Long Term Plan was included in the August meeting agenda.
Natural disaster events	Annual insurance reviews	Ensure accurate, appropriate and cost-effective cover for all built assets	GM Finance & Business Support	Medium	Review periodic updates from GM (Finance and Business Support) Committee has already reviewed whether to continue membership of LAPP.	In progress. Considered as part of additional cover being secured through MW LASS.
	Business continuity	Ensure Council can maintain business operations	GM Finance & Business Support	High	Review periodic updates from GM (Finance and Business Support)	Not yet considered. However, off-site storage of all servers has now been made secure.
	Disaster recovery	Ensure robust processes aligned with MCDEM requirements	Chief Executive	Very high	Review six-monthly updates on development of internal capability and external liaison, periodic MCDEM reviews, and recommend any changes or enhancements	In progress. Quarterly update on CDEM Improvement plans provided to Council's meetings in January, April, July 2018 and October
	Areas of unstable ground	Ensure awareness where land and buildings may be at risk		Low	to be determined	
Community facilities	Bulls community centre	Ensure robust project management for construction and fit-out	Chief Executive	High	Review and comment on project plan and exception reporting to each meeting	In progress. High-level project plan reviewed at Council workshop, 31 May 2018. Formal consideration of tenders at Council on 30 August 2018. Final decision (to award contract) made on 15 November 2018. Project team meets weekly/fortnightly.
	Marton civic centre	a) Ensure cost-effective option for new Civic Centre design	Chief Executive	High	Review and comment on project plan and exception reporting to each meeting	In progress. High-level project plan reviewed at Council workshop, 31 May 2018. Business case being prepared.
		b) Ensure robust project management for construction and fit-out	Chief Executive	High	Review project plan and exception reporting to each meeting	Not yet started.

	Taihape community facilities (on Memorial Park) and community centre (town hall site)	a) Ensure Memorial Park facility has external funding and community support		High	Review and comment on project plan and exception reporting to each meeting. Workshop consideration, 15 November 2018; report to be prepared for Council's meeting on 29 November.	In progress. High-level project plan reviewed at Council workshop, 31 May 2018. Discussions with Park users and key stakeholders led to a further report being required by Council for Assets/Infrastructure Committee's July 2018 meeting and a public meeting being held in Taihape on 3 August. This led the Committee to agree to investigate costs for the grandstand to be fully functional (as well as strengthened) and to seek clarification from Clubs Taihape on its intentions. Further consideration at Council workshop with decision report to be provided to Council's meeting on 29 November 2018.
		b) Ensure cost-effective and community support for new Civic Centre design		High	Review project plan and exception reporting to each meeting	Not yet started.
Risk management framework	Alignment with national/sector approach	Ensure framework reflects sector good practice	GM Community & Regulatory Services		Understand and give effect to Local Government Risk Agency expectations in the framework and follow-up actions	LGRA yet to be established.
	Biennial reviews	Ensure framework reflects changing risk environment	GM Community & Regulatory Services	Very high	Review proposed changes to framework and recommend to Council	Review due December 2019
	Half-year management actions to reduce risk	Ensure identified risks are being reduced	GM Community & Regulatory Services	High	Review adequacy of management action and recommend any changes to actions at August and February meetings	In progress. Proposed actions to address risk from December revision of the framework provided to Committee's February 2018 meeting. Report on actions taken provided to Committee's June and November 2018 meetings.

Topic	What	Why	Who/How		Committee decision/action	
Ongoing analysis of capital expenditure	Capacity	Ensure that the projected capital work programme is realistic (i.e. affordable and achievable)	GM Finance & Business Support	Very high	Review proposed capital programme at October or December meetings. Recommend changes to Council if warranted.	In progress. At its September 2017 the Committee considered a report on Council's involvement with the Local Government Funding Agency and recommended to Council that it participate in the Agency's scheme as a borrower. Council approved this recommendation. The capital programme for 2019/20 forecasted in the Long Term Plan will be reviewed as part of the preparation for the 2019/20 Annual Plan.
	Consenting requirements and timelines	Ensure that consenting requirements are reflected in capital programme		High	Examine briefing on consenting requirements at October meetings	Complete. Works programmes included in the draft Long Term Plan have been timed as to consenting requirements including seeking interim consents for Marton and Ratana wastewater upgrades and allowing for full consideration of options and (at Ratana) fulfilment of funding commitments. Horizons has made explicit its expectations about the timing of applications to renew consents.
	Carry-overs	Ensure that carry-overs are minimised and validated against external factors.	GM Finance & Business Support and GM Infrastructure	Medium		In progress. Council approved carry-forwards from 2017/18 to 2018/19 (incorporated in the final Long Term Plan) totalling \$19,229,729. In addition, \$177,780 was approved additional to the Long Term Plan budgets. Carry-forwards from 2018/19 to 2019/20 to be considered by Council's meeting on 31 January 2019.
Water supply	Drinking-water standards compliance	Ensure Council's potable water supplies address changes from Havelock North enquiry and government's timetable for implementing them	GM Infrastructure	Very high	Understand government policy setting; review project plan for giving effect to this and exception reporting to each meeting, and recommend Committee's view to Council.	In progress. Government's decisions on the Havelock North enquiry's recommendations not yet announced. Structural reform proposals from central government yet to be finalised, although Cabinet paper on scope/process released on 19 November. LGNZ has conducted a survey of territorial authority views and issued a position statement.
	Accurate billing for usage	Ensure that all water usage is paid for and that historical rights are correctly applied	GM Finance & Business Support	Medium	Review project plan and exception reporting to each meeting	Not yet considered.
Alignment with Council strategic framework and key priorities	Progress with key priorities (reported monthly to relevant Council committees)	Ensure that the identified key priorities are implemented or modified to give effect to the strategic direction	Chief Executive	High	Review draft consultation document for 2018-28 LTP at December 2017 meeting and determine whether risks and uncertainties have been adequately addressed.	Complete. Discussion at Committee's February 2018 meeting

Information management	Progress in implementing robust, integrated and accessible electronic corporate records systems	Ensure Council meets Public Records Act and LGOIMA requirements	GM Finance & Business Support	Medium	Review periodic updates on work programme and compliance with LGOIMA. There is currently no compliance reporting undertaken by Archives New Zealand	Not yet considered.
Infrastructure Shared Services (with Manawatu District Council)	Performance under revised agreement	Ensure Rangitikei is getting value for money and minimises risk of non-compliance in levels of service or funding of infrastructure	Chief Executive	Medium	Consider half-yearly assessments from Chief Executive and determine whether a recommendation to Council is warranted in terms of perceived risks	In progress. First quarterly update to Council's meeting on 29 March 2018. Principal Adviser Infrastructure started on 3 September 2018.
Appetite for risk around consents	Policy and procedure for exercise of discretion and enforcement of Code requirements	Ensure Council and local building sector are clear on balance between compliance and discretion	Chief Executive	Medium	Consider periodic updates from Chief Executive and determine whether a recommendation to Council is warranted in terms of perceived risks	Complete. Further consideration of issue on Committee's February 2018 meeting agenda. Approach considered and endorsed at Council's 1 March 2018 meeting. Subsequent notification of approach to local builders/building service providers. Enforcement strategy (and prosecution policy) adopted by Council on 26 April 2018; a report back on its effect due with Council's 29 November 2018 meeting.
Infrastructure inspection regimes	Condition reporting reflects age, maintenance and incidents	Ensure that asset condition reporting is comprehensive, is reviewed against inspections, and is reflected in capital/renewal programmes	GM Infrastructure	High	Review draft infrastructure strategy at October 2017 meeting and make recommendation to Council on adequacy of risk assessment	In progress. Draft strategy (combined infrastructure and financial) as provided to Audit included in Committee's February 2018 meeting agenda. However, there is uncertainty about the basis for the condition assessment reporting which needs to be resolved.

Attachment 3

Memorandum

To: Audit/Risk Committee

From: Michael Hodder. Community & Regulatory Services Group Manager

Date: 19 October 2018

Subject: **Riskpool – call on members, July 2019**

File: 5-FM-6-1

Attached is a letter dated 12 October 2018 advising that there will be a Riskpool call on members, payable on 1 July 2019. Rangitikei District Council will be invoiced \$26,023.76. There will be at least further (potentially final) call during 2022 or 2023 when the scheme is wound up.

Riskpool was established in 1997 as a local authority mutual liability fund. Since 2002, leaky building claims have dominated Riskpool's claims. These have come from owners of buildings that councils consented to, inspected and issued code compliance certificates for, which subsequently developed weather tightness problems (largely arising from once water gets inside the building it cannot easily get out, so rots wooden components).

Rangitikei withdrew from RiskPool on 11 June 2009. Despite frequent invitations to reconsider membership, Council declined to do so. However, while not noted in the various invitations to rejoin, membership of RiskPool is by Fund Year and membership ends only when the fund year is closed. To date, none of Riskpool's fund years has been closed. Council's withdrawal in June 2009 meant it was not a member in subsequent fund years, but its obligations for fund years before then remained. The last call from Riskpool evident in Council's files was in August 2012 (for \$46,879.75).

This situation affects other councils in the Horizons region which also withdrew. Legal advice is being sought.

This briefing was provided to the Finance/Performance Committee's meeting on 25 October 2018. The potential contingent liability has not been noted in Council's recent Annual Reports.

Recommendation

That the memorandum 'Riskpool – call on members, July 2019' be received.

Michael Hodder
Community & Regulatory Services Group Manager



12 October 2018

Andy Watson
Mayor of Rangitikei District Council
Private Bag 1102
Marton 4742

Dear Andy

Riskpool Call for 1 July 2019

Riskpool offered public liability and professional indemnity cover for twenty years. The decision was made that new covers from Riskpool would not be offered from 1 July 2017. This was a difficult decision to make, but support from the sector had dropped, particularly from the larger Council's. Without support from the sector Riskpool could not offer the competitively priced cover it had been able to offer in the past.

Members were advised last year that further additional contributions from members (calls) would be required.

As at 30 June 2018, Riskpool's accounts show a deficit of \$7.4 million. The deteriorating claims experience in 2017-18 means that Riskpool needs to make at least one interim call before a final call is made on wind up. The call will be \$6 million payable on 1 July 2019, split \$3million each to fund years 7 and 10.

The amount of this call for Rangitikei District Council will be \$26,023.76 payable on 1 July 2019 (or earlier if you wish). An invoice from Riskpool for this amount will be sent to the Council in May 2019.

Another and hopefully final call from Riskpool is likely in 2022 or 2023. It is expected that the amount of that call will be less than this one.

Kind regards

Tony Marryatt
Chairman of Riskpool

C/- Civic Financial Services Ltd (Funding and Scheme Manager)
04 978 1263
lan.brown@civicfs.co.nz

cc: Ross McNeil, Chief Executive of Rangitikei District Council

13 May 2014

File No: 5-FM-6-7

Juliet Martin
General Manager
New Zealand Mutual Liability Riskpool
P O Box 5521
Lambton Quay
Wellington 6145

Dear Juliet

Professional indemnity and public liability renewal - year 18 - Rangitikei District Council

Thank you for your letter (and email) of 9 May 2014 to George McIrvine, who is currently away on annual leave.

While we appreciate your invitation to re-join Riskpool, the Council will not be doing that.

Yours sincerely

Michael Hodder
Acting Chief Executive



New Zealand Mutual Liability RiskPool

P O Box 11-145
Wellington
New Zealand

Telephone 0-4-4958228
DD 0-4-4958216
Facsimile 0-4-4958177

15 June 2011

Clare Hadley
Rangitikei District Council
Private Bag 1102
Marton 4741

RECEIVED

23 JUN 2011

To: C-H
File: 5-FM-6-7
Doc: 11-0853

Dear Clare

LIABILITY RISKPOOL MEMBERSHIP

We are sure that this year's insurance renewals are not without their challenges and no doubt those challenges are consuming more executive time than usual, and do not wish to unnecessarily add to that.

The Board of RiskPool has asked us to invite Council to consider membership for the 2011-12 year. Our limits of indemnity for Public Liability and Professional Indemnity remain at \$100m each claim and in the annual aggregate. Our cover is fully reinsured and the fund has achieved a renewal that has allowed us to continue to provide cost benefits to our membership. The current membership remains committed to its Local Government liability fund for the 2011-12 fund year.


Based on our historical knowledge of Council and its claim experience we are able to confirm that if Council were to re-join RiskPool its contribution would be \$25,000.00 plus GST. This is based on excesses council last had as a RiskPool member.

Should Council wish to re-join RiskPool for the 2011-12 fund year, we will do what we can to assist with the transition.

Council will have access to our pro-active claims management services and our complimentary liability risk management advisory services.

Please feel free to call and discuss membership, or alternatively the writer is available to meet with you if you wish.

Yours sincerely
LIABILITY RISKPOOL


Paul Carpenter
SCHEME MANAGER



New Zealand Mutual Liability RiskPool

P O Box 11-145
Wellington
New Zealand

Telephone 0-4-4958228
DD 0-4-4958216
Facsimile 0-4-4958177

15 June 2009

RECEIVED

Michael Hodder
Rangitikei District Council
Private Bag 1102
Marton 4741

16 JUN 2009
To: MH
File: 5-FN-6-7
Doc: 09 1108

Dear Michael

RISKPOOL RENEWAL – WEATHERTIGHTNESS CLAIMS COVERAGE

Notwithstanding Council's letter dated 11 June 2009 advising of Council's withdrawal from RiskPool for the 2009-10 Fund Year, we thought it important to advise you of developments regarding RiskPool's weathertight claims cover.

We refer to our letter dated 11 May 2009 advising RiskPool renewal terms and also advising of our negotiations with our reinsurers to maintain the \$500,000 aggregate cover for weathertight claims for your Council.

The Board is delighted to advise that those negotiations have been successful and RiskPool has achieved reinsurer agreement to maintain that aggregated cover for your Council. As mentioned in our 11 May 2009 letter, the maintenance of this cover is at no additional cost to the renewal terms outlined in that letter. This is subject to formal Board approval. We have been able to achieve this outcome because your Council was identified as being low risk for these claims.

We trust that is in order and I will be in touch with you to discuss this with you further.

Yours sincerely

LIABILITY RISKPOOL


Paul Carpenter
SCHEME MANAGER

Attachment 4

Audit Focus Risk Analysis

Purpose

To carry out a preliminary assessment of the current range and frequency that topics of internal audit interest are being identified by Councils.

Analysis

A review of the following was carried out to gain some background as to where the current focus of Internal Audit is.

1. Internal Audit three year plans of the MWLASS¹s Councils that were available at the time of writing. Where an area of audit was included more than once in the three years it was counted twice. NZTA claims audit for example appears 3 times as one council's internal audit plan includes NZTA claims as an annual review.
2. Internal audit topics of focus as publicity available for the following non-MWLASS councils²
 - a. Hamilton
 - b. Christchurch
 - c. Porirua
 - d. Auckland
 - e. Waikato Regional Council
3. Relevant extracts from
 - a. Deloitte's Internal Audit Insights for 2018 (global)
 - b. Four Hot Internal Audits Topics 2018 (global)³

Findings

Over 30 areas of interest were identified for review, many of these only once and quite topic specific. For example: LOGOIMA requests, parks and property, native plant nursery, flood protection follow-up and water billing.

Procurement processes, controls, contract management and variations on these types of description were the most frequently mentioned area of interest being mentioned nine times in quite specific terms with a further two mentions as Vendor Risk/Third-party risk/contracted out key services. Additional matters that cross into this topic were Health and safety Contractor Management.

Area of Audit Focus	Number of Mentions
Procurement processes, controls, contract management	9 + 2
Cyber security ⁴ . Count doesn't include an IT Strategy & governance review 2017-18	6 (+1)

¹ 3 years

² Extracted off the web

³ Financial Executives International (FEI)

⁴ Also listed as a separate item by the Institute of Directors (IOD) Four Pillars of Governance Best Practice as a role for internal audit

Two x unusual transactions analysis (payroll, procurement, conflict of interest, journals) Three x sensitive expenditure, One x suspicious transactions	6
Payroll processes and controls (includes One x Leave Management)	5
Cash handling processes and controls	4
Business Continuity and Disaster Recovery/Crisis management	4
Fraud and Integrity/Antifraud Assessment	3
NZTA claims (one Council annually in 3 year plan)	3
Project Management	3
Health and Safety (2 H&S plus 1 H&S Contractor Management)	3
Risk Management/ Risk Management Maturity Assessment plus specific items that would fall into the risk category for example health and safety, legislative compliance, IT strategy and governance, insurance management.	2 (+specific items)
International: "New risk from business innovation, culture, regulatory compliance"; culture risk mentioned twice	
Vendor Risk/Third-party risk/contracted out key services (also reported in Procurement Count)	2
Stakeholder Engagement	2

Office of the Auditor General (OAG) Focus

In their *Introducing our Work about Procurement*, September 2018 report the OAG stated, "we will focus on procurement that is critical to improving outcomes for New Zealanders. We will look at the governance, management, and effectiveness of procurement in procurement-intensive public organisations and in high-spending areas. We will also look at procurement approaches that intend to achieve increased efficiency and innovation, including the use of all-of-government contracts, panels of suppliers, and public private partnerships. We are interested in how risks are managed where there is a dependence on suppliers of critical services."⁵

"We continue to see cases of procurement-related fraud in the public sector. This kind of fraud is carried out mainly through using false invoices – for example, employees with delegated authority entering false or overstated invoices for payment. We continue to see the misuse of credit and fuel cards. Cyber-related fraud also continues to pose risks to public organisations".⁶

"We have also considered in recent years allegations of procurement-related corruption involving public organisations. We will continue to demand transparency in how public organisations use public funds and what they have achieved".⁷

"Using a case-study approach, we intend to examine a small selection of procurements by local councils to highlight the importance of procurement capacity and capability and identify matters that local councils should focus on to reduce the risk of procurement failures."⁸

⁵ Introduction section. OAG *Introducing our Work about Procurement*, Sept 2018

⁶ Extract Para 1.23 OAG *Introducing our Work about Procurement*, Sept 2018

⁷ Extract Para 1.24 OAG *Introducing our Work about Procurement*, Sept 2018

⁸ Extract Para 3.12 OAG *Introducing our Work about Procurement*, Sept 2018

15 November 2018

Michael Hodder
Community & Regulatory Services Group Manager
Rangitikei District Council
Private Bag 1102
MARTON 4741

Dear Michael,

Audit Focus Risk Analysis for Audit and Risk Committee Agenda

Further to my email of 24 October 2018, enclosed now for the agenda of the Audit and Risk Committee being held on 29th November 2018, is the Audit Focus Risk Analysis.

I look forward to meeting the Audit and Risk Committee members, you and other Rangitikei District Council staff present at the meeting on the 29th November.

Yours sincerely,

Rachael Dean
Senior Internal Auditor

pp. 
Michael Swift.

Attachment 5

Actions from risk management framework (revised December 2017)

These actions address those situations where Council's Audit/Risk Committee, having considered the present systems and processes, has not accepted the assessed risk. The level of risk (e.g. 'D5') and assessment of effectiveness of controls (e.g. '3') are those shown in the risk management framework and explained in the risk matrix (attached).

The first half-yearly evaluation was done in June 2018.

		What will be done?	Progress to 31 May 2018
	Governance		
1.6	<p>Pursuing inappropriate business strategies</p> <p>Dec 2017: D5 2</p> <p>June 2018: D5...2</p> <p>Nov 2018: D5 2</p>	Development of a policy framework to define when a business case approach for projects will be adopted. ¹	<p>A policy framework has yet to be determined.</p> <p>However, the approach is being adopted for major community infrastructure projects where there are options which need consideration. The proposed relocation of Marton Administration is an instance of this.</p>
1.7	<p>Needs of stakeholders are not met</p> <p>Dec 2017: C2 3</p> <p>June 2018: C2 3</p> <p>Nov 2018: C2 3</p>	Clear use of survey results in terms of changes to services and facilities and reporting these back to stakeholders	Survey released in May 2018; results were analysed and improvement plans prepared (in conjunction with activity managers), provided to the relevant Council committee, with monitoring reports due in March 2019.
1.10	<p>Ineffective Council leadership</p> <p>Dec 2017: D4 3</p> <p>June 2018: D4 3</p> <p>Nov 2018: D4 3</p>	Development of agreed guidelines with Council on protocols to achieve a more effective governance-management balance with greater focus on understanding and addressing strategic risks	No formal discussion yet with Council.
	Business risks		
2.1	<p>Customer service eroded</p> <p>Dec 2017: C3 4</p> <p>June 2018: C3 4</p> <p>Nov 2018: B3 4</p>	<p>Monthly analysis for management of issues in service request.</p> <p>Customer service philosophy to be made explicit across the organisation</p> <p>Greater focus on getting feedback on specific transactions and analysing this</p>	Formal training for every staff member arranged (with an external provider) in July and new service charter developed and circulated.

¹ Not necessarily a dollar sum. Note that the business case is an input into a decision - **not** the decision

2.2	<p>Exposure to Council following poor tender process</p> <p>Dec 2017: D4 4 June 2018: D4 4 Nov 2018: D4 4</p>	<p>Review the procurement policy, potentially including:</p> <p>a) Mandatory use of local Tenderlink for all purchase with a total estimated cost exceeding \$50,000.</p> <p>b) Review by Management Team of recommendations for tenders under \$250,000 prior to decision by Chief Executive.</p> <p>c) Full disclosure of tender processes in public excluded sessions of Council, prior to decision, for tenders over \$250,000.</p>	<p>Proposed revision considered (in Council workshop) on 20 September 2018. Policy changes yet to be formalised.</p>
2.3	<p>Exposure to Council following poor contract management processes</p> <p>Dec 2017: D4 2 June 2018: D4 2 Nov 2018: D4 2</p>	<p>Develop and adopt policy for contract management</p> <p>Monthly reporting of performance of contracts with annual value exceeding \$250,000 to the relevant Council Committee.</p>	<p>Draft policy yet to be considered.</p>
2.6	<p>Inability to recover/continue business following disaster</p> <p>Dec 2017: D4 1 June 2018: C2 3 Nov 2018: C2 3</p>	<p>Develop a business continuity plan (to include consideration of both Taihape and Manawatu as alternative admin centres)</p> <p>Implement Civil Defence Improvement Plan (prepared in 2017)</p>	<p>Offsite business continuity in place.</p> <p>Civil defence Improvement Plan being implemented – quarterly reporting to Council</p>
2.7	<p>Relationship with Maori deteriorate</p> <p>Dec 2017: D4 3 June 2018: D3 3 Nov 2018: C2 4</p>	<p>Advance the Maori responsiveness framework</p> <p>Respond (as far as practicable) to Te Roopu Ahi Kaa's preferences for the proposed Maori/Iwi Liaison Officer role</p>	<p>Maori responsiveness framework agreed by Te Roopu Ahi Kaa and Council. This has been formally monitored on a quarterly basis.</p> <p>A half-time Strategic Adviser – Iwi/hapū position established, with appointee starting on 11 June.</p>
2.8	<p>Resource base does not meet community needs</p> <p>Dec 2017: E2 3 June 2018: E2 3</p>	<p>Continued lobbying (to central government and LGNZ) for ongoing, adequate financial</p>	<p>Ongoing</p> <p>A series of discussions has been initiated by the Mayor and the Chief Executive with key Ministers, in particular</p>

	Nov 2018: E2 3	support for roading, utilities and community infrastructure.	over accessing support from the Provincial Growth Fund
2.9	Business objectives not met Dec 2017: D3 2 June 2018: D3 2 Nov 2018: D3 2	Monthly monitoring by Management Team of progress with the capital programme.	Ongoing Early recognition of the need to carry-forward a substantial part of the capital programme in both utilities and community infrastructure
2.11	Shared Services falters and/or leads to higher costs for equivalent services Dec 2017: D4 3 June 2018: D3 4 Nov 2018: D3 4	Negotiate and monitor a more rigorous agreement with Manawatu for the delivery of infrastructure services to Rangitikei.	Completed Quarterly reviews (first at Finance/Performance Committee, 29 March 2018). This is a comprehensive review, with input from senior managers as well as Manawātū, thus increasing confidence that the relationship is robust.
2.12	Exposure to Council following non-compliance in consent processes. Dec 2017: D4 3 June 2018: D4 3 Nov 2018: D4 3	Review processes for monitoring drinking-water standard compliance and ensure full adherence to these.	<i>To be determined following government decisions on Havelock North Inquiry.²</i>
Built assets			
4.1b	Inability to provide services to stakeholders following damage to assets – by earthquakes Dec 2017: D8 0 June 2018: D8...0 Nov 2018: D8 0	Get clarity on meeting IL4 requirements for Emergency Operations Centres – and requirements for places of public assembly	June 2018 GHD commissioned, January 2018. Report received October 2018. Rough order of costs is \$325,000 for the Administration Building and \$98,000 for the Assets Building (but this would be less adequate, given its layout and distance from the emergency generator). Negotiations continue with Whanganui Area Health Board about having the Taihape Hospital function as a local EOC for the north of the District.
Human resources			
5.1	Breach of health and safety requirements Dec 2017: D4 4 June 2018: D4 4 Nov 2018: D4 4	Give effect to changes recommended as part of the ACC tertiary accreditation process and the audit undertaken by MW LASS	Ongoing SafePlus self-assessment tool will be available mid-2018. Informal audit by MW LASS considered processes and practices satisfactory.

² Use monthly compliance reporting as basis of discussion with Mid central health Drinking-water assessor

			Note special focus on (i) driver safety and (ii) asbestos management plans and actions arising from these.
5.3	<p>Poor employee performance</p> <p>Dec 2017: C3 4</p> <p>June 2018: C3 4</p> <p>Nov 2018: C3 4</p>	<p>Ensure Continuous Improvement process helps employees understand impact of individual performance on others and the organisation as a whole – i.e. personal; accountability for actions and their consequences.</p>	<p>Ongoing</p> <p>Impact will not be certain until the next employee survey is undertaken</p>
5.6	<p>Loss of corporate or tacit knowledge</p> <p>Dec 2017: D3 2</p> <p>June 2018: D3 3</p> <p>Nov 2018: D3 3</p>	<p>Implement Promapp which provides comprehensive documentation about 'how' things are done</p> <p>Use MW LASS to develop and apply shared expertise in specialised areas</p>	<p>Ongoing</p> <p>Reporting through Corporate Management Team</p> <p>Ongoing</p>
Information systems			
6.1	<p>Poor information management</p> <p>Dec 2017: D4 2</p> <p>June 2018: D4 2</p> <p>Nov 2018: D4 2</p>	<p>Ensure full documentation in SharePoint of contracts and projects undertaken by Infrastructure Shared Services.³</p> <p>Assess feasibility of replacing NCS/MagiQ to gain greater functionality and integration with SharePoint.</p>	<p>Ongoing</p> <p>Information Strategic Plan has been developed but postponed until new GM Finance & Business Support in place.</p> <p>Use of SharePoint a specific topic in the new Shared Services agreement.</p> <p>Accessibility of pre-SharePoint files evaluated.</p> <p>Consideration is being given to a replacement of NCS/MagiQ shared with other MW LASS councils.</p>
Financial management			
7.3	<p>Financial exposure in the event of a loss or disaster</p> <p>Dec 2017: D7 3</p> <p>June 2018: D6 3</p> <p>Nov 2018: D6 3</p>	<p>Adopt strategies to bridge gap between insurance (underground assets and roading)</p>	<p>Ongoing</p> <p>Priority task for the Principal Advisor Infrastructure</p>

³ This is part of the agreement negotiated with Manawatu District Council – 2.11. A related issue is access to the roading RAMM database.

	Natural resources and hazards		
8.3	<p>Insufficient regard to risks posed by earthquake-prone buildings</p> <p>Dec 2017: C3 3 June 2018: C3 3 Nov 2018: C3 4</p>	<p>Undertake mandatory assessment of all earthquake-prone buildings (including Council's) during 2018.</p> <p>Ensure staff and public awareness of risks posed by Council's own buildings</p>	<p>Focus remains on obtaining new, purpose-built and safe replacements for premises regularly used by staff and the community. Most Utilities plants have been assessed with remedial action taken/planned.</p> <p>Building team has been undertaking the initial visual inspections of buildings in the Marton CBD (including the Council's buildings) and advising owners of the outcome.</p> <p>Ongoing</p>

19 November 2018

Risk matrix

		Likelihood				
		Almost certain	Likely	Possible	Unlikely	Rare
Consequences or Impact	Catastrophic	Extreme	Extreme	Extreme	High	High
	Major	Extreme	Extreme	High	High	Moderate
	Moderate	Extreme	Extreme	High	Moderate	Low
	Minor	Extreme	High	Moderate	Low	Low
	Insignificant	High	High	Moderate	Low	Low

See table 2 of the Risk management policy for meaning of impacts in terms of human life, service levels. The environment, compliance and corporate governance, financial performance and community/political

		Likelihood				
		Almost certain	Likely	Possible	Unlikely	Rare
Consequences or Impact	Catastrophic	E8 (9)	E7 (8)	E5 (7)	D8 (6)	D6 (5)
	Major	E6 (8)	E4 (7)	D7 (6)	D5 (5)	C4 (4)
	Moderate	E3 (7)	E2 (6)	D4 (5)	C3 (4)	B4 (3)
	Minor	E1 (6)	D3 (5)	C2 (4)	B3 (3)	B2 (2)
	Insignificant	D2 (5)	D1 (4)	C1 (3)	B1 (2)	A (1)

Control effectiveness ratings

Rating	Effectiveness	Description	Quantification
0	Not effective	This control does not address risk	0%
1	Slightly effective	The control is not reliable as it is not well-designed, documented and/or communicated	1-20% effective
2	Somewhat effective	Control may be reliable but not very effective as control design can be improved	21-40% effective
3	Reasonably effective	Control is reliable but not effective as documentation and/or communication could be improved.	41-60% effective
4	Mostly effective	Control is mostly reliable and effective. Documentation exists but can be better communicated.	61-80% effective
5	Very effective	Control is reliable and effective. Fully documented process and well communicated.	81-100% effective

Source: Lismore City Council

Attachment 6

Yorke Peninsula Council Strategic Risk Register 2016 - 2020

Extreme
High
Moderate
Low

Risk Category	Risk No	Strategic Risk	#	Causes/Triggers	#	Consequences to YPC Council Strategy	Current			#	Impact Reduction Controls	#	Strategies to be Implemented	Residual			Strategic Management Plan Ref.	Risk Owner
							L	C	RR					L	C	RR		
Political	1	Cost shifting, Reduction and/or change in government funding.	1	Political parties, priorities change	1	Less tied or capped grants	L	MAJ	E	1	Detailed strategic and operational planning (i.e. rates modelling and budgeting)	1	Review opportunities for Partnerships/Shared Services with other LGAs and other agencies	P	MAJ	E	Goal 1 - Economically Prosperous Peninsula (1.5) Goal 2 - Community Connected through Infrastructure (2.4) Goal 5 - Responsible Governance (5.4)	Director Corporate and Community Services
			2	Demographics and population change	2	Lack of trust entering into new programs with Government				2	Lobby for more funding (politicians)							
			3	Reduction in funds available for local government due to financial pressure on State and Federal governments	3	Government funding reduced effect Council Services and potential Capital investment				3	Support and Representation on Local Government Association (LGA) and Australian Local Government Association (ALGA)							
			4	Changes to grant priorities	4	Effect and pressure on Councils Reputation				4	Plan to find other sources of revenue							
			5	Reprioritisation of their funding	5	Increased cost to ratepayers												
Political	2	Externally imposed organisational changes (including amalgamation)	1	Poor governance	1	Disruption/reduced Councils services	U	MAJ	H	1	Open/transparent/good governance	1	Succession Planning (Executive Management)	U	MAJ	H	Goal 5 - Responsible Governance (5.1, 5.2; 5.3; 5.5; 5.8; 5.10)	Chief Executive Officer
			2	Financial unsustainability	2	Employee unrest and/or stress				2	Open dialogue with State Government	2	Development Organisational Strategic Performance Reporting					
			3	Streamlining Services Local Government/Perceived economy of scale	3	Increase of assets and services to be managed				3	Strategic planning	3	Define Risk Management Framework					
			4	Legislative change	4	Effect and pressure on Councils Reputation				4	Long Term Financial Plan							
			5	Community Lobbying for Change														
Environment	3	Impacts of climate and increased number and/or severity of major disaster/climatic events	1	Severe Weather events	1	Additional costs above budget forecast	L	C	E	1	Asset and Infrastructure Management Plan	1	Street Trees/Shading/Trees/Climate Change Response Strategy	L	MAJ	E	Goal 2 - Community Connected through Infrastructure (2.1; 2.6) Goal 3 - Valued and Restored Environment (3.1; 3.2; 3.3; 3.4; 3.5; 3.6; 3.7, 3.9) Goal 5 - Responsible Governance (5.5)	Chief Executive Officer Director Assets and Infrastructure Services
			2	Increased unusual weather events.	2	May have a negative impact on YPCs reputation if overwhelmed by remediation requirements				2	Notifications from External Emergency Management Service providers (BOM, SES, CFS, SAPOL, etc.)	2	Emergency planning/Framework					
			3	Natural Disasters	3	Difficulty in forward planning				3	State Emergency Management Plan (SEMP)	3	Coastal Management Strategy					
					4	Public safety may be at risk if severity of events causes unknown/unidentified damage to infrastructure that then fails				4	Insurance	4	Environmental Management Plan					
					5	Decrease in revenue (potential population shift and decrease in land value)				5	International Council for local Environmental Initiatives (ICLEI) Water Campaign Local Action Plan							
					6	Damage to infrastructure potentially resulting in safety hazards to staff and community				6	Partnership with Environmental local Groups (i.e. Natural Resource Management (NRM))							
					7	Non Insurable events and Unbudgeted costs				7	Yorke and Mid North Climate Change Action Plan							
					8	Disruption/reduced Councils services				8	Roadside Vegetation Management Plan Review							
Economic	4	Changes in Economic Conditions in the Region	1	Changes in demographics	1	Changes (increase/decrease) to Councils services required and priorities	P	MOD	H	1	Support/Representation on Business, Regional Development Australia (RDA) YP Tourism and Community Initiatives		Current Impact Reduction Controls are deemed adequate in managing this risk.	P	MOD	H	Goal 1 - Economically Prosperous Peninsula (1.1; 1.2; 1.3; 1.4; 1.5; 1.6; 1.7; 1.8; 1.9) Goal 2 - Community Connected through Infrastructure (2.3; 2.4; 2.5; 2.7) Goal 4 - Community Engaged and Supported (4.1; 4.3; 4.4; 4.6; 4.7; 4.9; 4.10; 4.11; 4.13) Goal 5 - Responsible Governance (5.6; 5.9)	Chief Executive Officer
			2	Reduction in funds available for local government due to financial pressure on State and Federal governments	2	Planning and development impacts				2	Strategic Management Plan		No further action required					
			3	2. Close down of services (e.g. bus, schools, hospitals, etc.)	3	Socio economic impacts				3	Disability Action Plan (Access Committee) and support for Community Transport							
			4	Skill shortages within Region	4	Increase/Decrease on Councils ability to raise revenue to cover increased/decreased cost to Councils Services				4	Development Plan and Strategy							
			5	loss or gain of industry and business in region	5	Decrease in community members and the number of volunteers and community groups				5	Youth Engagement							
					6	New opportunities not realised				6	Marketing and promotion of Council Areas through Social Media and community engagement							
					7	Lots of expense but not necessarily results (recruitment - Lack of trained staff (medical and technical)				7	Appointment of Trainees from local region							
										8	Advocating/Lobbying with industry groups and government							
										9	Regional Health Plan							



Yorke Peninsula Council Strategic Risk Register 2016 - 2020

																		Extreme
																		High
																		Moderate
																		Low
Risk Category	Risk No	Strategic Risk	#	Causes/Triggers	#	Consequences to YPC Council Strategy	Current			#	Impact Reduction Controls	#	Strategies to be Implemented	Residual			Strategic Management Plan Ref.	Risk Owner
							L	C	RR					L	C	RR		
Legal	5	Changes to regulations and legislation impact Council operations	1	External pressures on Government (i.e. Lobbying by LGA, developers, community, activist groups, royal commissions, ombudsman investigations, ICAC, etc.)	1	Inappropriate land use for our area with potential Impact on development				1	Development Plans		Review of Financial internal controls library				Goal 1 - Economically Prosperous Peninsula (1.1; 1.2; 1.5)	Chief Executive Officer Director Development Services
			2	State government and/or political changes (including policies)	2	Council potentially losing power to make decisions				2	Support and Representation on Local Government Association (LGA) and Australian Local Government Association (ALGA)						Goal 3 - Valued and Restored Environment (3.9)	
			3	Climate/Increased environmental awareness (seawalls, emergency management)	3	Changes to documentation, Management systems and processes	L	MOD	H	3	Liaison/lobbying with Government Agencies			L	I	M	Goal 5 - Responsible Governance (5.3)	
			4		4	Reduction in community understanding				4	Provide training for staff in changes to legislative/regulatory changes							
			5		5	Additional workload/resources required				5	Ensure compliance - systems							
			6		6	Effect on Service Standards/Quality				6	Notification of legislative/regulatory changes from external body (including Local Government Association (LGA) initiatives, updates, etc.).							
Technology	6	Technology advances more rapidly than council is able to adapt	1	Limited infrastructure and/or systems	1	Reduced customer service/reputation				1	Proactive staff	1	IT Strategic Management Plan				Goal 2 - Community Connected through Infrastructure (2.2)	Director Corporate and Community Services
			2	Unskilled/trained staff	2	Community isolation				2	Training and provision of resources						Goal 4 - Community Engaged and Supported (4.3; 4.12)	
			3	Unaware of new technologies	3	Inefficient services (high cost and inflexible)				3	Research and/or investigate current trends						Goal 5 - Responsible Governance (5.2; 5.7)	
			4	Limited funding to buy in	4	Increased costs	L	MOD	H	4	IT Budgeting (infrastructure and asset management)			P	MIN	M		
			5	Limited resources	5	IT integrity and/or data losses				5	Community accessibility of services							
			6	Limited support/commitment to new emerging IT Solutions						6	Use External expertise							
			7	Cyber attack						7	Networking/participating with IT professionals/organisations							
										8	Mobility of Services							
Social	7	Councillors impose changes to Strategic Objectives	1	New Council/Councillors	1	Disgruntled community / organisation / staff				1	Community Consultation policy and procedure		Curent Impact Reduction Controls are deemed adequate in managing this risk. No further action required				Goal 5 - Responsible Governance (5.1; 5.2; 5.8)	Chief Executive Officer
			2	Funding changes/rate capping	2	Financial Instability/budgeting changes				2	Alignment to Strategic Management Plan							
			3	Influential senior officers	3	Loss of staff/volunteers	P	MOD	H	3	Marketing and promotion through Social Media and community engagement.			P	MIN	M		
			4	Poorly developed strategic objectives	4	Reputational damage				4	Regular comprehensive review of existing priorities (budgeting capital, etc.)							
			5	Conflict of Interest	5	Change to Council objectives/priorities				5	Elective Members Inductions/training							
Social	8	Changes of community expectations of Council	1	Lack of community engagement/understanding	1	Council/Councillor turnover (also staff)				1	Community Consultation policy and procedure		Curent Impact Reduction Controls are deemed adequate in managing this risk. No further action required				Goal 1 - Economically Prosperous Peninsula (1.4; 1.5)	Director Corporate and Community Services
			2	Changes in demographic/social make up	2	Reputation, credibility, loss of goodwill, poor morale				2	Marketing and promotion through Social Media and community engagement.						Goal 2 Community Connected through Infrastructure (2.2)	
			3	Benchmarking/comparison with other Councils Services	3	Changes to Councils services				3	Strategic Management Plan						Goal 3 - Valued and Restored Environment (3.4)	
			4	Changes to Councils services	4	Community apathy and/or unwillingness to get involved/unresponsiveness	P	MIN	M	4	Annual Business Plan			U	MIN	L	Goal 4 - Community Engaged and Supported (4.1; 4.3; 4.7; 4.12; 4.13)	
			5	Unsubstantiated information in the Community						5	Feedback/complaints/service requests systems and processes						Goal 5 - Responsible Governance (5.1; 5.8; 5.10)	
										6	Asset Management Plan							

Risk Category has been based on the PESTLE modle. PESTLE is a popular frame work for gaining an understnding of key factors and trends in broader society. PESTLE Analysis is a popular framework for organising these factors and trends and isolating how they influence industries and the firms within them.

P	E	S	T	E	L
<ul style="list-style-type: none">- Government policy- Political stability- Corruption- Foreign trade policy- Tax policy- Labour law- Trade restrictions	<ul style="list-style-type: none">- Economic growth- Exchange rates- Interest rates- Inflation rates- Disposable income- Unemployment rates	<ul style="list-style-type: none">- Population growth rate- Age distribution- Career attitudes- Safety emphasis- Health consciousness- Lifestyle attitudes- Cultural barriers	<ul style="list-style-type: none">- Technology incentives- Level of innovation- Automation- R&D activity- Technological change- Technological awareness	<ul style="list-style-type: none">- Weather- Climate- Environmental policies- Climate change- Pressures from NGO's	<ul style="list-style-type: none">- Discrimination laws- Antitrust laws- Employment laws- Consumer protection laws- Copyright and patent laws- Health and safety laws

PR098 - Risk Management Procedure Extract
Appendix A – Council Risk Management Matrix

Consequence Rating							
Description	Safety	Reputation	Legal & Regulatory	Environmental	Financial	IT / Records	Service Delivery
Catastrophic	Fatality. Severe injury or illness giving rise to a disability or impairment. Litigation.	State negative media coverage. Irreparable damage to reputation. Public outcry.	Significant prosecution for organisation and individuals. Fines. Very serious litigation.	Extensive, very serious and long-term impairment of the environment. EPA involvement or investigation.	> \$1 mil	Extensive loss / damage to IT and communications assets and infrastructure. Permanent loss of data. Widespread disruption to the business.	Extreme loss of service quality.
Major	No fatality. Serious (but non-life threatening) injury or illness. Critical failure of internal controls.	Extensive local negative media coverage. Loss of reputation that will require external resources. Public concern.	Major breach of legislation or regulation. Prosecution. Fines. Litigation.	Serious (>6months) impairment of the environment.	> \$250k to < \$1 mil	High risk of loss, data corrupt. Significant catch up required. Business Continuity Plan implemented.	Major decline in the quality and value of service delivery. Probable decrease in the community's confidence in the Council.
Moderate	No fatality. Non-life threatening injury/illness. Medical treatment and/or hospitalisation required. Serious breach involving statutory authority investigation. Significant failure of internal controls.	Significant local media attention. Significant number of complaints.	Serious breach of legislation or regulation with investigation and/or report to relevant authority. Limited fine or other penalty possible.	Moderate damage or impairment of the environment. Repairable in 1 to 6 months.	> \$50k to < \$250k	Moderate to high loss / damage to IT and communications. Data lost.	Moderate decline in the quality and value of service delivery. Possible decrease in the community's confidence in the Council.
Minor	Minor reversible injury requiring medical treatment by doctor. No hospitalisation. Contained non-compliance with short term significance.	Heightened negative local media attention. Low number of complaints.	Breach of legislation or regulation with noted compliance failure. Requirement for report to regulator or authority.	Limited damage or impairment of the environment. Repairable within 1 month.	< \$50k	Minor loss / damage to IT and communications. Some catch up required.	Untimely service delivery to our community. Should not decrease the community's confidence in the Council.
Insignificant	A minor injury that is treated on site. Near miss or incident that does not give rise to any injury.	A number of complaints.	Minor non-compliance. Minimal failure of internal controls.	Minor containable incident with no measurable impairment or impact of the environment.	< \$20k	Negligible loss of or damage to IT and communications. No loss of data.	Minimal decline in the quality and value of service delivery.

Likelihood Rating	
Almost Certain	Is expected to occur in most circumstances
Likely	Will probably occur in most circumstances
Possible	Might occur at some time
Unlikely	Could occur at some time
Rare	May only occur in exceptional circumstances

Risk Matrix						
Consequence and Reporting Action						
Likelihood		Insignificant	Minor	Moderate	Major	Catastrophic
	Almost Certain	High	High	Extreme	Extreme	Extreme
	Likely	Moderate	High	High	Extreme	Extreme
	Possible	Low	Moderate	High	Extreme	Extreme
	Unlikely	Low	Low	Moderate	High	Extreme
	Rare	Low	Low	Moderate	High	High

THINKING AHEAD. BEING PREPARED.

Cyber Security Resilience of New Zealand's
Nationally Significant Organisations 2017-2018

NATIONAL CYBER SECURITY CENTRE
A PART OF THE GCSB



New Zealand Government



Contents

Foreword	2
What we do	3
Executive summary	4
Introduction	6
Key finding: Governance	8
Key finding: Investment	10
Key finding: Readiness	12
Key finding: Supply Chain	14
Next steps	16



GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

In order for New Zealand to stay competitive we need to keep pace with the rapid changes in technology. Cyber security concerns are affecting our confidence in keeping on top of this. With a mindset shift, organisations can benefit from having a robust plan. It's all about maintaining good oversight, good resources, getting the right expertise on board, and being in a state of constant readiness. It's simple when it comes down to it; thinking ahead and being better prepared.

FOREWORD

The cyber security risks facing New Zealand's nationally significant organisations (NSOs) are increasing at the same rate as society's dependency on information technology.

Cyber security is a complex issue affecting a broad spectrum of New Zealand organisations, and New Zealand society as whole. From NSOs to individuals; from the executive board room to technical specialists on the front line, a joined up approach is key to improving New Zealand's cyber security posture.

New Zealand's National Cyber Security Centre (NCSC) – a part of the Government Communications Security Bureau – has developed a nationwide understanding of the cyber security resilience of New Zealand's NSOs. This report shares insight gathered from the first comprehensive cyber security survey of New Zealand's NSOs.

It identifies four key focus areas in which New Zealand organisations could improve, and provides practical steps that organisations can take to strengthen their cyber security posture and resilience.

The NCSC would like to acknowledge the vital contribution made by NSOs in taking the time to talk with us over the past year. This report would not have been possible without the input and cooperation of NSOs up and down the country.

Each contributing organisation has received an individual response that outlines areas for their own improvement. At the same time, the NCSC is publishing this summary assessment to highlight wider trends and to inform decision making more generally.

New Zealand's NSOs should be optimistic about their ability to improve their own cyber security posture. There is a risk that organisations feel powerless to improve cyber security when the most commonly noted trend is that threats and incidents continue to increase. However, international data shows us that improvements in cyber security are possible when pursued systematically and strategically.

Continual improvement of cyber security across New Zealand's NSOs demands a joint effort. The NCSC will continue to provide support and guidance as part of our core business. But at the same time, organisations themselves, security suppliers and IT vendors play an integral role in lifting the cyber security resilience of our most important information infrastructures and in turn protecting the national security of New Zealand.



Andrew Hampton
Director General
Government Communications Security Bureau

WHAT WE DO

The NCSC is a part of the Government Communications Security Bureau (GCSB). We deal with advanced cyber threats that have the potential to affect New Zealand's national security and the economy.

Our mandated focus is on New Zealand's nationally significant organisations. These include the most critical government departments, key economic generators, niche exporters, research institutions and operators of critical national infrastructure.

We are aware of a range of international cyber threat actors that target New Zealand computer systems and information infrastructure for financial gain or as a means of advancing their own position.

New Zealand's cyber threat environment is increasingly complex and far from benign. The sources of hostile cyber activities and cyber crime include both state-sponsored and non-state actors.

The NCSC works with New Zealand's NSOs to counter these threats:

- We supply advanced cyber threat detection and disruption services (CORTEX) to organisations of national significance.
- We respond to cyber incidents that pose a potential threat to New Zealand's national security and economic well-being.
- We provide analysis and assessment of cyber threats to our customers and partners.
- We foster a mature security culture based on standards set out in the Government's Protective Security Requirements and the New Zealand Information Security Manual.

The NCSC also works closely with CERT NZ (Computer Emergency Response Team) to provide guidance and help on cyber threats. CERT NZ helps business, organisations and individuals wanting prevention and mitigation advice about online security issues.

“New Zealand's cyber threat environment is increasingly complex and far from benign.”

EXECUTIVE SUMMARY

As New Zealand organisations adopt digital products and services at pace, they need to ensure they adjust their business risk settings, particularly the implementation of good cyber security policies and practices.

Digital transformation is underway in organisations across the public and private sectors and cyber security is crucial to ensure this transformation is sustainable and achievable. Without effective cyber security, organisations will struggle to consistently deliver digital products and services in a way that retains the trust and confidence of their customers or stakeholders.

The NCSC's analysis of data gathered from 250 New Zealand NSOs has identified four areas of good practice where organisations can focus their efforts for the greatest effect. These areas are:

- **Governance** – Promoting cyber security at a senior leadership level to protect an organisation's most important digital assets.
- **Investment** – Investing in cyber security to minimise risk and maximise returns.
- **Readiness** – Preparing the organisation to detect, respond, and recover from a cyber security incident.
- **Supply Chain** – Maintaining oversight and awareness of the cyber security risks in an organisation's supply chain.

The diversity and size of New Zealand organisations means they are not conducive to a 'one-size-fits-all' approach. Often, small organisations have insufficient resources to protect all assets equally or a growing organisation may have a higher risk appetite. However, the focus areas identified in this report overlap and are mutually reinforcing; even small improvements in any of these categories will help raise cyber resilience overall.

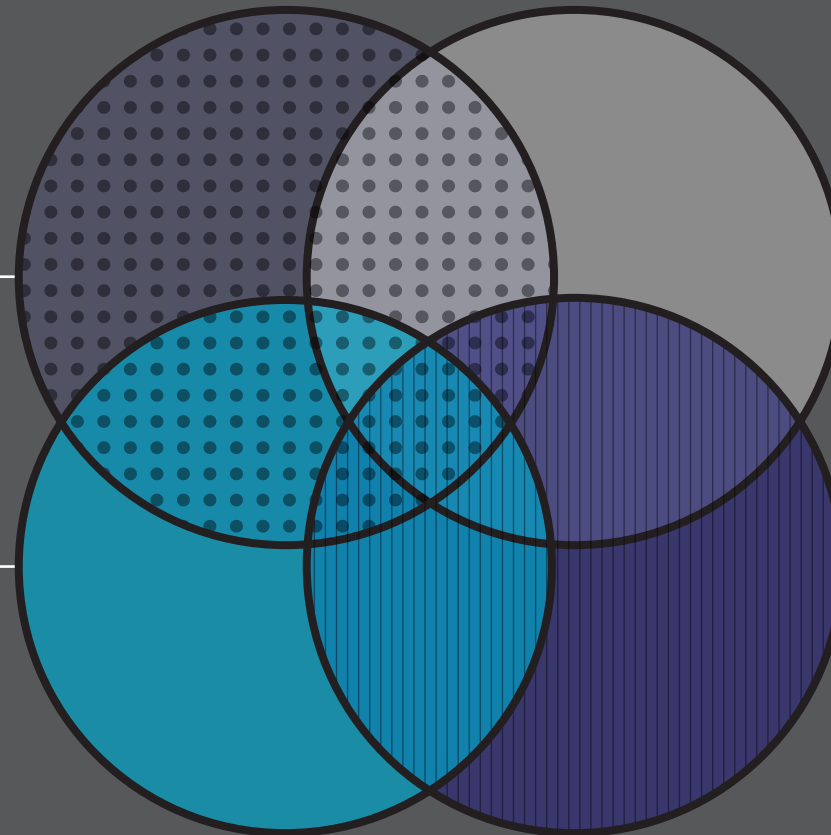
To assist organisations to improve their cyber security and resilience, the report outlines practical steps that can be taken in the four areas mentioned and provides links to useful resources.

GOVERNANCE

Promoting cyber security at a senior leadership level to protect an organisation's most important digital assets.

INVESTMENT

Investing in cyber security to minimise risk and maximise returns.



READINESS

Preparing the organisation to detect, respond, and recover from a cyber security incident.

SUPPLY CHAIN

Maintaining oversight and awareness of the cyber security risks in an organisation's supply chain.

INTRODUCTION

This report summarises key findings from cyber security assessments undertaken with New Zealand's NSOs.

250

250 organisations of national significance responded to a survey developed by the NCSC.

135

Over half of the organisations interviewed have fewer than 500 employees.

The report provides organisations and cyber security professionals with a New Zealand-centric snapshot of where the greatest improvements in cyber security can be achieved. The NCSC is using the information gathered in our survey to focus and inform decisions about our cyber security products, services and the support we provide to NSOs. The data will also assist us to measure New Zealand's progress towards improved levels of cyber security over time.

Methodology of survey

This report is based on the responses of 250 organisations of national significance to a survey developed by the NCSC. All respondents are nationally significant organisations. The survey was composed of 50 questions based on industry standards and principles contained in the New Zealand Information Security Manual and Protective Security Requirements.

The survey was delivered by the NCSC's Outreach and Engagement team, which conducts over 2000 engagements annually with NSOs. Each organisation's response to these questions was based on their own perception and not the NCSC's assessment of their capabilities. The information provided by individual organisations has been anonymised to protect their identity.

NCSC's focus on NSOs

The NCSC's mandated focus, and the focus of this report, is on New Zealand's NSOs. These include the most critical government departments, key economic generators, niche exporters, research institutions and operators of critical national infrastructure. Although modest in size by international standards – over half of the organisations interviewed have fewer than 500 employees – they all provide an important contribution to New Zealand's economic security and wellbeing.

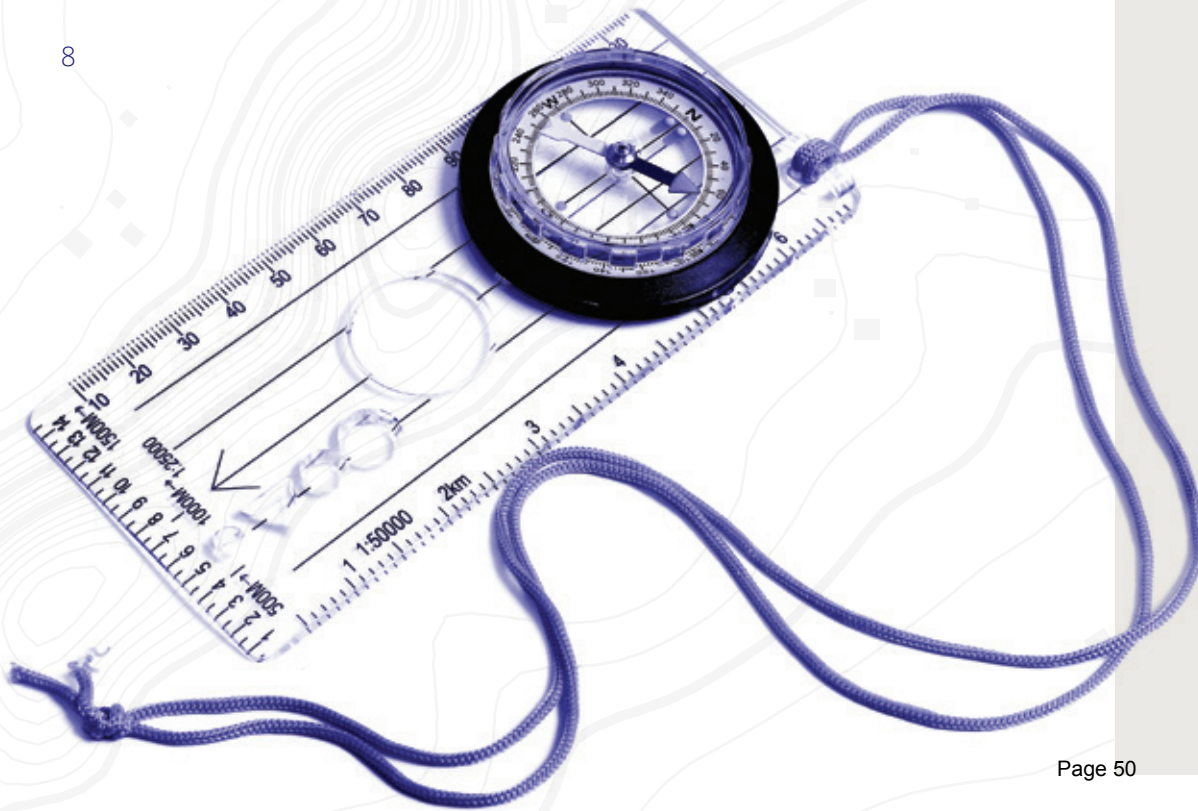
The assessment data identifies how these NSOs would benefit from the NCSC's support. It allows the NCSC to use an evidence-based approach to focus its attention and target resources to achieve the best value for government investment in cyber security. The baselining of cyber security of New Zealand's organisations of national significance is an important step in a journey to support our most important organisations to raise their cyber security resilience.

“The assessment data identifies how these NSOs would benefit from the NCSC's support.”

CHARTING YOUR COURSE.

Promoting cyber security at a senior leadership level to protect an organisation's most important digital assets.

8



What is cyber security governance and why is it important?

Governance refers to the oversight of cyber security at a board or executive level. Boards and executives are ultimately responsible for the outcomes of any cyber incident, including the impact on stakeholder and customer confidence. Executives and board members play a critical role in driving cyber security as a priority within the organisation, and equally important, ensuring it aligns with organisational objectives.

The creation or elevation of the Chief Information Security Officer (CISO) role within an organisation recognises the need for cyber security to be represented at a senior level. The effectiveness of the CISO function influences the alignment between cyber security investment and the organisation's business objectives. The CISO should be able to articulate to other board members the impact of poor security on the organisation's business operations, new projects and legal risks; as well as monitoring the return on investment in security.

The New Zealand cyber security governance gap

Only 19% of organisations surveyed have a dedicated Chief Information Security Officer (CISO). The remaining 81% either do not have a CISO at all, or have a senior manager that performs the CISO function as part of a broader role. When a CISO has two roles there is inevitable tension between delivering technology projects and advocating for security. Having separate roles ensures both outcomes are effectively represented.

The absence of a dedicated CISO often reflects the smaller size of New Zealand organisations, where specialisation to this extent is not always financially viable. However, it also shows cyber security can lack a strong advocate at executive or board level discussions.

The absence of high level representation within organisations is compounded by a lack of regular reporting of cyber security information to senior management – 39% of organisations do not provide cyber security reporting to senior management or only do so on an ad hoc basis. Even without a CISO, an organisation can still make cyber security issues visible to management through regular reporting of incidents or issues.

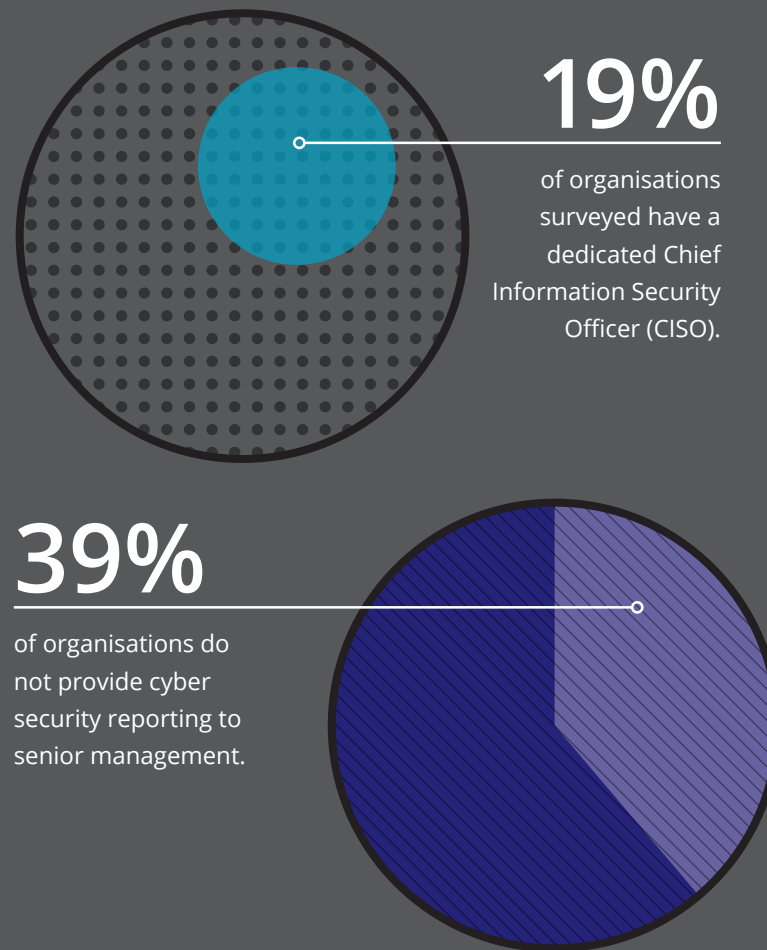
Suggested steps to increase maturity

- Identify the person, or people, who are accountable for cyber security in your organisation.
- Ensure your organisation's leadership receives regular reporting on security issues from your IT team or service provider.
- Make cyber security reporting easier to consume. For example, report cyber security 'near misses' in the same way as you might report Health and Safety issues.

Useful resources

- <https://www.iod.org.nz/Governance-Resources/Publications/Practice-guides/Cyber-Risk-Practice-Guide>
- <https://www.ncsc.govt.nz/assets/NCSC-Documents/cyber-security-risk-management-board.pdf>

The organisations surveyed:



PUTTING THE RIGHT THINGS IN PLACE.

Investing in cyber security to minimise risk and maximise returns.

10



Cyber security investment in New Zealand

73%

The majority of organisations surveyed (73%) increased their spending on cyber security in the past year. However, the NCSC's survey suggests that this investment had not translated into an increased confidence in their cyber security resilience.

33%

A likely contributing factor is that only 33% of organisations had fully identified their critical information assets. If an organisation is unclear about what its most critical assets are, it is difficult to be confident they are protected. It also becomes very difficult to make risk-based decisions to prioritise spending in the most important areas.

52%

Spending has increased across all areas of cyber security, but most organisations are spending on new tools and vulnerability assessments. This focus on investment in technology has come at the cost of investment in people. As a result, 52% of organisations reported they had insufficient numbers of skilled staff to satisfy their perceived security requirements.

38%

Only 38% of organisations surveyed had some separation between their cyber security budget and regular IT budget. This lack of separation can result in cyber security budgets being used for non-security related IT purposes, and limits the ability to track return on cyber security investments.

Why is well-directed investment critical for cyber security?

Investment is necessary for any organisation to improve their cyber security. An organisation that decides not to invest in cyber security is more likely to become a victim and experience higher costs in the event of a cyber incident. However, not all investment returns the same value to an organisation. Agreement at a governance level on the organisation's risk appetite and identification of key assets are critical first steps to ensure investment is directed and balanced appropriately.

Area of spending	Percentage of organisations that increased spending in this area in the past 12 months
IT STAFF TRAINING	54%
MORE IT SECURITY STAFF	45%
VULNERABILITY ASSESSMENTS	61%
NEW TOOLS	70%
AUDITS	55%

Suggested steps to increase maturity

- Balance strategic, longer term investments in the development of assets and staff over "one off" costs for vulnerability assessment snapshots.
- Identify the information assets that are most critical to your business and assess the risks posed to these assets.
- Create a separate budget line to effectively manage and track IT security spending.

Useful resources

- <https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697>
- <https://www.ict.govt.nz/assets/ICT-System-Assurance/Risk-Assessment-Process-Information-Security.pdf>

“The focus on investment in technology has come at the cost of investment in people.”

KEEPING WATCH.

Preparing the organisation to detect and recover from a cyber security incident.

12



Why focus on readiness for a cyber security incident?

It is a matter of 'when' not 'if' an organisation will experience a cyber security incident. Readiness for an incident enables organisations to reduce the overall cyber security risk through prompt and effective recovery. The longer a breach or incident goes undetected, the greater the impact it will likely have. A 2018 report commissioned by IBM and undertaken by the Ponemon Institute found the average time taken by organisations to identify an intrusion was 197 days. The ability to detect an intrusion and to respond promptly is the difference between a minor and a major compromise.

The level of cyber security readiness in New Zealand

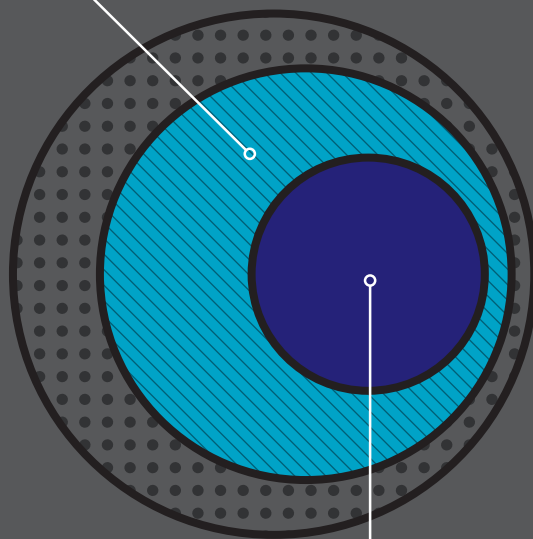
The first step in responding to any cyber incident is knowing it has occurred. In New Zealand, 41% of organisations are either mildly confident or not confident in their ability to detect an intrusion.

Without the ability to detect cyber threats, intrusions can go unnoticed for long periods and have a greater impact. The ability to detect cyber threats requires the right tools and the right people. Trained staff with a focus on security can help organisations evaluate risk, make informed decisions and plan ahead. When things go wrong, trained staff will help an organisation detect and recover from an incident. Only 38% of organisations reported having full time IT security staff, while 67% also include IT security functions as an add-on to an existing IT role.

The organisations surveyed:

63%

of organisations
have an incident
response plan.



33%

have not tested their
plan in the last year.

When an organisation becomes aware of an incident, being ready to respond can reduce the impact of a compromise. A key readiness factor is having a plan to allow an organisation to react quickly and decisively when an incident occurs – just 63% of organisations have an incident response plan. However, 33% have not tested their plan in the last year. An up-to-date incident response plan takes the guesswork out of determining appropriate actions, roles and responsibilities in the midst of a crisis. It also serves as a framework to preserve evidence in the event legal action is sought following an incident.

Suggested steps to increase maturity

- Acquire the tools or services that enable detection of incidents.
- Prepare a cyber security incident response plan and test it on a regular basis.

Useful resources

- <https://acsc.gov.au/publications/protect/essential-eight-explained.htm>
- <https://www.ncsc.govt.nz/assets/NCSC-Documents/New-Zealand-Security-Incident-Management-Guide-for-Computer-Security-Incident-Response-Teams-CSIRTs.pdf>
- <https://www.cert.govt.nz/it-specialists/critical-controls>

IN SAFE HANDS.

Maintaining oversight and awareness of the cyber security risks in your supply chain.

14



Why is supply chain security increasing in importance?

Outsourcing cyber security requirements to third-parties or managed services providers can be an effective way for a small organisation to overcome the challenges of IT investment. However, this does not transfer risk. Even if an organisation outsources IT or security functions, the board and executives must remain accountable for the performance of those functions.

Outsourcing IT, cyber security or other business functions can enhance security but it also reduces visibility of potential risks. Organisations need to be aware of the strength of each link in their IT or security supply chain. Organisations are also responsible for ensuring third party providers are delivering improvements to security at the outset and for the duration of a contract.

To understand cyber security risk, good information is critical. For those organisations reliant on their service provider for cyber security reporting, it is important that regular and clear reporting is part of the contract.

Supply chain security in New Zealand

For many organisations, the primary opportunity to influence the security levels of IT services provided by third parties is during contract negotiation. Out of those organisations that contract with managed service providers, 64% considered IT security as part of the vendor contracting process.

However, after the contract was signed, many organisations were unsure whether these clauses were adhered to by their providers. While 72% of organisations use some type of managed service provider, 36% of those have no mechanisms in place to confirm whether their vendor is delivering on the agreed level of IT security. As a result, 41% of organisations remain less than confident of their ability to detect an intrusion.

Suggested steps to increase maturity

- Include cyber security as a consideration when assessing new vendors.
- Include regular security reporting as part of the contract and, where possible, build specific security clauses into Service Level Agreements.
- Ensure you have the right to audit your vendor's performance periodically to validate the agreed level of security is being provided.

Useful resources

- <https://www.us-cert.gov/APTs-Targeting-IT-Service-Provider-Customers>
- <https://acsc.gov.au/publications/protect/questions-for-service-providers.htm>
- <https://www.baesystems.com/en/cybersecurity/blog/how-to-manage-your-supply-chain-cyber-risk>

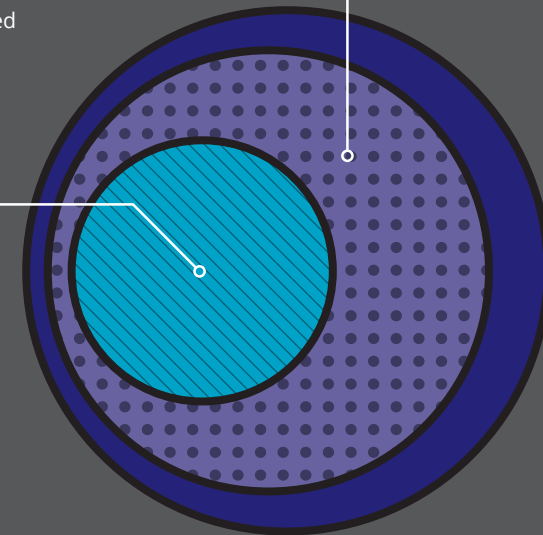
The organisations surveyed:

72%

of organisations use some type of managed service provider.

36%

of those have no mechanisms in place to confirm whether their vendor is delivering on the agreed level of IT security.



41% of organisations remain less than confident of their ability to detect an intrusion.

THINKING AHEAD. BEING PREPARED.

NEXT STEPS

The survey results have given the NCSC a unique insight on the cyber resilience of New Zealand's NSOs. We are committed to supporting them to improve their cyber security resilience.

Using the evidence gathered, the NCSC will:

- Provide individual and aggregated reporting to all the organisations that were surveyed.
- Use information provided to refine and tailor future NCSC products and services to better meet customer needs.
- Work with different industries and sectors to address key sector specific resilience issues.
- Develop information campaigns, based on the focus areas of this report, to continue to drive improvements in New Zealand's NSOs security practices.
- Conduct future surveys to observe and measure changes to the cyber resilience of NSOs.

If you wish to discuss the findings of this report please email the NCSC at info@ncsc.govt.nz



REFERENCE LIST

Focus area	Suggested steps to increase maturity	Useful Resources ¹
GOVERNANCE	<ul style="list-style-type: none"> Identify the person, or people, who are accountable for cyber security in your organisation. Ensure your organisation's leadership receives regular reporting on security issues from your IT team or service provider. Make cyber security reporting easier to consume. For example, report cyber security 'near misses' in the same way as you might report Health and Safety issues. 	<ul style="list-style-type: none"> https://www.iod.org.nz/Governance-Resources/Publications/Practice-guides/Cyber-Risk-Practice-Guide https://www.ncsc.govt.nz/assets/NCSC-Documents/cyber-security-risk-management-board.pdf
INVESTMENT	<ul style="list-style-type: none"> Balance strategic, longer term investments in the development of assets and staff over 'one off' costs for vulnerability assessment snapshots. Identify the information assets that are most critical to your business and assess the risks posed to these assets. Create a separate budget line to effectively manage and track IT security spending. 	<ul style="list-style-type: none"> https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697 https://www.ict.govt.nz/assets/ICT-System-Assurance/Risk-Assessment-Process-Information-Security.pdf
READINESS	<ul style="list-style-type: none"> Acquire the tools or services that enable detection of incidents. Prepare a cyber security incident response plan and test it on a regular basis. 	<ul style="list-style-type: none"> https://acsc.gov.au/publications/protect/essential-eight-explained.htm https://www.ncsc.govt.nz/assets/NCSC-Documents/New-Zealand-Security-Incident-Management-Guide-for-Computer-Security-Incident-Response-Teams-CSIRTs.pdf https://www.cert.govt.nz/it-specialists/critical-controls/
SUPPLY CHAIN	<ul style="list-style-type: none"> Include cyber security as a consideration when assessing new vendors. Include regular security reporting as part of the contract and, where possible, build specific security clauses into Service Level Agreements. Ensure you have the right to audit your vendor's performance periodically to validate the agreed level of security is being provided. 	<ul style="list-style-type: none"> https://www.us-cert.gov/APTs-Targeting-IT-Service-Provider-Customers https://acsc.gov.au/publications/protect/questions-for-service-providers.htm https://www.baesystems.com/en/cybersecurity/blog/how-to-manage-your-supply-chain-cyber-risk

¹ The links provided are merely an example of the information available. The inclusion of these links is not an endorsement of one vendor over another.



For futher information visit: www.ncsc.govt.nz
or email: info@ncsc.govt.nz