

6 April 2022

IR-01-21-37476

Scott

fyi-request-17124-35f67b4b@requests.fyi.org.nz

Dear Scott

Thank you for your Official Information Act 1982 (OIA) request of 20 December 2021, in which you asked for information regarding COVID-19 compliance:

This follows on from IR-01-21-30445

I would like to make a follow up request to Police for the following:

- 1) A copy of the AoG COVID-19 Compliance Operating Model (i.e. a copy of the entire document which you have extracted one page from for your initial response)*
- 2) Copies of all decision papers and other reports produced by the Operational Steering Group and submitted to the Governance Group, dated since the beginning of July*
- 3) The identity of every agency represented in the Operational Steering Group's membership*

On 10 February 2022, Police also accepted a transfer of your request originally submitted to the Ministry of Health. Those questions are:

- 1) The group's terms of reference*
- 2) The identity of every agency represented in the group's membership*
- 3) The minutes of all meetings held since the beginning of July*
- 4) All reports produced by the group, dated since the beginning of July*
- 5) The document titled "AoG COVID-19 Compliance Operating Model"*

This response will address both sets of questions due to duplication. Some questions have been previously responded to by Police in OIA response IR-01-21-30445 sent to you on 7 December 2021.

- 1. A copy of the AoG COVID-19 Compliance Operating Model (i.e. a copy of the entire document which you have extracted one page from for your initial response)*

Police National Headquarters

180 Molesworth Street. PO Box 3017, Wellington 6140, New Zealand.
Telephone: 04 474 9499. www.police.govt.nz

Please find attached a copy of the of the All of Government (AoG) COVID-19 Compliance Operating Model for your information.

2. *Copies of all decision papers and other reports produced by the Operational Steering Group and submitted to the Governance Group, dated since the beginning of July*

Attached are the following six documents produced and presented to the Governance Group since July 2021:

- Compliance Data and Insights ISR review – Governance group 1 September 2021
- Compliance Data and Insights End of Shift Report – 9 September 2021
- Compliance Data and Insights Governance Report – 16 September 2021
- Compliance Data and Insights Governance report – 23 September 2021
- Compliance Data and Insights COVID-19 response review – Governance Group 6 October 2021
- Compliance Data and Insights COVID-19 response review – Governance Group 14 October 2021
- AoG Compliance Governance Group memo – 25 November 2021
- High Level: Transition Timeline and Activities

Please note that some information has been withheld under section 9(2)(a) of the OIA, in order to protect the privacy of natural persons, including that of deceased natural persons.

3. *The identity of every agency represented in the Operational Steering Group's membership*

The following agencies represented at the Steering Group were:

- Ministry for Primary Industry
- Worksafe NZ
- Ministry of Health
- New Zealand Police
- Ministry of Business, Innovation and Employment

4. *The group's terms of reference*

This information was previously provided to you in Police's response to OIA request IR-01-21-30445.

5. *The minutes of all meetings held since the beginning of July*

As per OIA request IR-01-21-30445, this part of your request is refused under section 18(e) of the OIA as the information does not exist.

You have the right to ask the Ombudsman to review my decision if you are not satisfied with the response to your request. Information about how to make a complaint is available at: www.ombudsman.parliament.nz.

Yours sincerely

A handwritten signature in black ink, appearing to read 'R. Le Prou', is positioned to the left of a vertical line.

Superintendent Russell Le Prou
Controller: COVID Resilience
New Zealand Police



21 APRIL 2020

All of Government (AoG) COVID-19 Compliance Operating Model

OCC Update

v.012



Mission

Our mission:

“To achieve compliance to prevent the spread of COVID-19, while maintaining trust and confidence”

Principles:

Aligned on purpose

Preventative

Flexible and agile

Risk-based

Transparent and visible

Evidence-led

Proportionate and fair

Types of COVID-19 Non-Compliance

There are different types of non-compliance, and a range of underlying reasons for non-compliance to occur, both intentional and non-intentional. The compliance Operating Model considers these types of non-compliance, and directs appropriate interventions or redirects to appropriate support, based on situational context and risk.



Individuals

Any member of the New Zealand public.

Non-compliance example:

- Not complying with public health guidelines
- Non-essential travel
- Non-compliance with quarantine or managed isolation



Groups

Any mass gathering of people.

Non-compliance example:

- Parties
- Events



Organisations

Any private, public or not-for-profit organisation.

Non-compliance example:

- Non-essential businesses operating
- Not complying with public health guidelines



Locations

Any public or private location.

Non-compliance example:

- Areas with high occurrences of non-compliance (e.g. beaches)
- Regions with identified COVID-19 clusters

Drivers of non-compliance:

**Complacency | Misunderstanding | Social norm | Financial | Cultural | Risk-reward |
Social connection | Altruism | Unable to comply | Criminal intent | Legal challenge**

Graduated Response Model

1. Engage, Encourage, Educate

- Awareness is key to prevention and driven by strategic communications.
- Proactive engagement and community presence should be delivered across all regulating agencies through their BAU (or enhanced BAU) activities.
- Redirection to welfare or community/iwi support is utilised based on situational context and risk.
- All agencies with a regulatory function can play a role in educating and encouraging compliance when specific instances of non-compliance is identified, including:

- | | |
|------------------|-----------------|
| - Local Councils | - MBIE |
| - Worksafe | - MPI |
| - Maritime NZ | - Corrections |
| - Police | - MSD |
| - MoT | - DHBs / PHUs |
| - NZTA | - Civil Defence |

2. Warn

- Where there is evidence of education and repeated (or sufficiently serious) offences against COVID-19 control measures formal warnings (or notices to improve) are issued by those with legal powers to act.

See following slide for detail on powers to act.

Compliance starts with awareness...
...with many regulating Agencies having a role to play.

We will enable this by:

- Providing clear messages to the public regarding what to do to comply, and what to expect in instances of non-compliance.
- Ensuring Agencies understand their compliance role, and how they can interact with the AoG Compliance function.
- Ensuring strategic insights and recurring compliance issues are used to inform ongoing strategic communications

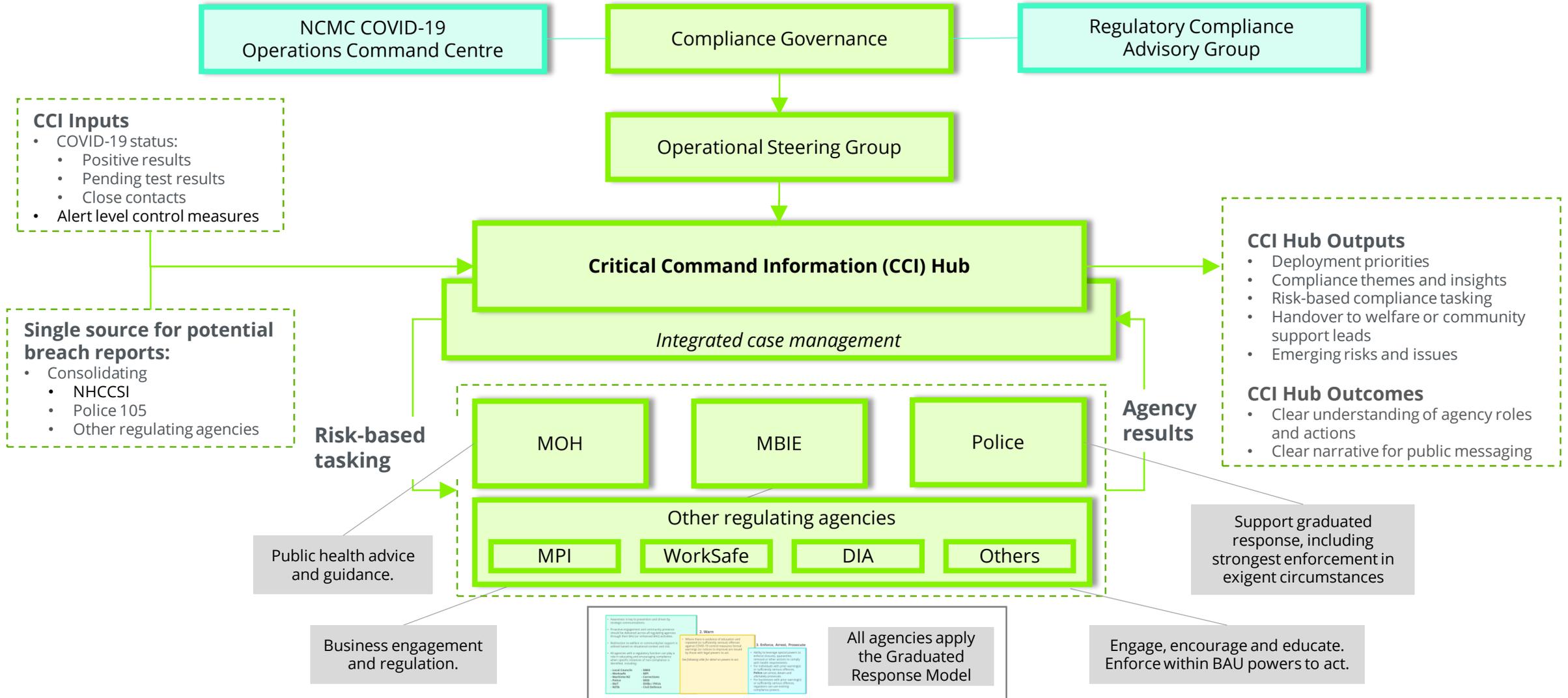
3. Enforce, Arrest, Prosecute

- Ability to leverage special powers to enforce closures, quarantine, removal or other actions to comply with health requirements.
- For individuals with prior warning(s) or sufficiently serious offences, Police can arrest, detain and ultimately prosecute.
- For businesses with prior warning(s) or sufficiently serious offences, regulators (e.g. Worksafe) can use existing compliance powers.

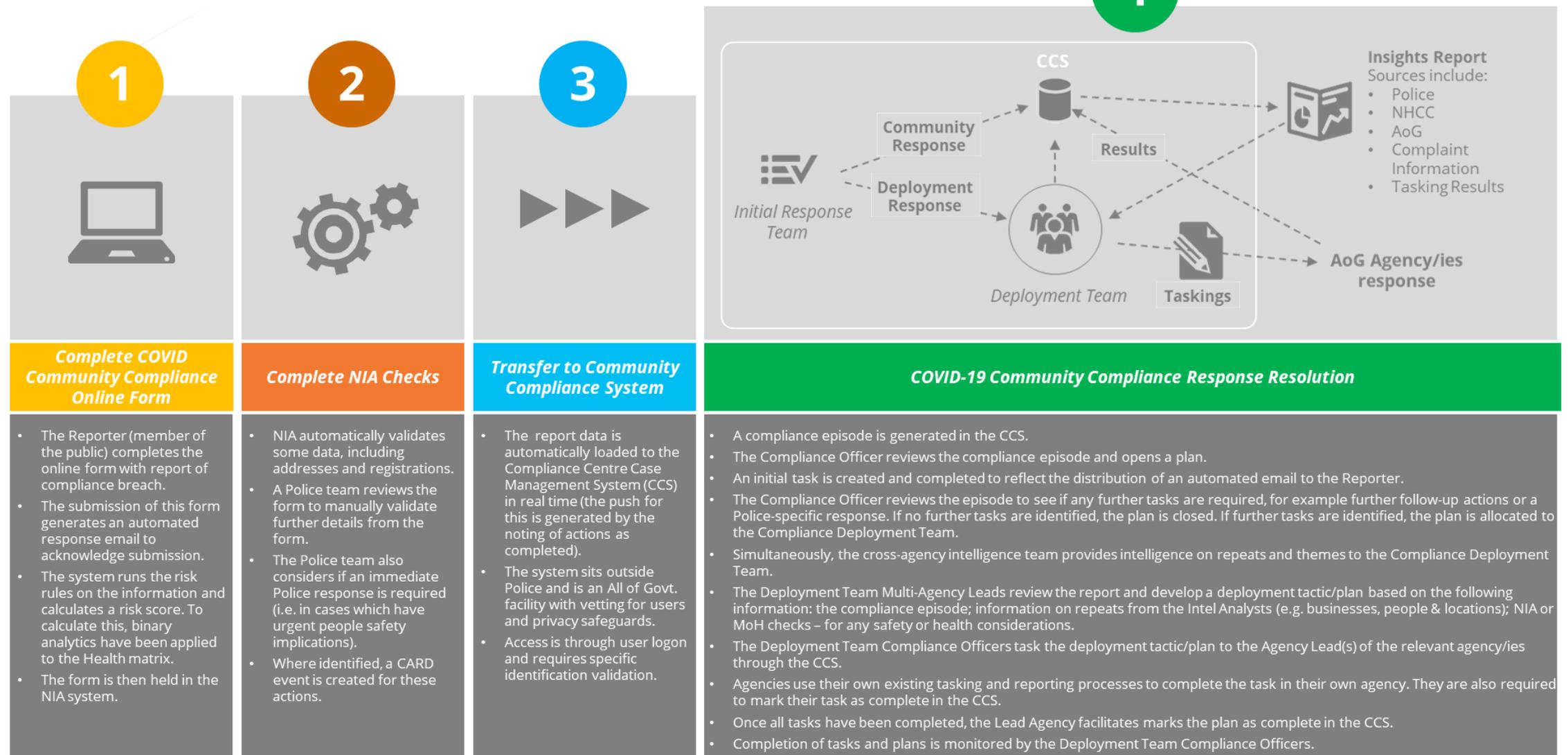
Where non-compliance is linked to a location (rather than an individual or location) additional compliance interventions may be deployed (e.g. signage at step 1; additional patrols at step 2; road blocks at step 3).

Compliance Operating Model

A Compliance Operating Model has been developed to support the consistent application of the Graduated Response Model.



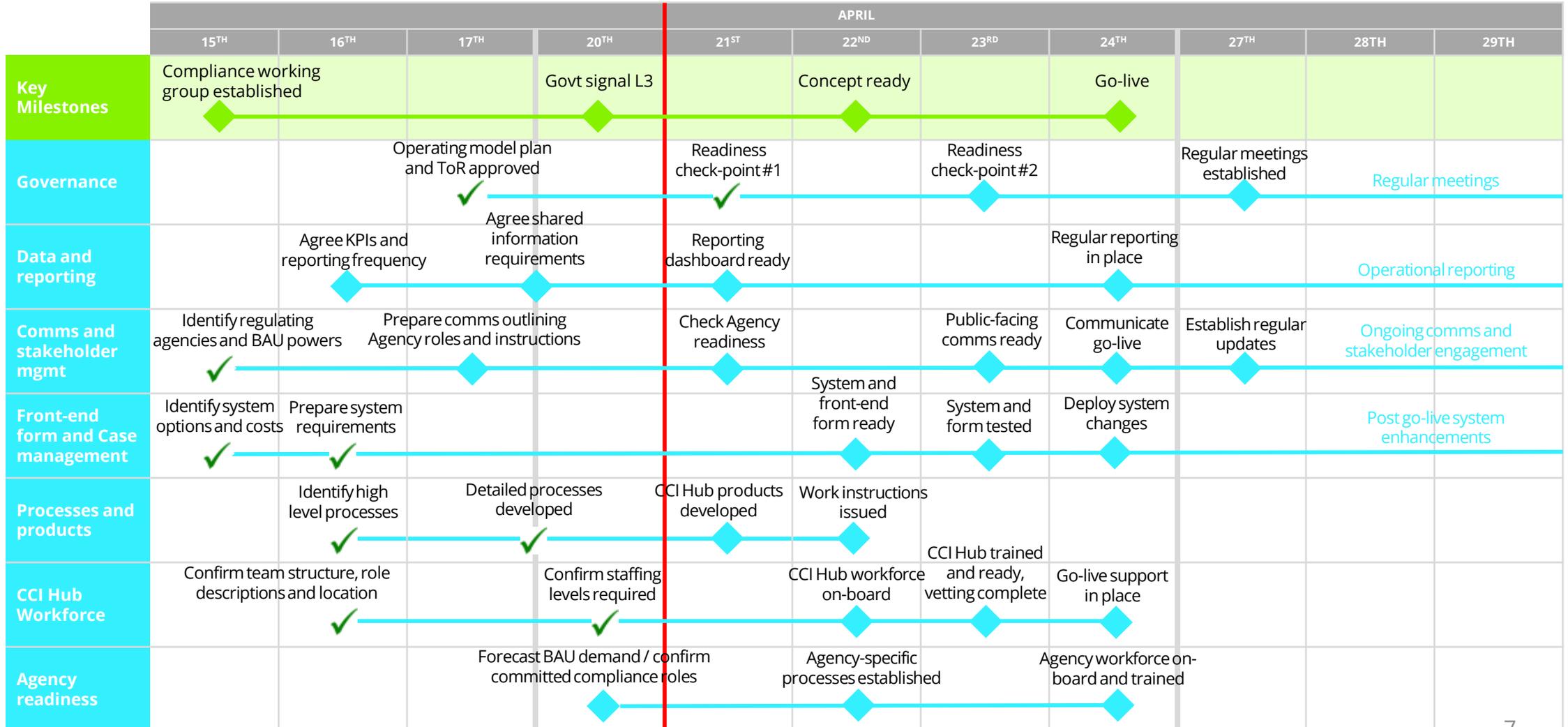
Breach Report Process



Status Update: Implementation Plan

A Compliance Operating Model will be established by Friday 24 April.

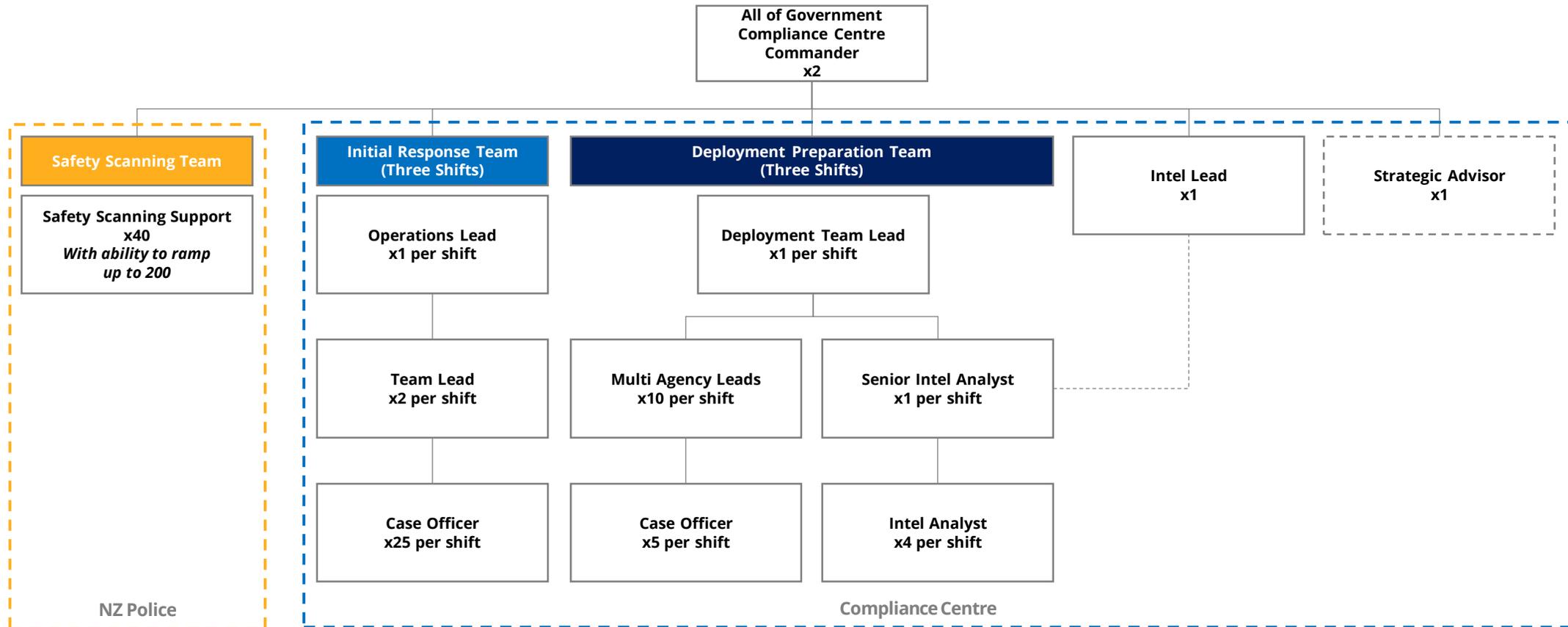
Key: ◆ Milestone ◆ Key Milestone ✓ Completed



Today

Compliance Centre Resource Requirements

Below is an overview of the resourcing requirements which have been identified to staff the Compliance Centre. **This comes to a total of 148 roles.**



Option A is our preferred option because it enables appropriate tasking and prioritisation based on risk.

Further options have been developed but are not being recommended at this stage:

- **Option B** was an outbound calling model, which would enable every task to be followed-up with the Reporter, but would require significant resources to support (246).
- **Option C** is a processing centre model with all actions of tasks undertaken by individual organisations (123 resources).

COVID-19 COMPLIANCE RESPONSE

Uruta Urupare

New Zealand Government

Unite
against
COVID-19

Purpose of this paper

1. The purpose of this paper is to seek endorsement from the All-of-Government (AoG) COVID Compliance Governance Group to have compliance returned to relevant agencies and be built into business as usual practices from the 3rd of December 2021

Background

2. New Zealand Police have been AoG COVID Compliance workstream lead since its inception in April of 2020. This workstream was designed to be a centralised compliance framework with New Zealand Police who as the lead agency are supported by the Ministry of Health, WorkSafe New Zealand, the Ministry for Primary Industries and the Ministry of Business Innovation and Employment.
3. The existing model has served its purpose very well and, with support from your agency, the workstream has successfully managed more than 45,000 complaints. To manage this workload the workstream has fluctuated in staffing levels over time, from a baseline of 10 to up to 150 staff from across the supporting agencies.
4. On the 11th November Deputy Commissioner Dunbier forwarded a letter to the Deputy Chief Executives of AoG Compliance Agencies. The letter articulated an approach to move from a Police led AoG Compliance approach, to transitioning compliance back to relevant agencies.
5. On the 22nd November, Prime Minister Ardern announced that all of New Zealand will transition from the Alert Level system to the COVID Protection Framework on the 3rd December.
6. The current reporting platform, risk matrix and case management practices are specific to Alert Level settings, therefore the current AoG compliance framework will not be fit for purpose under the COVID Protection Framework.

Proposal

7. ***As at 11:59pm on the 2nd December COVID compliance transitions to the relevant agencies for management. At this time the triage and entry point for COVID compliance complaints will be moved to the COVID-19 website. It will then be up to individual agencies to manage complaints and apply their own deployment thresholds as per individual agency risk mitigation practices.***

Transition plans

8. Police will lead the transition of the current reporting platform to the COVID-19 website working with the DPMC to achieve this.
9. Each agency will provide the preferred entry point details for complaints to be redirected from the COVID-19 website to their respective agencies. Refer to attached process map (appendix 1)
10. All agencies will need to contribute to the transition timeline and action plan (appendix 2)

Recommendations

It is recommended that the All-of-Government (AoG) COVID Compliance Governance Group:

- a) **Note** that the current AoG approach to COVID compliance has served its purpose well, however with the transition to the COVID-19 Protection Framework the current approach is no longer fit for the future and agencies must adapt to incorporating compliance into BAU by 11.59pm on the 2nd of December 2021. YES / NO
- b) **Endorse** the transition proposal and the associated transition plans is the preferred AoG COVID Compliance approach. YES / NO
- c) **Agree** that Police will lead the transition process with DPMC assistance to achieve transition outcomes. YES / NO

SIGNATORY DATED: 25TH November 2021

Graham Mclean
Head of Planning and System Readiness· Department of the Prime
Minister and Cabinet (Role) DMPC

Steve Watson
National Manager, Compliance and Investigations and Information and
Education, Tenancy Services, MBIE

Phil Knipe
Chief Legal Advisor at Ministry of Health

Simon Humphries
Head of Specialist Interventions WORKSAFE

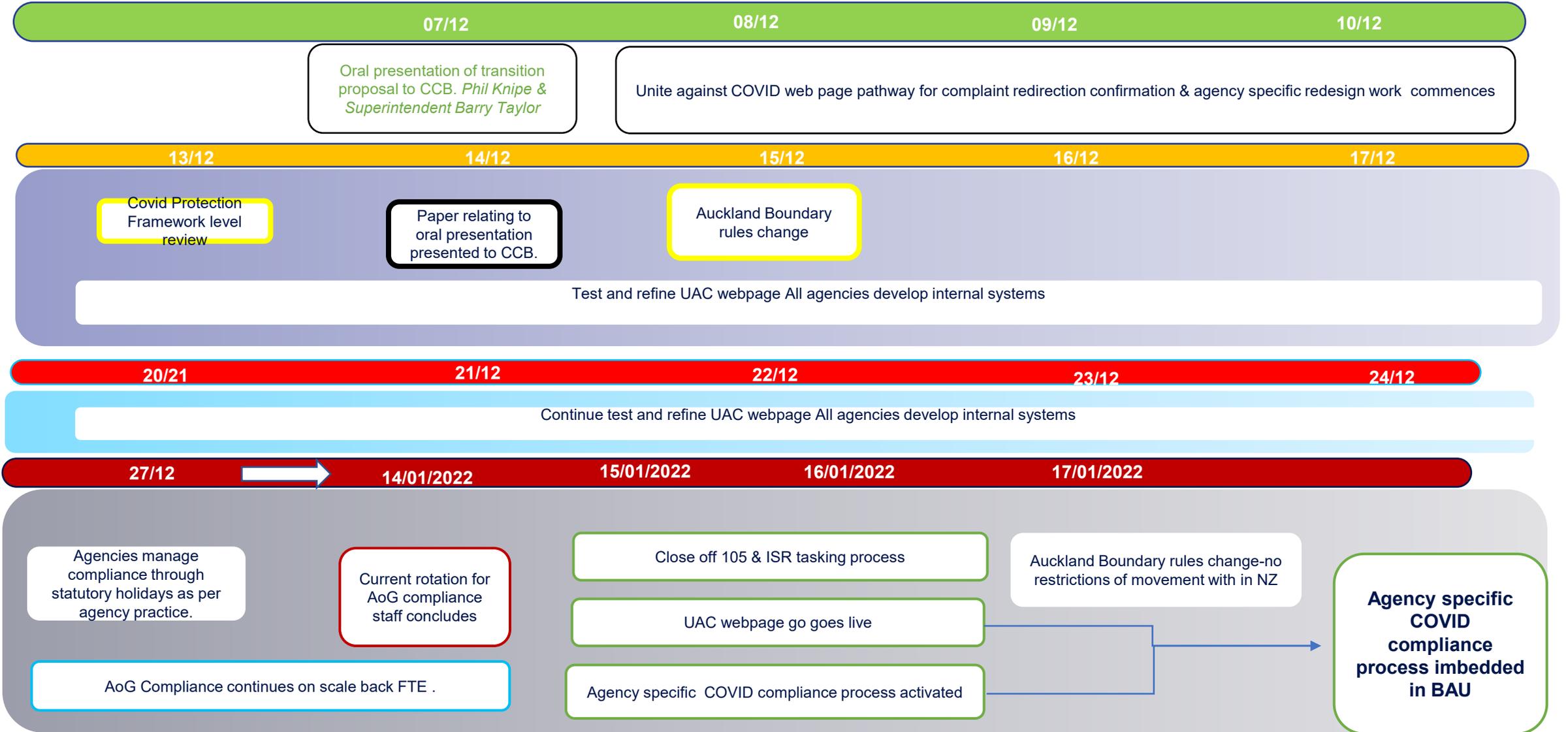
Gary Orr
Director of Compliance at Ministry for Primary Industries

Fiona Proudfoot
Group Manager New Zealand Customs Service

Barry Taylor
Director - Major Events New Zealand Police.

High Level: Transition Timeline and Activities:

The following timeline and activities is based on COVID Chief Executives Board (CCB) endorsement of transition from All-of-Government (AoG) COVID Compliance to BAU activities.



Compliance Data and Insights ISR review – Governance group 01/09/2021

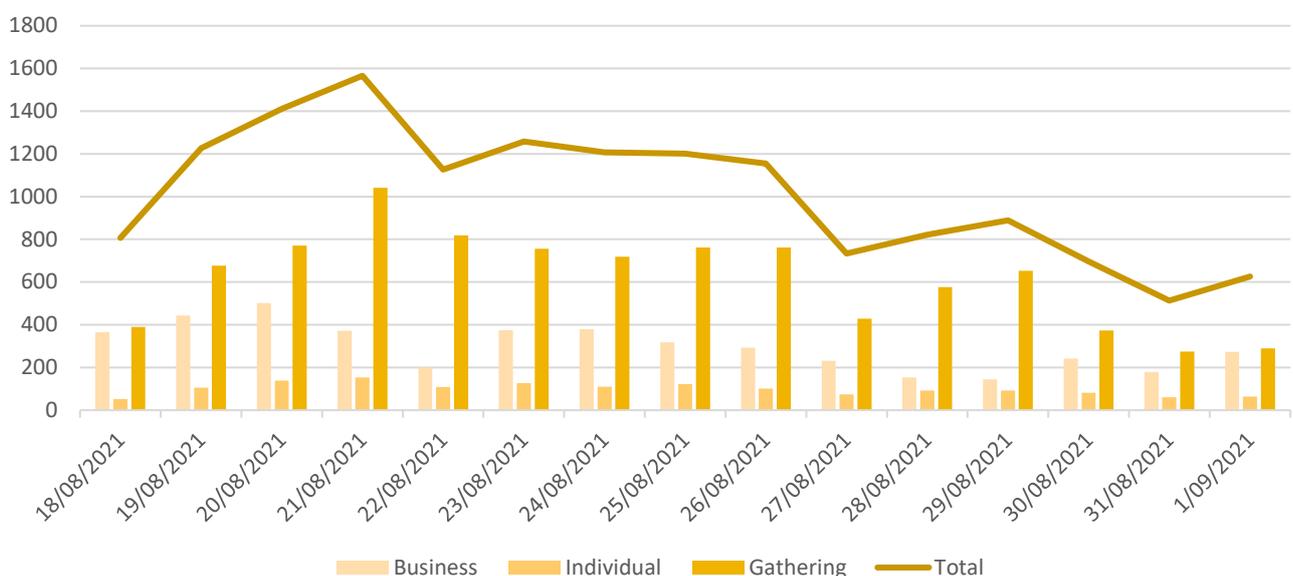
Unless otherwise stated, data relates to 00:00 to 18/08/2021 to 08:00 01/09/2021.

Episodes

Between the 00:00hs 18th of August and 23:59hs 1st September 2021, 15238 breach reports (henceforth 'episodes') were received in the Compliance ISR system, at an average rate of 1016 new reports per-day, although this has begun to decline over the past 5 days (Figure 1). A majority of episodes relate to Gathering breaches (61%), followed by Businesses breaches (29%) and then Individual breaches (10%).

Gathering breach reports saw a steady increase between 18/08 and 21/08, potentially due to a combination of good weather and the apparent containment of the outbreak to Auckland (as of 20/08 31 cases, all within the Tāmaki Makaurau region, were reported). Following the announcement of cases outside of Tāmaki Makaurau on 21/08 and the continued increase in case numbers, close contacts and locations of interest, it is possible that the potential scope and long-term impact of the outbreak was taken more seriously, resulting in more compliant (gathering) behaviour. The number of reports relating to gathering breaches was relatively steady until 27/08, at which point it has begun to decline. This decline can also be seen with business and gathering breaches. This may be influenced by a number of factors including increased compliance, apparent 'inaction', ambivalence to breaching and the upcoming Alert Level change outside Tāmaki Makaurau/ Northland.

Figure 1. Count of new breach reports each day



Plans

Episodes requiring review for action or part of a repeat breaching pattern for an individual, business or location are given plans¹. As of 08:00hrs 01/09/2021, 35% of have resulted in plans. High-risk episodes are most likely to result in a plan; 46% of high-risk episodes have a plan compared to 16% of low risk and 27% of medium risk episodes that have generated plans. Of all plans created, 63% are currently high-risk, 32% are medium risk episodes and the remaining 5% are low-risk.

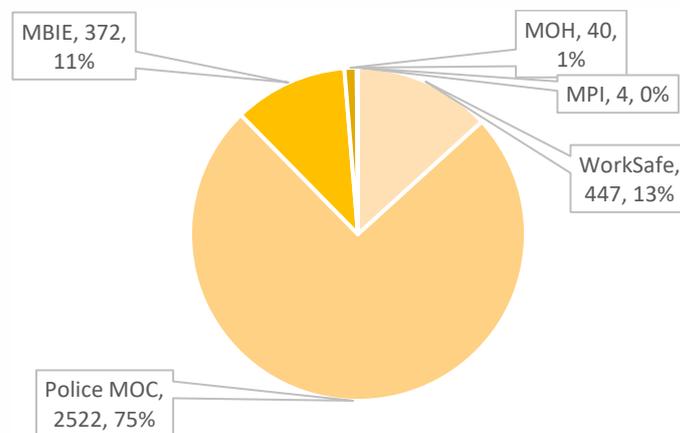
Tasks

Plans requiring attention and action by an agency are given tasks². As of 08:00hrs 01/09/2021, 67% of plans have tasks. Of all tasks created, 41% are currently high-risk, 53% are medium risk episodes and the remaining 5% are low-risk.

Task agency

Police have been tasked with most tasks (75%; Figure 2), followed by WorkSafe and MBIE who have received a similar proportion of tasks (11% and 13% respectively). This appears in part to be due to the high proportion reports relating to Gatherings, but observational analysis suggests that Police are also being tasked when other agencies do not attend breaches relating to business (statistics not available).

Figure 2. Frequency and proportion of tasks assigned to each agency



Status by task agency

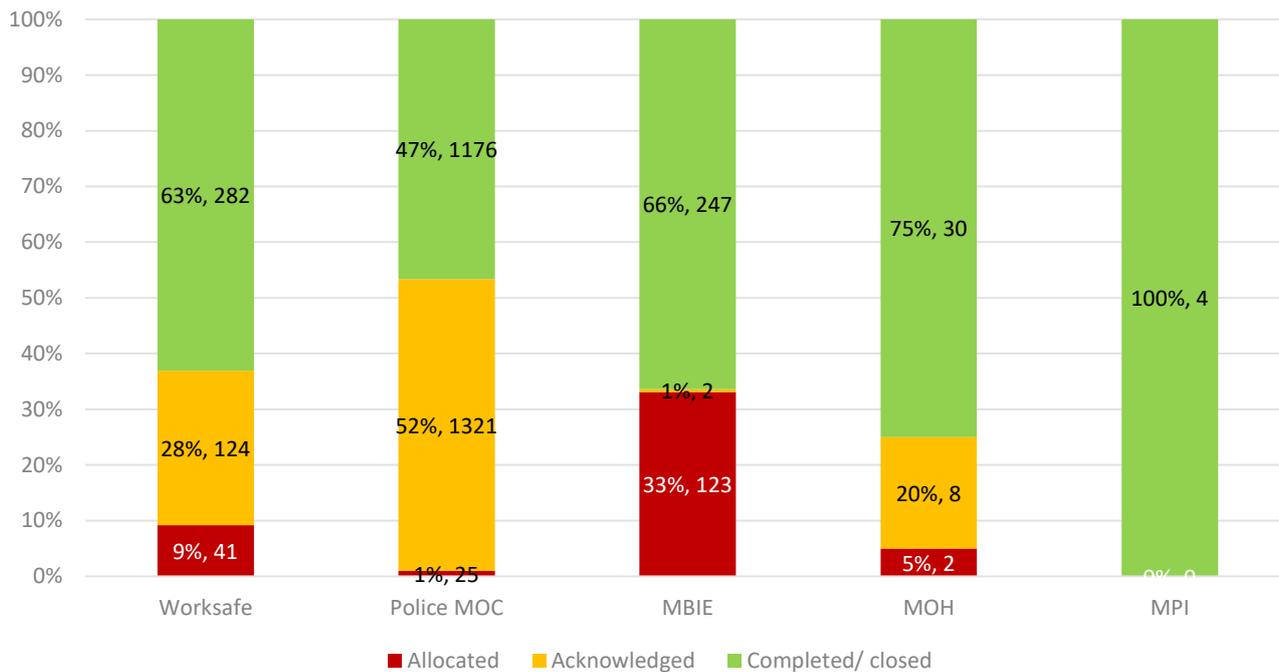
Considering the three agencies that have been tasked with virtually all compliance action, MBIE have the highest completion rate (66%), followed by WorkSafe (63%). It is worth noting that tasks assigned

¹ Multiple episodes relating to the same individual, business or location should be consolidated into a single plan.

² There may be multiple tasks for each plan.

to Police may already have been completed but not updated in the system³, and therefore the completion rate of Police is likely much higher than 47%. MPI only have 4 tasks and have completed all of these while MOH have received 30 tasks and have completed 75%. Allocated tasks – tasks that have been assigned to an agency but not formally read/ confirmed (acknowledged) by that agency – are highest for MBIE (33%) followed by WorkSafe (9%).

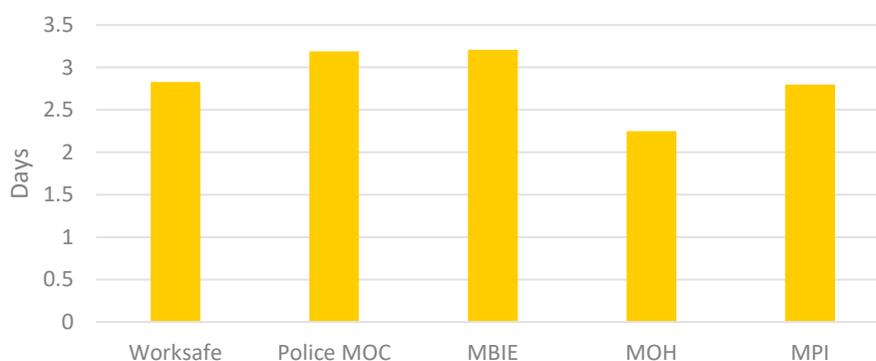
Figure 3. The frequency and proportion of tasks assigned to each Agency by Status.



Time taken to complete tasks by task agency

On average, tasks take a little under 3 days to complete, with some agencies running slightly higher. Again, it is important to note that due to the method of entering Police tasks into the ISR system, the delay between a task being sent out.

Figure 4. Days to complete tasks after being allocated.

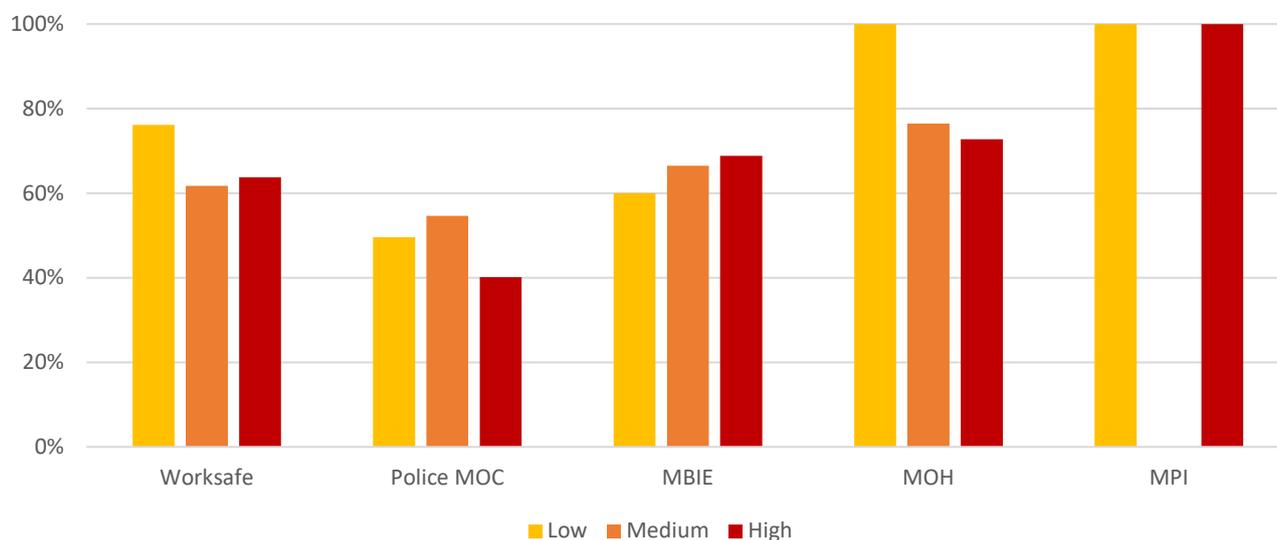


³ A large amount of Police tasks are entered into the Police system CARD and then manually transferred into ISR. This means that Police tasks may have already occurred before being officially created or noted as acknowledged/ completed.

Status by Risk by Agency

The proportion of tasks at each risk level that have been completed/ closed for each agency are displayed in Figure 5. Again, MPI has so few taskings that these should not be considered in comparison to other agencies. MOH, which also has very few taskings, has completed a higher proportion of low risk tasks compared to medium or high risk tasks. WorkSafe and MBIE, which have comparable task numbers, have closed a similar proportion of medium and high risk tasks, although WorkSafe does appear to have closed more low risk tasks than medium or high risk tasks. Police appear to have closed a smaller proportion of high risk tasks compared to low or medium risk tasks, however again the method of entering and completing Police tasks into the ISR system should be considered here.

Figure 5. Proportion of tasks that are complete/ closed at each Risk level by Agency



Repeat breaching

It was possible to determine repeat breaching following tasking for all plans/ tasks, however sampling analysis was completed with a portion of plans with tasks assigned to each agency⁴.

Overall, the most common action taking was to Educate (37; 30%) followed by sending a standard email in relation to the order (36; 19%); the latter action was typically completed by MBIE. It was also noted in the present sample the 7 WorkSafe tasks (14%) and 9 MBIE tasks (19%) were completed after the due date⁵.

Excluding MPI (the few tasks assigned cause drastic skew in data), 35 (20%) plans had multiple episodes with 9 of these having further episodes following the initial tasking (23%).

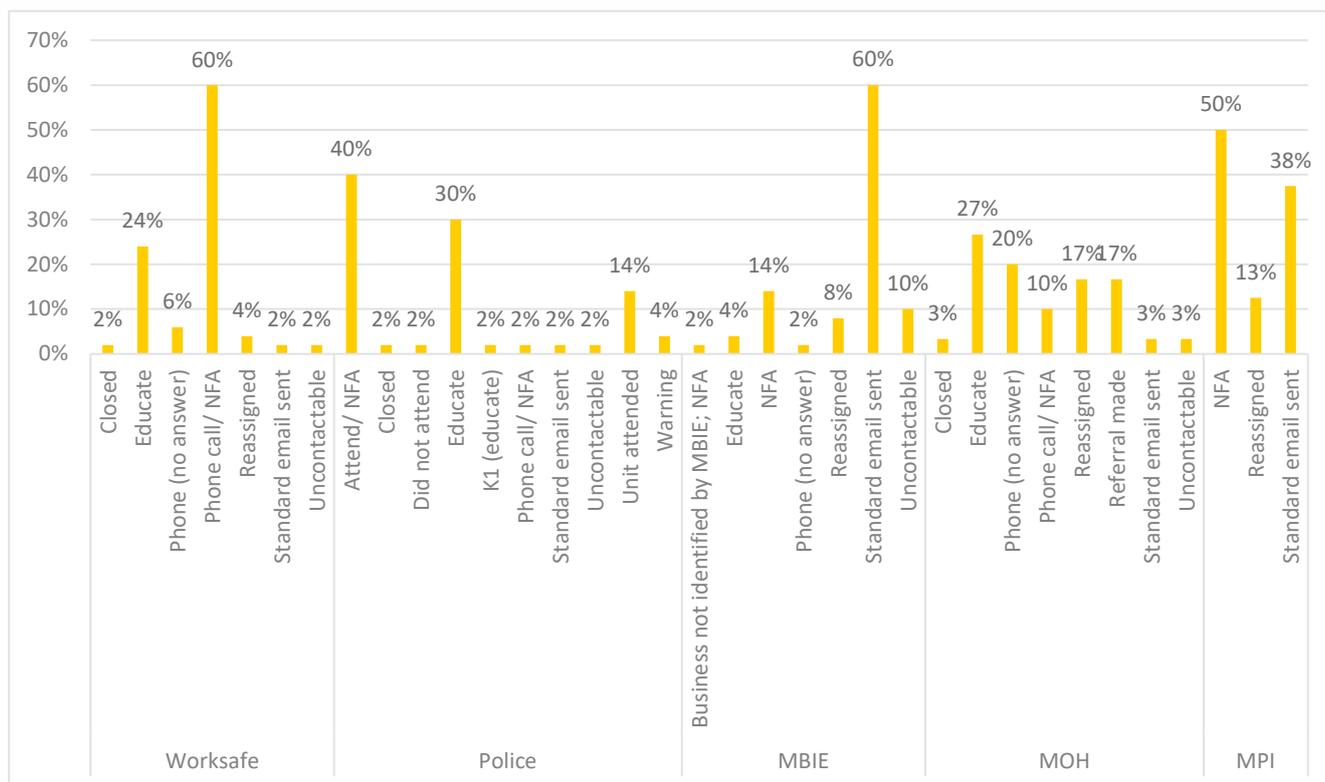
By agency, the most likely action in a task was:

⁴ WorkSafe = 50, Police = 50, MBIE = 50, MOH = 30, MPI = 4

⁵ Tasks are typically due 48 hours after being allocated.

- WorkSafe = Phone call/ NFA (60%); contact was made and established that no breach occurred
 - Educate = 24%
- Police = Attend/ NFA (40%); attended and established that no breach occurred
 - Educate = 30%
- MBIE = Standard email sent⁶ (60%); email sent, no response or follow up specified
 - Educate = 4%
- MOH = Educate (27%)
- MPI = NFA (50%); determined no breach occurred from narrative of job

Figure 6. Proportion actions from tasks according to agency



⁶ See Appendix 1

Appendix 1. MBIE Standard email

[You will need to search for the business online. Some businesses only have a phone number so you need to ring them to get an email address:]

Suggested script:

*Hello, this is [first name **only**] from the Ministry of Business, Innovation and Employment. Am I speaking to the business owner?*

When speaking to the business owner:

I'm just calling to check in with you on [your business's] operations under Alert Level 4. We received information that suggests that your business was open in Alert Level 4, I wanted to send you information from our website to help you make decisions on whether your business can operate. Do you have an email address I can send this to?

Once you have the email address:

Thank you, we'll be in touch with some guidance for you.

[Note if they don't want to provide an email, just say – OK, thanks anyway.]

Do NOT give advice over the phone over whether they are an AL4 essential business. Say Sorry I can't give advice over the phone. I can send you information from our website to help you make a decision over whether your business can operate.]

Production

	<i>Author:</i>	<i>Reviewed and released by:</i>
<i>Name</i>	s.9(2)(a) OIA (Police)	s.9(2)(a) OIA (Police)
<i>Role</i>	Data and Insights Lead	Compliance Response Commander
<i>Phone</i>	s.9(2)(a) OIA	

Handling Instructions

All IN CONFIDENCE information (including data) should clearly identify the originating government agency and date.

Method	Rules
Electronic transmission	<p>IN CONFIDENCE data can be transmitted across external or public networks but the level of information contained should be assessed before using clear text.</p> <p>Username/Password access control and/or encryption may be advisable (with the aim of maintaining public confidence in public agencies).</p>
Manual transmission	<p>May be carried by ordinary postal service or commercial courier firm as well as mail delivery staff in a single closed envelope.</p> <p>The envelope must clearly show a return address in case delivery is unsuccessful. In some cases involving privacy concerns, identifying the originating department may be inappropriate and a return PO Box alone should be used.</p>
Storage and disposal	<p>IN CONFIDENCE information can be secured using the normal building security and door-swipe card systems that aim simply to keep the public out of administrative areas of government departments.</p> <p>Must be disposed of by departmental arrangements.</p>

Compliance Data and Insights End of Shift Report – 9 September 2021

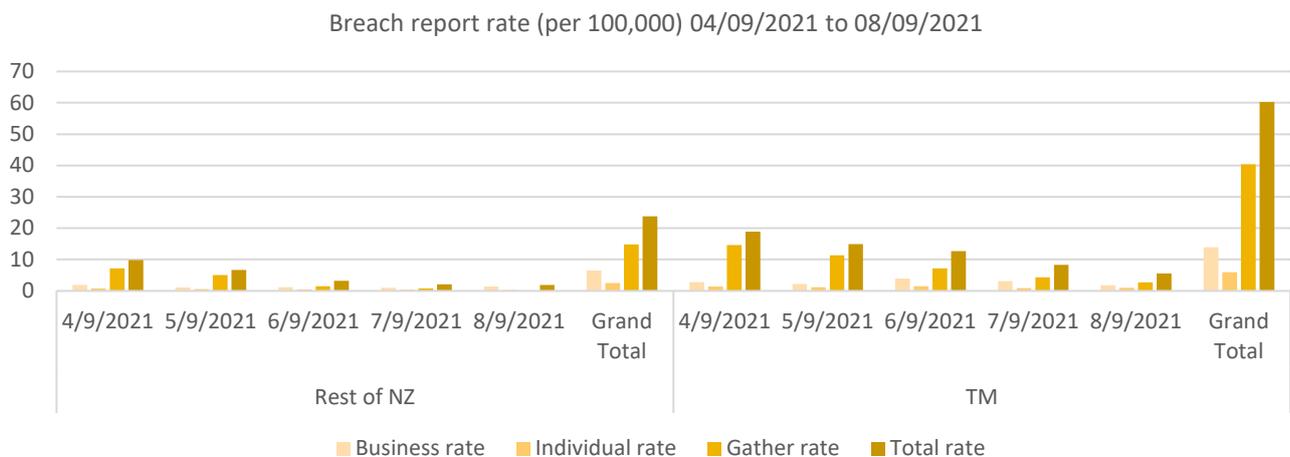
ISR

Unless otherwise stated, data relates to 00:00 18/08/2021 to 08:00 09/09/2021.

Episodes and plans

To date there have been 18,611 breach reports recorded in ISR; 18% of these have been high-risk, 41% medium risk and 12% low risk. A total of 8455 plans have been created. Currently¹, 53% are high-risk, 40% medium risk and 7% low risk.

The number of reports received has continued to decline, with 172 reports were recorded in the last 24 hours, down 24% from the previous 24-hour period.



Considering Tāmaki Makaurau and the Rest of NZ separately, both continue to show a decline in the number of reports. Over the last 5 days there have been 1077 reports from Tāmaki Makaurau and 864 from the rest of NZ, however the report rate (per 100,000) is much higher in Tāmaki Makaurau (60.27) than the rest of NZ (23.77).

Considering the past 24-hours alone:

- 59% of breach reports relate to Tāmaki Makaurau with gathering breaches accounting for a majority (49%) of reports.
- Throughout the rest of NZ, breach by businesses accounted for a majority (72%) of reports. Interestingly, the predicted increase in report numbers, particularly those relating to breach by businesses did not occur. There are multiple potential explanations:

¹ Plan risk level can be escalated if additional reports (episodes) are received and added to the plan.

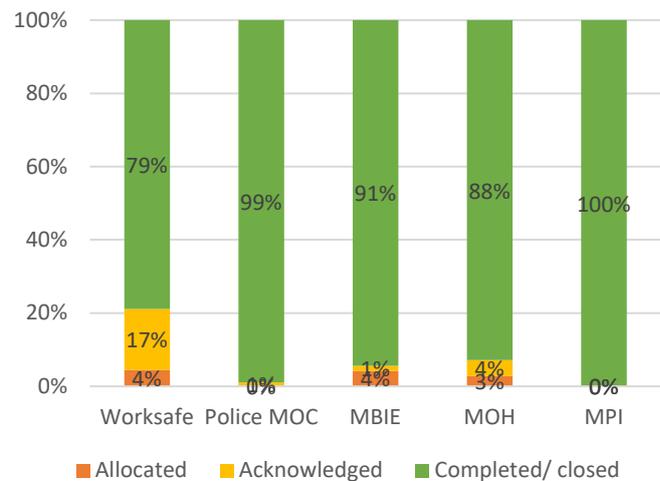
- a) Good compliance with the new L2 order requirements
- b) Low reporting of breaches due to apathy or confusion as to what constitutes a breach
- c) Poor weather across the country in combination with a lot of people continuing to work from home may mean that a lot of people were not about to witness/report breaches.

Tasks

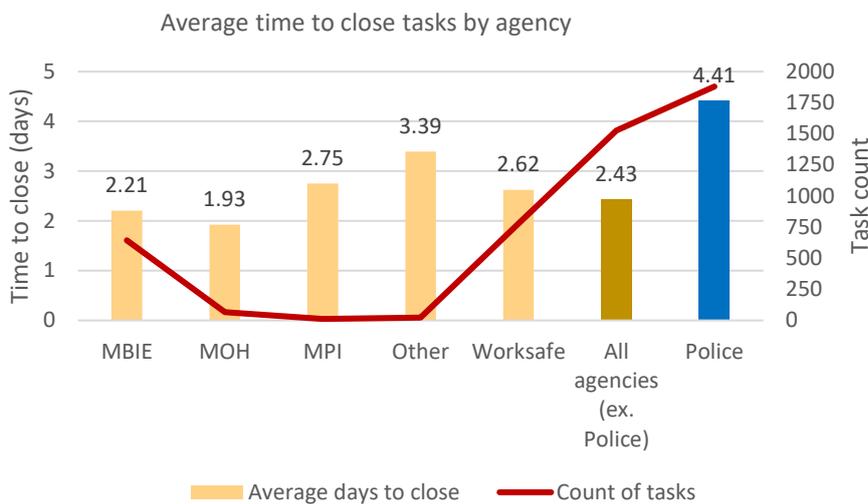
Overall, 94% of tasks have now been completed/ closed (up 4-points from yesterday), with a further 4% currently tasked out to agency awaiting action/ confirmation of action. High risk tasks have the highest completion rate (97%) followed by medium risk tasks (92%) and then low risk tasks (90%).

Most agencies are progressing well with closing tasks, Worksafe had the highest proportion (17%) of tasks that have been acknowledged but either no actioned or action has not been reported back to Compliance, however this is down (i.e. improved) 5-points from the previous day.

% of tasks at each stage at each agency 18/08/21 & 09/09/21



Time to close tasks



The time taken to close tasks since the 18th of August has, on average², been a little under 2 ½ days.

MOH have the fastest closure rate, however, as can be seen in the figure, the number of tasks assigned to this agency was much lower than others like MBIE, Worksafe and Police.

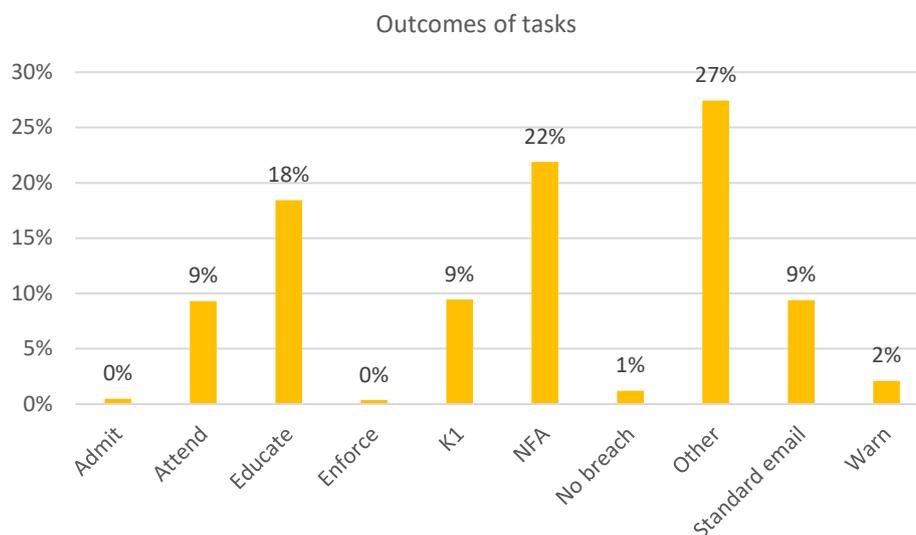
Appendix A. shows that as the number of tasks assigned to agency increases, so too does the time to close tasks (MBIE, Worksafe and Police investigated only).

² Excluding data relating to tasks assigned to Police. These were analysed separately because the completion/closed dates of tasks is often several days after the action was actually taken and reported, thereby making the delay in closing tasks appear greater than in actuality.

Outcomes of tasks

Task outcomes have been identified using a keyword search on the outcome comment³. This keyword search identified specific outcomes for 73% of all tasks; for the remainder ('Other') the outcome could not be identified⁴.

The outcome of a majority (27%) of tasks could not be determined and a further 22% were NFA.



Considering the Graduated Response Model, 18% were educated and 2% were warned. Only a negligible proportion were Enforced (including infringements).

Appendix B. Provides a full breakdown of outcomes for each agency. For each agency, the highlights are as follows:

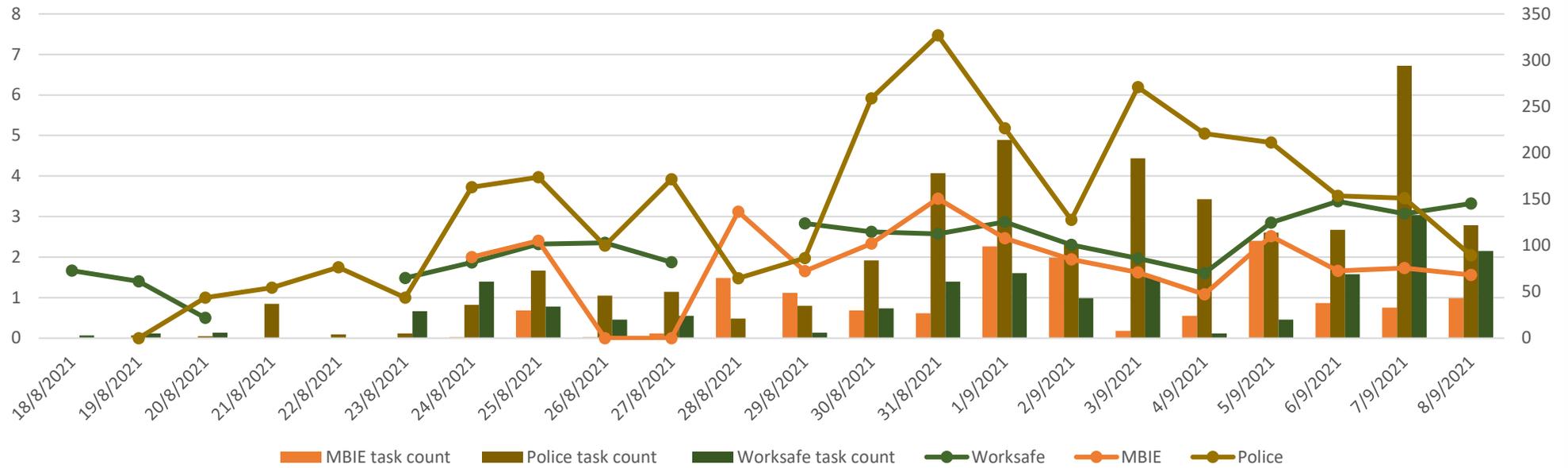
- MOH: outcome could not be determined for 82% of tasks
 - 13% were NFA and 5% were education.
- MPI: outcome could not be determined for 50% of tasks
 - 20% were NFA and 10% were attended with no further details on outcome specified.
- MBIE: a standard email was sent in 49% of tasks with no further information on outcome specified
 - 26% of outcomes could not be determined, 14% were educate and 10% were NFA
- Worksafe: 64% were NFA
 - 27% were educate and 8% of outcomes could not be determined
- Police: 34.15% of outcomes could not be determined
 - 17% were educate, 17% were attended and 17% were 'K1' (potentially attended but cannot confirm)
 - 3% were warned

³ Note: given that this was completed using a keyword search, there is a margin for error in the outcome identified and agency identified as actioning the task.

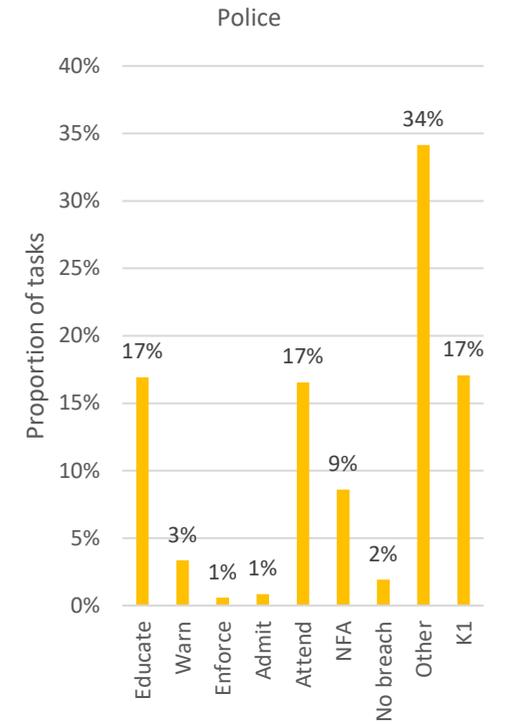
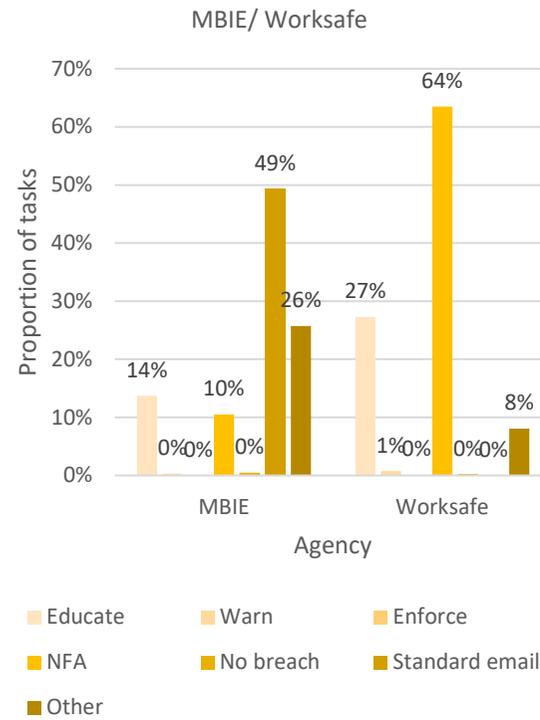
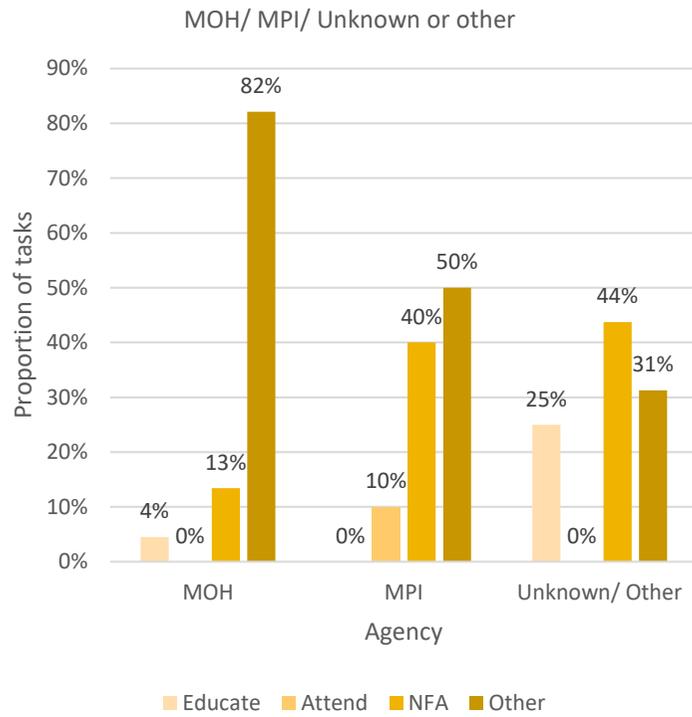
⁴ Educate, Warn and Enforce (inc. infringement) are GRM steps. If the GRM step cannot be identified: admit reflects where the accused breacher has admitted the breach, attend reflects when someone has attended, NFA reflects no further action (reason unclear), No breach reflects no breach occurred, Standard email reflects the outcome is noted as standard email sent with no further detail, K1 reflects NFA from Police but it is unclear if Police attended and other reflects all other outcomes.

Appendix A. Average time to close tasks mapped onto the number of tasks assigned to each agency.

Average time to close tasks mapped onto the number of tasks assigned to each agency



Appendix B. Outcome of closed tasks by Agency.



Production

	<i>Author:</i>	<i>Reviewed and released by:</i>
<i>Name</i>	s.9(2)(a) OIA	
<i>Role</i>	Data and Insights Lead, COVID-19 Compliance Response	
<i>Phone</i>	/	

Handling Instructions

All IN CONFIDENCE information (including data) should clearly identify the originating government agency and date.

Method	Rules
Electronic transmission	<p>IN CONFIDENCE data can be transmitted across external or public networks but the level of information contained should be assessed before using clear text.</p> <p>Username/Password access control and/or encryption may be advisable (with the aim of maintaining public confidence in public agencies).</p>
Manual transmission	<p>May be carried by ordinary postal service or commercial courier firm as well as mail delivery staff in a single closed envelope.</p> <p>The envelope must clearly show a return address in case delivery is unsuccessful. In some cases involving privacy concerns, identifying the originating department may be inappropriate and a return PO Box alone should be used.</p>
Storage and disposal	<p>IN CONFIDENCE information can be secured using the normal building security and door-swipe card systems that aim simply to keep the public out of administrative areas of government departments.</p> <p>Must be disposed of by departmental arrangements.</p>

Compliance Data and Insights

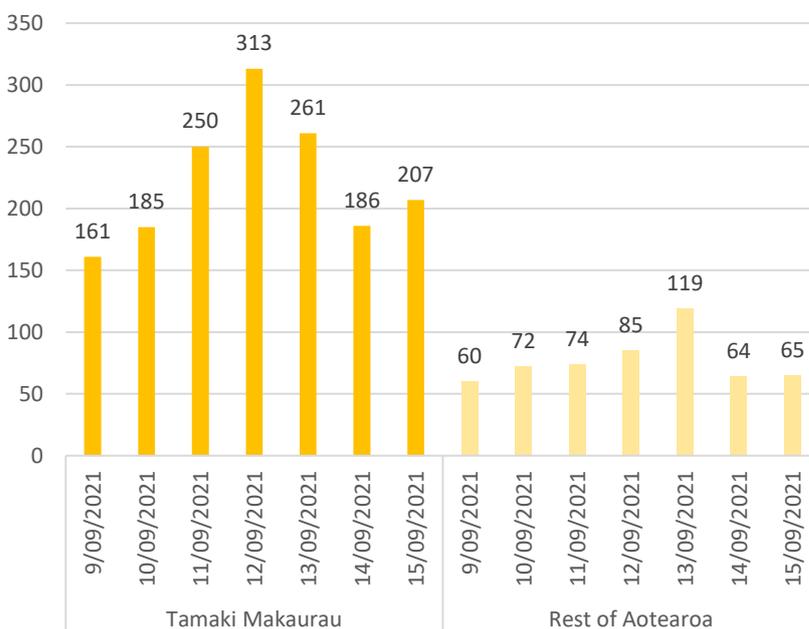
Governance Report – 16 September 2021

Unless otherwise stated, data relates to 00:00 18/08/2021 to 07:30 16/09/2021.

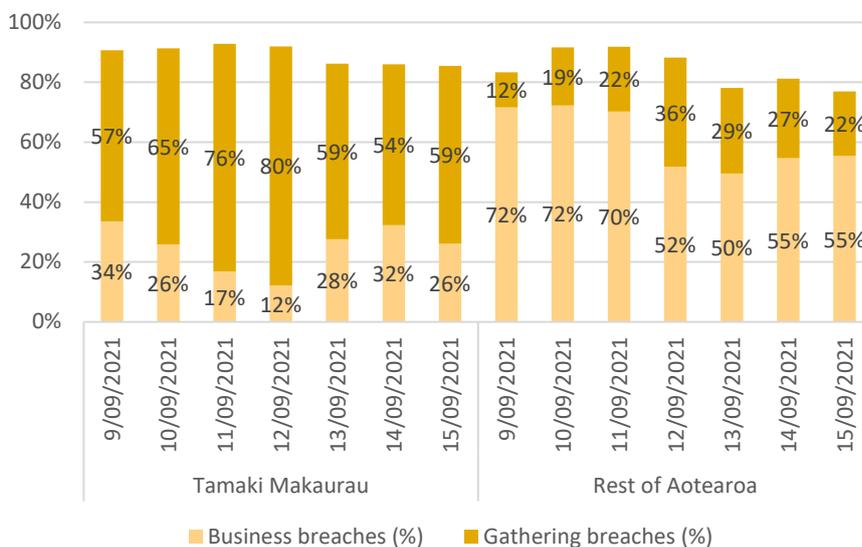
Episodes

Since the 18th of August 2021, 20,708 breach reports have been received (business = 6090, individual = 2076, gathering = 12542). On Wednesday 15th September there were 272 new breach reports, an 8% increase on Tuesday but still somewhat lower than Saturday through Monday. The increase in reports across Tuesday to Wednesday was primarily driven by additional reporting in Tāmaki Makaurau.

The proportion of reports originating from Tāmaki Makaurau has been relatively stable over the past 7 days (average = 74%) but peaked yesterday at 76% (range = 69% - 76%).

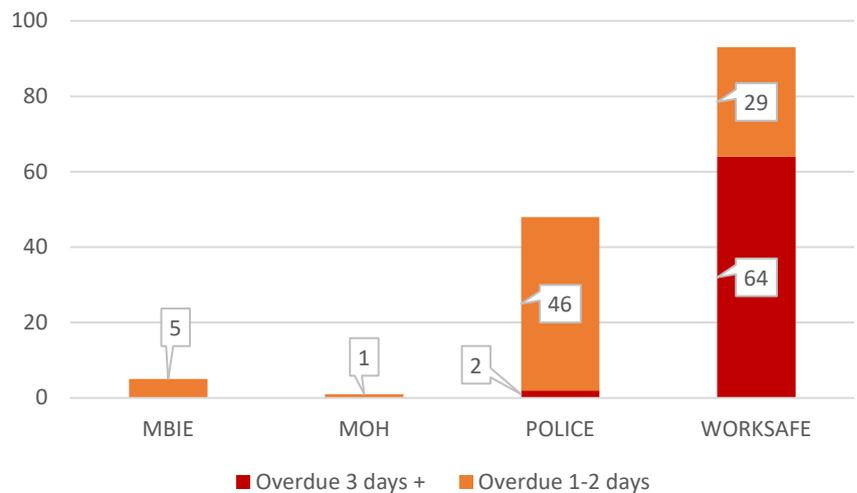


The proportion of reports in Tāmaki Makaurau relating to gatherings is on average 64%, although there has been some fluctuation (range = 54% to 80%). The proportion of reports relating to business breaches is on average 61% across the rest of Aotearoa; the rate of business breaches has decreased and maintained at a lower rate (average = 53%) since Sunday, with more breach by individuals in this period.



Tasks

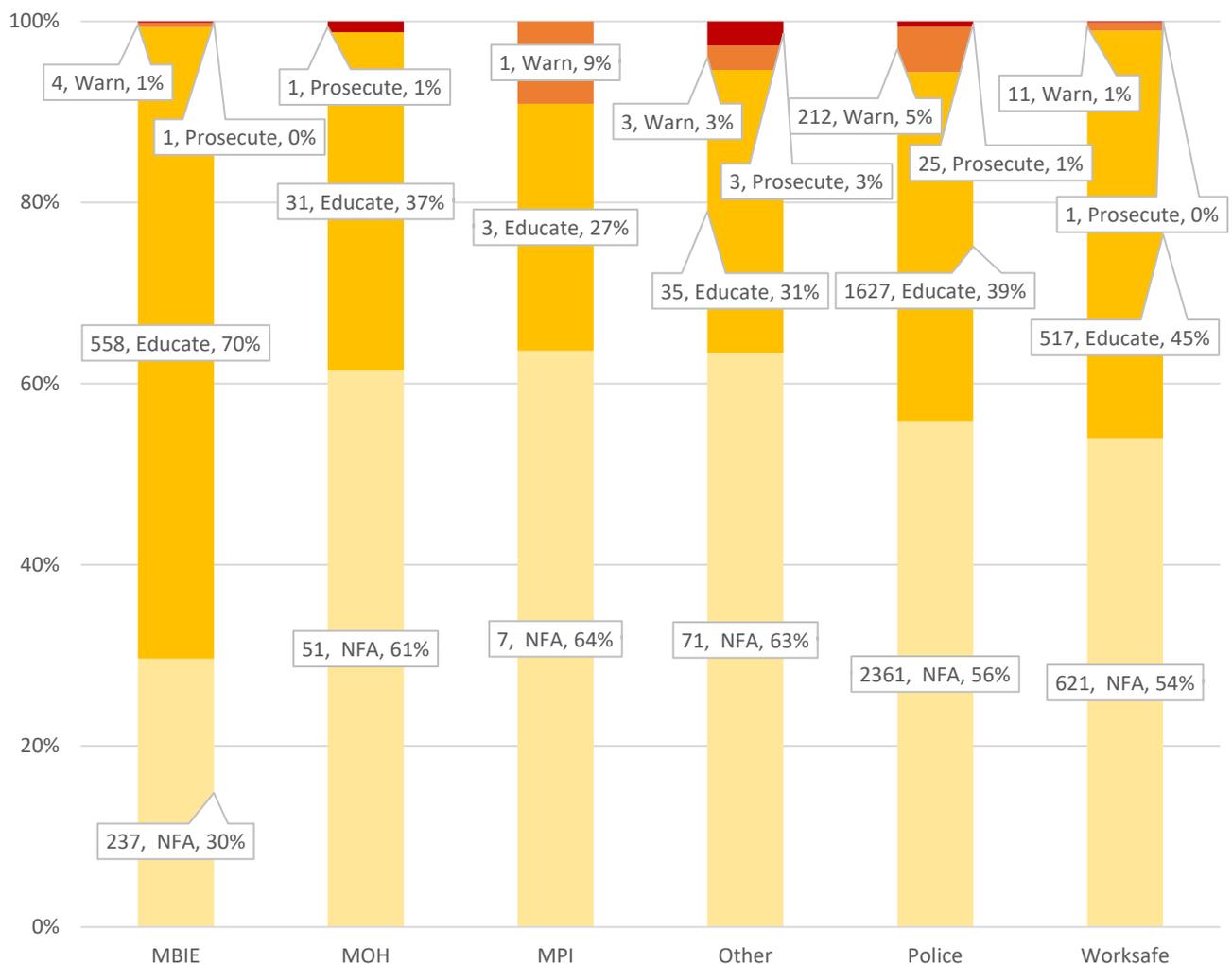
To date, 95% of tasks have been closed. There are currently 147 overdue tasks, 63% (93) are currently assigned to Worksafe and 33% (48) are assigned to Police. **Of all overdue tasks 45% (66) of which are 3 or more days overdue, 97% (64) of these are assigned to worksafe.**



Outcome of completed plans

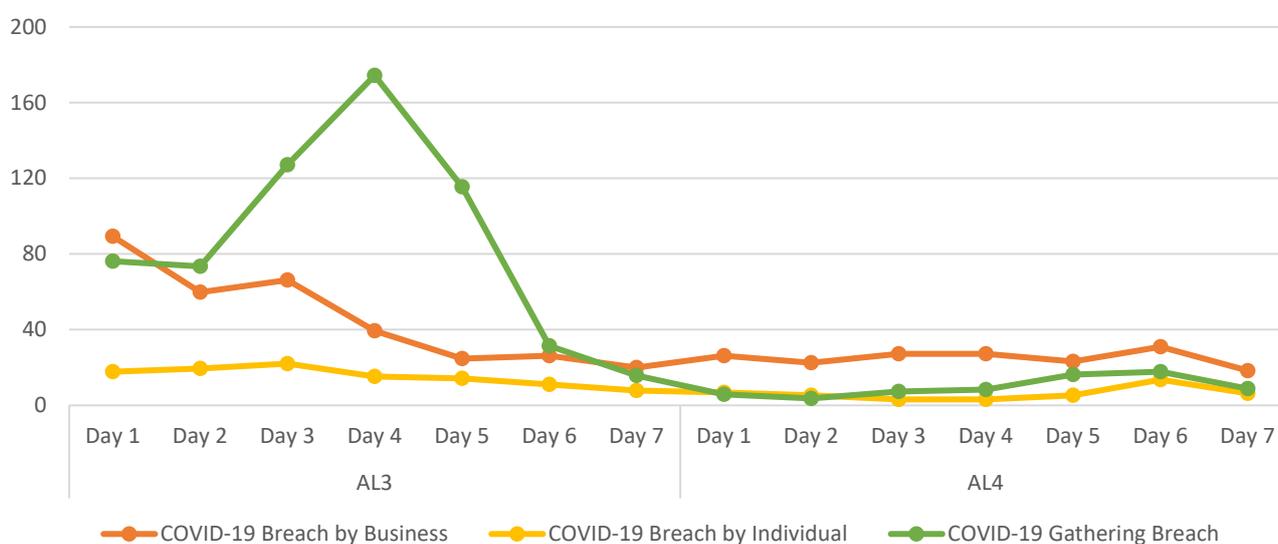
For plans with (all) tasks completed, 52% (3348) have been closed NFA, 43% (2771) have been educated, 4% (231) warned and a few nominal cases have been prosecuted (1%; 31).

Outcomes by agency



Predictive trends

Using breach reporting data from areas outside of Tāmaki Makaurau (Appendix A), estimated breach report trends in Tāmaki Makaurau at Alert levels 3 and 2 have been calculated¹. The reporting rate of Tāmaki Makaurau in the first 14 days of AL4 and the rest of Aotearoa at AL4, however over the past 10 days, Tāmaki Makaurau show a stable reporting rate. This was unanticipated based on previous lockdown patterns and may suggest that the region will continue to show a stable rate of reporting in Alert Levels 3 and 2, as opposed to the typical initial increased following the Alert Level shift and then a steady decline over the next few days. Therefore, it is possible that slightly high rates will be witnessed.



Breach by business predictions

This model predicts that, at AL3, there will be on average 47 breach reports relating to businesses each day in Tāmaki Makaurau. This is in addition to reports across the rest of Aotearoa which, based on data from the past 8 days, would be approximately 40 reports per day. It is also worth noting that some breach by individual or mass gathering breaches would also relate to businesses, increasing these rates subtly². **It is therefore anticipated that there will be approximately 100 breach by business reports a day from the 21st of September, while Tāmaki Makaurau is at AL3 and the rest of Aotearoa is at AL2.** If Tāmaki Makaurau were to move down to AL2 while the rest of Aotearoa remained at AL2, it is anticipated that there would be approximately 75 reports a day, decreasing further if the rest of Aotearoa were to move to AL1.

¹ Using population estimates were calculated by a per person rate was calculated for each breach type for areas outside of Tāmaki Makaurau. This rate was then multiplied by the population estimate for Tāmaki Makaurau.

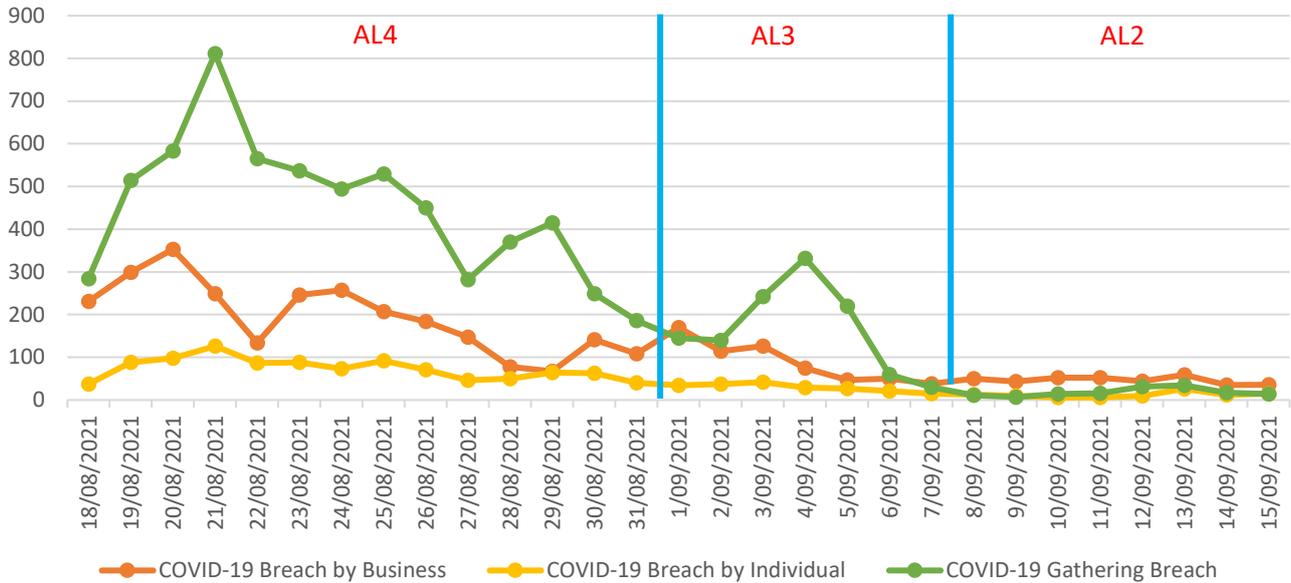
² Further analysis will be completed using the predicted rates of reports in Tāmaki Makaurau and the number of actual tasks assigned to business agencies (MBIE or Worksafe) at AL3 and AL2 to improve these estimates further.

Mass gathering breaches

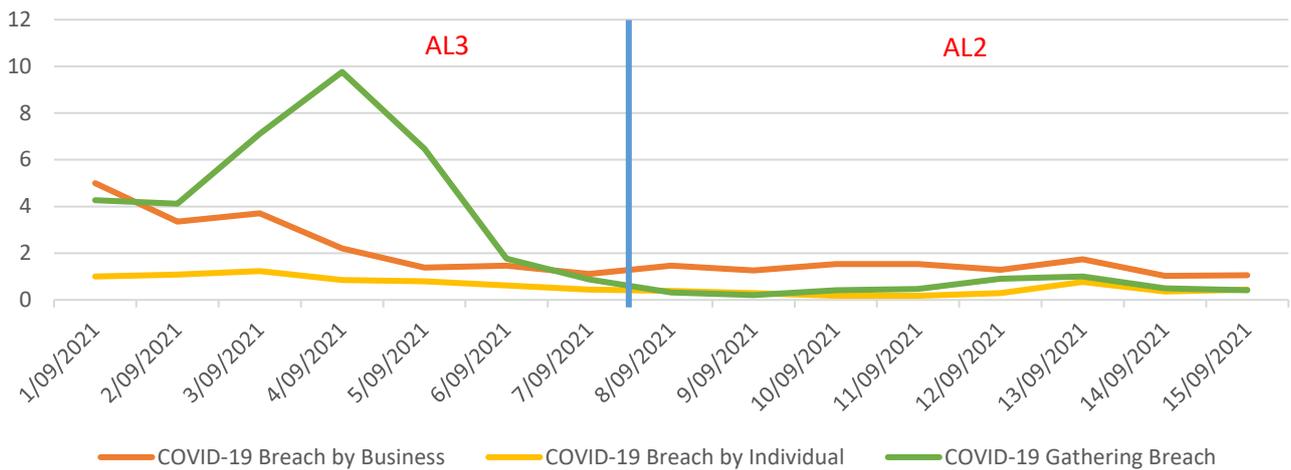
This model predicts that, at AL3, there will be on average 88 mass gathering breach reports each day in Tāmaki Makaurau. This is in addition to reports across the rest of Aotearoa which, based on data from the past 8 days, would be approximately 20 reports per day. As with businesses, some reports outside the breach by business category – namely breach by individual or unspecified breach types – would also relate to mass gatherings, increasing the rate subtly. **It is therefore anticipated that there will be approximately 110-120 mass gathering breach reports a day from the 21st of September, while Tāmaki Makaurau is at AL3 and the rest of Aotearoa is at AL2.** If Tāmaki Makaurau were to move down to AL2 while the rest of Aotearoa remained at AL2, it is anticipated that this rate would decrease dramatically – it is anticipated there would be approximately 30 reports a day, decreasing further if the rest of Aotearoa were to move to AL1.

Appendix A.

Breach reports (outside Tamaki Makaurau)



Reporting rate (outside of Tamaki Makaurau)



Production

	<i>Author:</i>	<i>Reviewed and released by:</i>
<i>Name</i>	s.9(2)(a) OIA	s.9(2)(a) OIA
<i>Role</i>	Data and Insights Lead	COVID-19 Compliance Commander
<i>Phone</i>		

Handling Instructions

All IN CONFIDENCE information (including data) should clearly identify the originating government agency and date.

Method	Rules
Electronic transmission	<p>IN CONFIDENCE data can be transmitted across external or public networks but the level of information contained should be assessed before using clear text.</p> <p>Username/Password access control and/or encryption may be advisable (with the aim of maintaining public confidence in public agencies).</p>
Manual transmission	<p>May be carried by ordinary postal service or commercial courier firm as well as mail delivery staff in a single closed envelope.</p> <p>The envelope must clearly show a return address in case delivery is unsuccessful. In some cases involving privacy concerns, identifying the originating department may be inappropriate and a return PO Box alone should be used.</p>
Storage and disposal	<p>IN CONFIDENCE information can be secured using the normal building security and door-swipe card systems that aim simply to keep the public out of administrative areas of government departments.</p> <p>Must be disposed of by departmental arrangements.</p>

Compliance Data and Insights

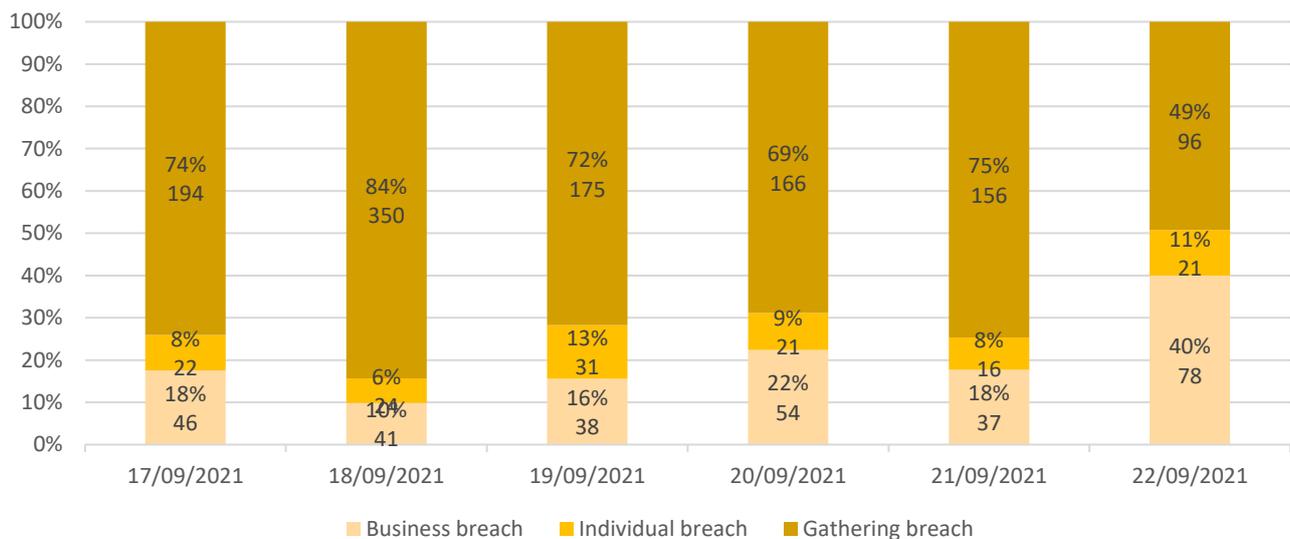
Governance report – 23 September 2021

ISR/CCS

Unless otherwise stated, data relates to 00:00 18/08/2021 to 07:30 23/09/2021.

Episodes

On Wednesday 22nd of September there were 262 new breach reports, bringing the total to 23,070. **Compared to the previous 48-hour period, the total number of breach reports decreased somewhat, however, as anticipated, there was a re-distribution of the type of breach report with a business breachers account for a larger proportion (40%; 23% increase) of all reports than across the previous 5-day period (average = 17%).**

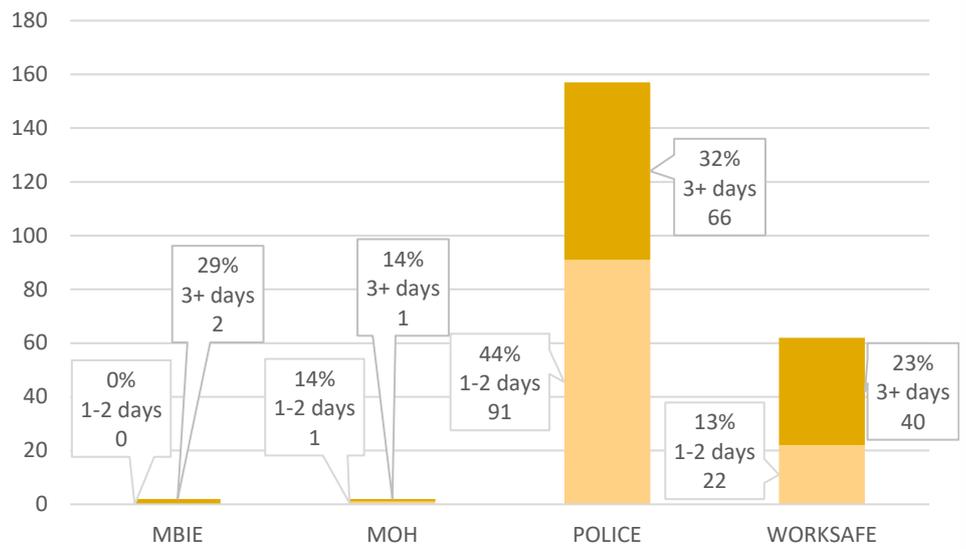


No notable changes were seen in the proportion of reports relating to Tāmaki Makaurau compared to the rest of Aotearoa, and no unusual patterns were noted in the breach reports relating to the rest of Aotearoa (consistent ~55% of breach reports relating to businesses).

Tasks

The proportion of tasks completed or closed is currently 95%. There are currently 223 tasks overdue (56% of all open tasks), 49% (109) of which are 3 or more days overdue. **The proportion overdue task 3 or more days overdue has fluctuated over the course of the week, previously peaking at 45% and reaching a low of 37%.**

The majority of overdue tasks currently reside with Police (70%), however Worksafe have a larger proportion of overdue tasks that are 3 or more days overdue (65%; Police 42%, MOH 50% - 1 case of 2 - and MBIE 100% - 2 cases of 2).



Production

	<i>Author:</i>	<i>Reviewed and released by:</i>
<i>Name</i>	s.9(2)(a) OIA	s.9(2)(a) OIA
<i>Role</i>	Data and Insights Lead	COVID-19 Compliance Lead
<i>Phone</i>	/	

Handling Instructions

All IN CONFIDENCE information (including data) should clearly identify the originating government agency and date.

Method	Rules
Electronic transmission	<p>IN CONFIDENCE data can be transmitted across external or public networks but the level of information contained should be assessed before using clear text.</p> <p>Username/Password access control and/or encryption may be advisable (with the aim of maintaining public confidence in public agencies).</p>
Manual transmission	<p>May be carried by ordinary postal service or commercial courier firm as well as mail delivery staff in a single closed envelope.</p> <p>The envelope must clearly show a return address in case delivery is unsuccessful. In some cases involving privacy concerns, identifying the originating department may be inappropriate and a return PO Box alone should be used.</p>
Storage and disposal	<p>IN CONFIDENCE information can be secured using the normal building security and door-swipe card systems that aim simply to keep the public out of administrative areas of government departments.</p> <p>Must be disposed of by departmental arrangements.</p>

Compliance Data and Insights COVID-19 response review – Governance Group 06 October 2021

ISR/CCS

Unless otherwise stated, data relates to 00:00 18/08/2021 to 07:30 06/10/2021.

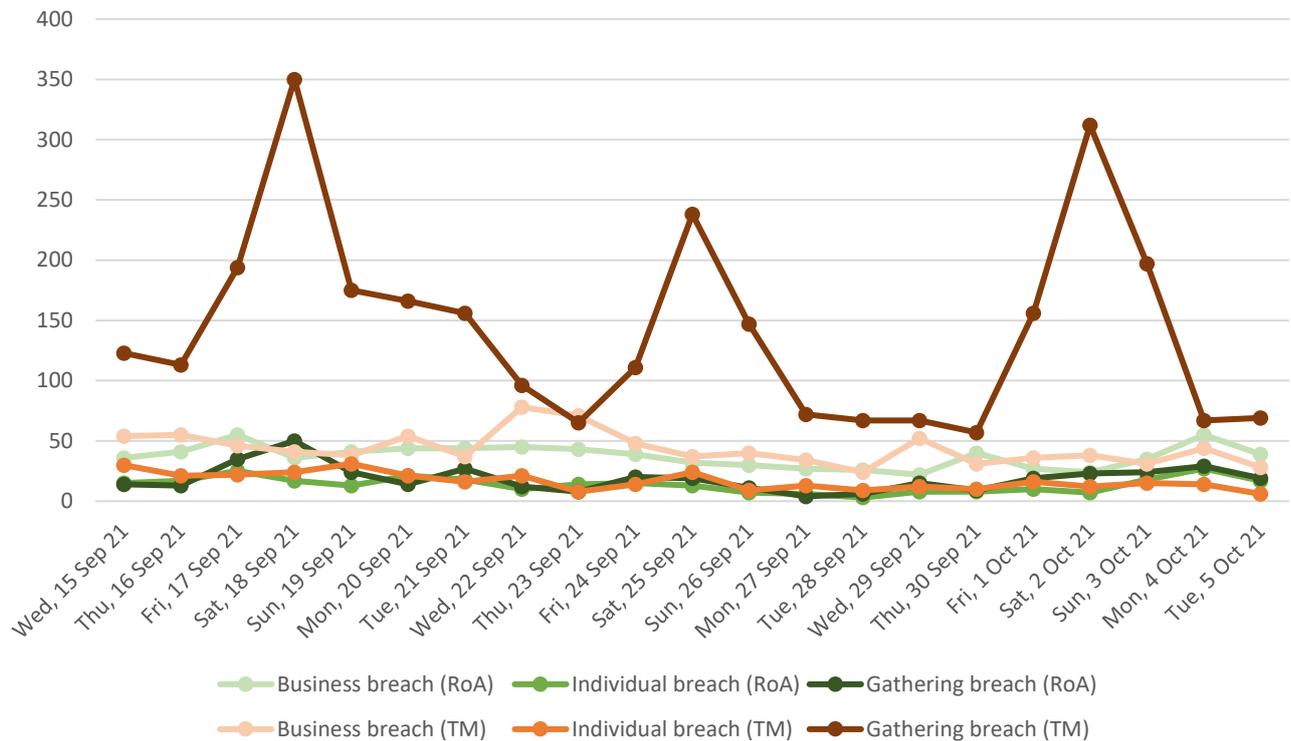
Episodes

To date, a total of 26,164 breach reports (episodes) have been received: 7,698 (29%) breach by business, 2,668 (10%) breach by individual and 15,798 (60%) mass gathering breaches.

- In Tāmaki Makaurau there have been a total of 12,164 reports (business = 3,261; individual = 1,068; gathering = 7,835). Across the rest of Aotearoa there have been a total of 14,000 reports (business = 4,437; individual = 1,600; gathering = 7,963).
- In Tāmaki Makaurau, the proportion of breaches involving gatherings was skewed slightly higher (64%) with few business breaches (27%). Across the rest of Aotearoa, the opposite pattern was found (business breaches = 32%, gathering breaches = 57%). This reflects the different restrictions of AL4/3 and AL2.
 - Key word trend analysis repeatedly identified categories gatherings at parks or beaches and household parties as predominant issues in the breach reports. Together, these data suggest that going forward or in future Alert Level escalation, it would be prudent to consider what work may be done to target these as promptly as possible, or even proactively.

Over the past week (29th September – 5th October), there have been 1,745 new breach reports. This is up 8% from the previous week (22nd – 28th September; 1616 reports).

- Across the last 3 weeks the same pattern has emerged; increased reporting of gathering breaches in Tāmaki Makaurau over the weekend period (Friday -Sunday).
 - The increase in reports last week from the week prior appears to be driven by particularly high levels of weekend activity in Tāmaki Makaurau.
- Having previously reached the lowest daily rate for breach reports during the week last week (Monday 27th – Thursday 29th September average = 156; low = Tuesday 28th September, 135 reports), the average daily rate over the past 2 days has not returned to this level. The average number of reports (207) across Monday 5th (236) and Tuesday 6th of October (178) is 33% higher than the mid-week average last week.



Risk

Most episodes have been related to high-risk breaches (47%), with only a small proportion (12%) of episodes were coded as low-risk. These proportions have not changed since last week and suggest that risk associated with breach behaviour is relatively stable.

Plans

To date, 14,392 plans have been created or updated.

- Since last week (29th October), an additional 1,262 plans have been created or updated.
- The rate of plan creation/ updating (10% increase over the week) is the same as the previous week (10%, 1,158 additional plans created/ update), suggesting that this aspect of the workload has been stable for at least 2 weeks.
- Considering last weeks decrease in mid-week episode numbers, this suggests that a higher proportion of episodes have required a plan and illustrates that episodes volume alone should not be used to determine the amount of work or resources required.

Tasks

There are currently 522 open tasks, with a majority assigned to Police (60%; 313) and most of the remaining assigned to Worksafe (31%; 162), a small amount to MBIE (7%; 23) and all others to Health (7)¹.

¹ The proportion of tasks completed or closed since the 18th of August currently stands at 94%. There has been no pronounced change in the closure rate for the last 3-4 weeks, however as time goes on and the number of tasks increases, the large number that are already closed will create skew in this rate. The change in the number

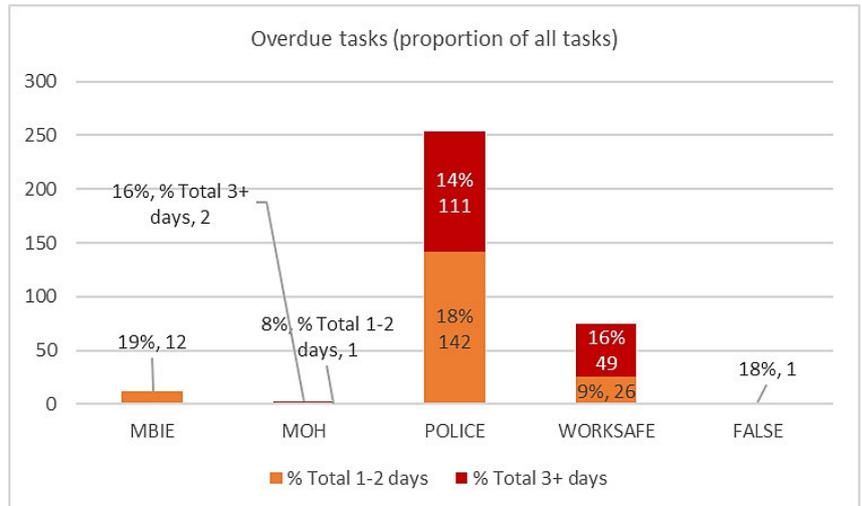
Overdue tasks

There are currently 344 tasks overdue (67% of all open tasks). Compared to last week, the proportion of open tasks that are overdue has not change drastically, although the actual number has increased by 66% (137 more overdue tasks), likely due to the increase number of tasks overall.

- **The majority of overdue tasks currently reside**

with Police (74%; 253), and has increased compared ot last week (60% of overdue tasks were assigned to Police).

- **Of all overdue tasks, 47% (162) are 3 or more days overdue.** A majority of these (69%; 111) are assigned to Police and the remainder is mostly assigned to Worksafe (30%; 49).
- This suggests a potentiall need to consider whether the resources available are sufficient for Police tasks, or whether the requirements/threshold for tasking to Police should be re-considered.



A majority of overdue tasks (58%; 200) have been updated after the due date. The proportion is lower than last week (87%) but there are more actual overdue tasks with recent updates (177), suggesting that the increased task load may be affecting the ability to update tasks promptly.

of open tasks across a couple of days/ week alongside the proportion of tasks that are overdue and the time to close tasks is a more accurate representation of progress in this space.

Production

	<i>Author:</i>	<i>Reviewed and released by:</i>
<i>Name</i>	s.9(2)(a) OIA	s.9(2)(a) OIA
<i>Role</i>	Data and Insights Lead	COVID-19 Compliance Lead
<i>Phone</i>	/	

Handling Instructions

All IN CONFIDENCE information (including data) should clearly identify the originating government agency and date.

Method	Rules
Electronic transmission	<p>IN CONFIDENCE data can be transmitted across external or public networks but the level of information contained should be assessed before using clear text.</p> <p>Username/Password access control and/or encryption may be advisable (with the aim of maintaining public confidence in public agencies).</p>
Manual transmission	<p>May be carried by ordinary postal service or commercial courier firm as well as mail delivery staff in a single closed envelope.</p> <p>The envelope must clearly show a return address in case delivery is unsuccessful. In some cases involving privacy concerns, identifying the originating department may be inappropriate and a return PO Box alone should be used.</p>
Storage and disposal	<p>IN CONFIDENCE information can be secured using the normal building security and door-swipe card systems that aim simply to keep the public out of administrative areas of government departments.</p> <p>Must be disposed of by departmental arrangements.</p>

Compliance Data and Insights COVID-19 response review – Governance Group 14 October 2021

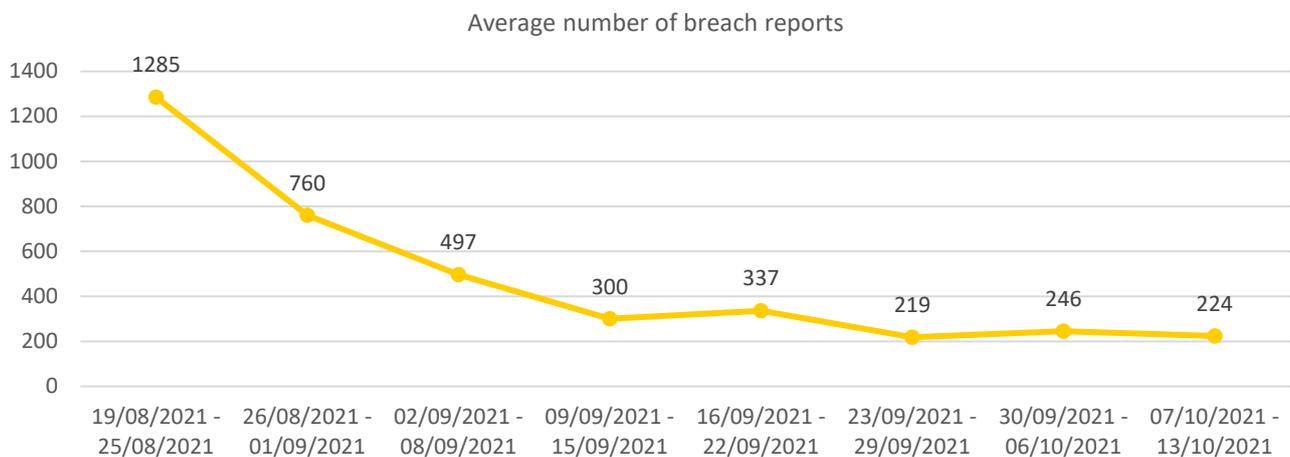
ISR/CCS

Unless otherwise stated, data relates to 00:00 18/08/2021 to 07:30 14/10/2021.

Episodes

Between the 18th of August 2021 and the 14th of October 2021 there have been 27,077 breach reports across Aotearoa: 30% (7,996) have been business breach reports, 10% (2,820) individual breach reports and 60% (16,261) gathering breach reports.

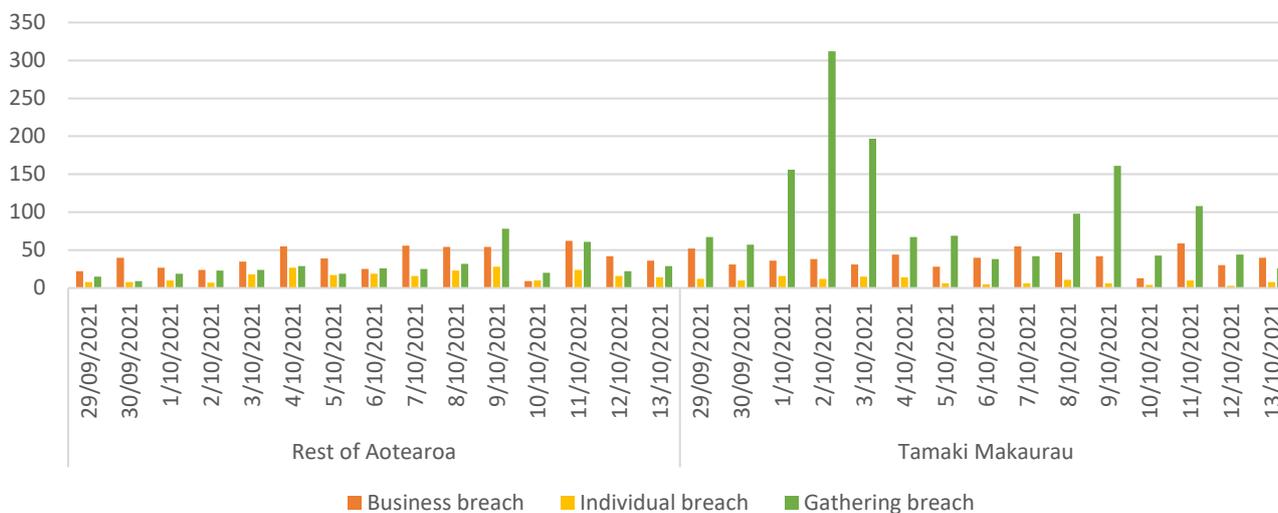
Over the past week (7th October – 13th October), there have been 1,720 new breach reports. Considering the average number of reports each week, this is on par with the previous 2 weeks and suggests the number of reports received nationally has stabilised.



Broken down by region (Tāmaki Makaurau vs the rest of Aotearoa) and breach type, the trends over the past two weeks show more variation.

- In the rest of Aotearoa, this variation is likely driven by the spread of COVID-19 and subsequent Alert Level changes in Waikato and Northland districts. Although there has been subtle increases across all breach types across the rest of Aotearoa, gathering breaches appear to have increased the most, albeit with moderate fluctuations over the past 5 days.
- In Tāmaki Makaurau, the trends are in line with past 5 weeks – stable levels of daily business and individual breach reports with gathering breach reports the most likely type across the whole week, peaking across Friday/ Saturday.

Breach reports



Note: additional analysis breaking down breach reports in the rest of Aotearoa by district, or comparing current Level 3 (Tāmaki Makaurau, Northland and Waikato) and Level 2 (rest of Aotearoa) areas would be beneficial in further testing some of the assumptions.

Tasks

There are currently 404 open tasks, with a majority assigned to Worksafe (41%; 167) followed closely by Police (38%; 153) and a then MBIE (18%; 72).

Overdue tasks

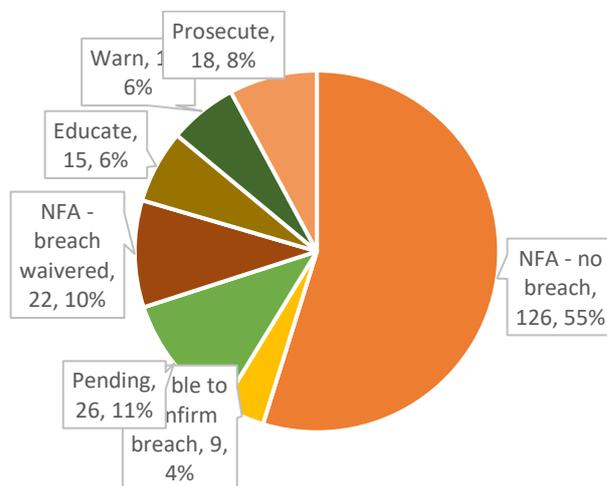
There are currently 255 tasks overdue (63% of all open tasks). Compared to last week, the proportion of open tasks that are overdue has not change drastically (down 4-percentage points), although the actual number has decreased by 26% (89 less overdue tasks).

- The majority of overdue tasks currently reside with Police (41%; 253), but this has decreased greatly compared to last week (74% - 253 - overdue tasks were assigned to Police); 37% (167) are assigned to Worksafe and 19% (72) to MBIE.
- Of all overdue tasks, for each agency, a majority are 3 or more days overdue (Police = 63%, 66 tasks; Worksafe = 64%, 60 tasks; MBIE = 80%, 39 tasks).

Boundary crossing

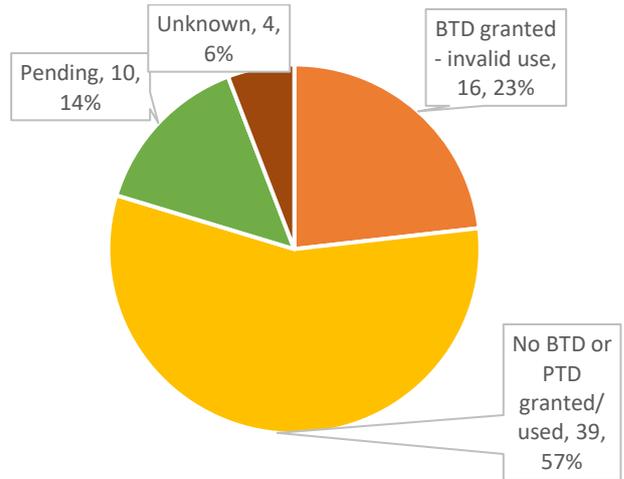
To date, 334 boundary crossings have been identified through the 105-reporting line and investigated by the COVID compliance team.

- A majority (55%) have been confirmed no breach, 30% (69) have been confirmed breach and the remainder either cannot be confirmed or are pending further investigation.



- Of those confirmed breaches:

- 32% (22) have been waived with no compliance action; 22% (15) have been educated; 20% (14) have been warned and 26% (18) have been prosecuted.
- A Majority (57%; 39) had no BTM, PTM or other documentation relating to an exemption under the order. Of these, 64% (25) have received some form of compliance action (educate = 8, warn = 7, prosecute = 10).
 - 23% (16) involve invalid use of a BTM. Of these, all except two have received some form of compliance action (educate = 3, warn = 6, prosecute = 6).
- 81% (56) involve movement from Auckland.
- 33% (23) involve movement to Waikato, 14% (10) to Northland and 12% (8) to the Bay of Plenty.



Production

	<i>Author:</i>	<i>Reviewed and released by:</i>
<i>Name</i>	s.9(2)(a) OIA	s.9(2)(a) OIA
<i>Role</i>	Data and Insights Lead	COVID-19 Compliance Lead
<i>Phone</i>	/	

Handling Instructions

All IN CONFIDENCE information (including data) should clearly identify the originating government agency and date.

Method	Rules
Electronic transmission	<p>IN CONFIDENCE data can be transmitted across external or public networks but the level of information contained should be assessed before using clear text.</p> <p>Username/Password access control and/or encryption may be advisable (with the aim of maintaining public confidence in public agencies).</p>
Manual transmission	<p>May be carried by ordinary postal service or commercial courier firm as well as mail delivery staff in a single closed envelope.</p> <p>The envelope must clearly show a return address in case delivery is unsuccessful. In some cases involving privacy concerns, identifying the originating department may be inappropriate and a return PO Box alone should be used.</p>
Storage and disposal	<p>IN CONFIDENCE information can be secured using the normal building security and door-swipe card systems that aim simply to keep the public out of administrative areas of government departments.</p> <p>Must be disposed of by departmental arrangements.</p>