



9 June 2021

[Redacted]

Reference: OIA-2020/21-0511

Dear [Redacted]

Official Information Act request for listed documents regarding Counter-Terrorism and the Royal Commission of Inquiry into the Terrorist Attack on Christchurch Mosques

Thank you for your request made under the Official Information Act 1982 (the Act), received by the Department of the Prime Minister and Cabinet (DPMC) on 12 April 2021. You requested:

"...copies of these five documents underlying the Royal Commission report:

- 1. The 2013 National Assessments Bureau assessment titled "Far Right Rising: A Dangerous Myth"*
- 2. The August 2018 draft National Risk Register; failing that, I request a copy of this document's Terrorism Risk Profile*
- 3. The September 2018 National Assessments Bureau Global Terrorism Update; failing that, I request a copy of this report's "extreme right terrorism" annex*
- 4. The 2018 Counter-Terrorism Strategic Framework*
- 5. The latest Security and Intelligence Board annual strategic assessment prior to 15 March 2019*

And I request copies of these six documents underlying the Counter-Terrorism Strategy:

- 1. The Counter-Terrorism System Capability Review*
- 2. The Counter-Terrorism Work Programme*
- 3. The Counter-Terrorism Implementation Plan*
- 4. The High-Level Framework for the Prevention of Violent Extremism*
- 5. The Public Information Action Plan*
- 6. The Counter-Terrorism Playbook. If the "Counter-Terrorism Handbook" is a separate document, I request a copy of this as well..."*

I note that on 11 May 2021 the time frame for responding to your request was extended under section 15A of the Act by 20 working days because it necessitated further consultations to be undertaken before a decision could be made on the request. Following this extension, I am now in a position to respond.

Please find enclosed copies of the following documents in the order of your request, subject to information being withheld as appropriate.

Date	Item
13 November 2013	Far-Right Rising: A Dangerous Myth (AR 54/2013-14)
June 2019	Summary of New Zealand's Terrorism Risk Profile
14 September 2018	2018 Global Terrorism Update (AR 31A/2018-19)
September 2018	New Zealand Counter-terrorism Strategic Framework
June 2020	Countering Terrorism and Violent Extremism System Capability Review: Paper 1 and CT / CVE System Capability Landscape
1 April 2021	Counter-Terrorism Work Programme 2021
19 June 2020	CT Strategy Implementation Plan - 2020
12 September 2018	Prevention of Violent Extremism – High Level Framework
11 July 2018	The Counter-Terrorism Playbook (pages 1 – 4)

Some information has been withheld in the above documents under the following sections of the Act:

- Section 6(a), as the making available of that information would be likely to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand,
- Section 6(b)(i), as the making available of that information would be likely to prejudice the entrusting of information to the Government of New Zealand on a basis of confidence by the Government of any other country or any agency of such a Government,
- Section 9(2)(ba)(i), to protect information which is subject to an obligation of confidence or which any person has been or could be compelled to provide under the authority of any enactment, where the making available of the information would be likely to prejudice the supply of similar information, or information from the same source, and it is in the public interest that such information should continue to be supplied,
- Section 9(2)(f)(iv), to maintain the constitutional conventions for the time being which protect the confidentiality of advice tendered by Ministers of the Crown and officials, and
- Section 9(2)(g)(i), to maintain the effective conduct of public affairs through the free and frank expression of opinions

With regard to the part of your request for the “August 2018 draft National Risk Register”, this was a draft internal document that was not progressed or agreed upon. Accordingly, I have decided to withhold this document in full under sections 9(2)(f)(iv) and 9(2)(g)(i), as outlined above.

I note you indicated that you would be interested in a copy of Risk Profile – Terrorism, if the draft National Risk Register could not be released. As I am sure you can appreciate, inherent risks need to be mitigated in releasing this Risk Profile. Accordingly, I have decided to summarise the information contained in this document in accordance with section 16(1)(e) of the Act. In doing so, I consider that the condition outlined in section 16(2)(c) of the Act is met.

With regard to the part of your request for “the latest Security and Intelligence Board annual strategic assessment prior to 15 March 2019”, I have decided to withhold this document under section 6(a) of the Act.

You will note two parts of the "Counter-Terrorism System Capability Review" are enclosed. Two further items comprise this Review. I have decided to withhold these parts in full under sections 6(a), 9(2)(ba)(i), and 9(2)(g)(i) of the Act, as outlined above.

In considering the current copy of the Counter-Terrorism Work Programme (enclosed), you may also be interested in the previous Work Programme. If you have not already seen it, a copy of that version is available at the following address (page 4):

<https://dpmc.govt.nz/sites/default/files/2020-02/2019-20%20CT%20Strategy-all-final.pdf>. The Public Information Action Plan is also available at this address (page 6). Accordingly, in so far as your request is for the Public Information Action Plan, I am formally refusing it under section 18(d) of the Act, as the information requested is publicly available.

In considering the item *Prevention of Violent Extremism - High Level Framework*, I would note that this item has been superseded by New Zealand's Counter-Terrorism Strategy. The Counter-Terrorism Strategy can be found online at: <https://dpmc.govt.nz/publications/new-zealands-counter-terrorism-strategy>.

With regard to the final part of your request, I have decided to release the first four pages of the Counter-Terrorism Playbook. The remainder of this document needs to be withheld under section 6(a) of the Act. You may be interested to know that the Counter-Terrorism Playbook was superseded by the Counter-Terrorism Handbook, which was finalised in late 2019. The Counter-Terrorism Handbook can be found online through the following link (page 3): dpmc.govt.nz/sites/default/files/2020-02/2019-20%20CT%20Strategy-all-final.pdf. In so far as your request relates to the Counter-Terrorism Handbook, I am accordingly also refusing this part under section 18(d) of the Act.

In making my decision, I have taken the public interest considerations in section 9(1) of the Act into account.

You have the right to ask the Ombudsman to investigate and review my decision under section 28(3) of the Act.

This response will be published on DPMC's website during our regular publication cycle. Typically, information is released monthly, or as otherwise determined. Your personal information including name and contact details will be removed for publication.

Yours sincerely



Dan Eaton
Acting Deputy Chief Executive
National Security Group

RESTRICTED

6(a)



NATIONAL
ASSESSMENTS
BUREAU

TE RANGA TĀTARI TAKE

DEPARTMENT OF THE PRIME MINISTER AND CABINET

Wellington, New Zealand

13 November 2013

FAR-RIGHT RISING: A DANGEROUS MYTH
AR 54/2013-14

(RESTRICTED 6(a))

6(a)

RESTRICTED

AR 54/2013-14
Assessment Report

13 November 2013

FAR-RIGHT RISING: A DANGEROUS MYTH

What's Happening?

- During the eurozone crisis, far-right movements across Europe stepped up their anti-immigrant, anti-Muslim, anti-establishment and anti-EU rhetoric. But although the far-right's share of the national vote has remained largely static over this period, their increased vocalisation of populist issues is putting pressure on mainstream political parties to respond. (U)

Why Is This Important?

- Mainstream European politicians appear to be responding to the threat of far-right and populist parties by advocating tough policies at home, especially in the area of immigration and the free movement of persons within the EU. This trend will likely be amplified at the EU level with the potential increase in anti-EU presence after the European Parliament election in 2014. (R)

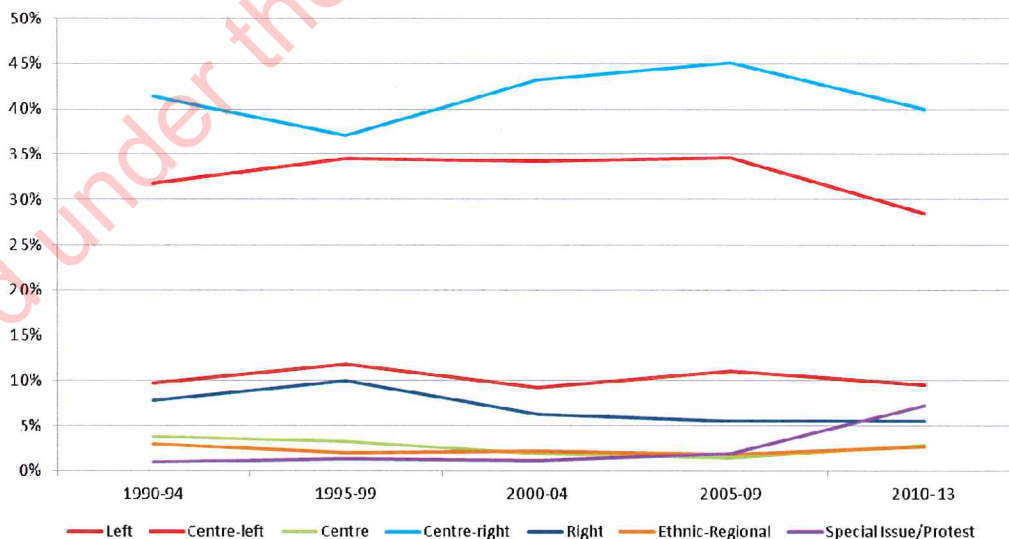
6(a)

Far-right support in Europe

Since 2010 media coverage of the eurozone crisis has promoted the idea that, as in the past, support for 6(a) far-right parties in Europe is once again growing at an alarming rate in reaction to the protracted economic crisis and the harsh austerity imposed by Brussels.¹ In the 17 elections that have occurred in eurozone countries since 2010, this apparent increased support for right-wing parties has not translated into votes (see charts below).² Troubled economies like Portugal, Ireland and Spain do not have far-right parties of any significant standing and in economies that do, like Italy, far-right parties have witnessed a reversal of fortunes at the polls. In relatively prosperous countries, the opposite is true. The proportion of parliamentary representation for far-right parties in Finland, Austria and Belgium has increased since 2010 to between 20 and 26 per cent. (U)

2. So while some support for far-right parties is an established part of Europe's long-term political trend (see charts below), it is difficult to locate a consistent and singular explanation for why and where the far-right has sustained its presence. It is certainly more complex than a simple focus on the economic crisis and the insecurity it breeds. Voters are disillusioned with the policy convergence of mainstream parties. They are also dissatisfied with current immigration policies and immigration levels. Immigrants are viewed as posing a threat to national culture and identity, personal safety (with higher crime rates) and access to subsidised economic resources at a time of fiscal austerity. (U)

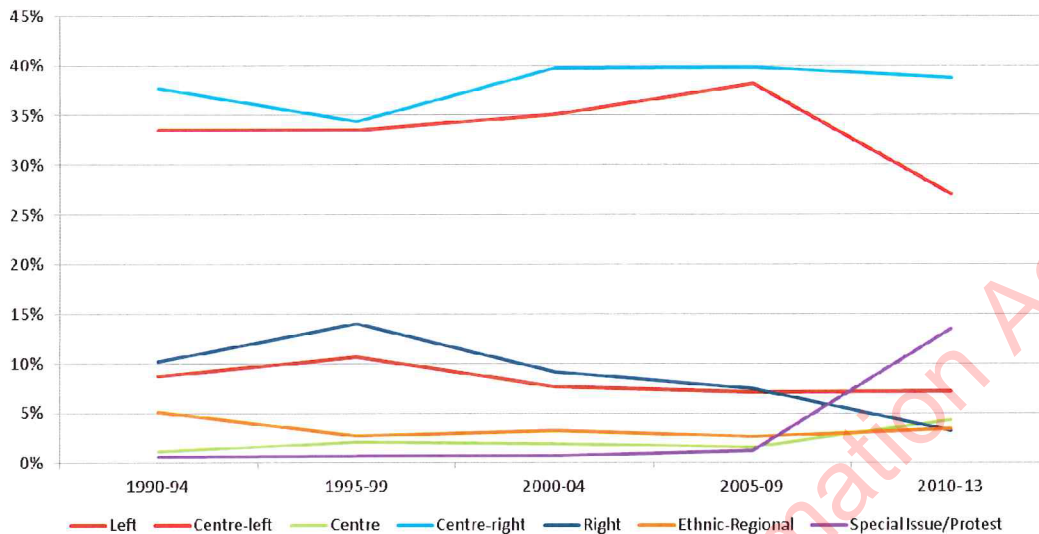
Avg. percentage share of votes across 17 eurozone countries



¹ Although there is no singular definition of what constitutes a far-right party, and they have varied platforms across Europe, a common element is their deeply nationalist and xenophobic rhetoric. (U)

² The level of permissiveness of the electoral system (single-winner versus proportional voting systems) also appears to magnify or shrink the strength of a far-right movement in a given country. (U)

Avg. percentage share of votes across Cyprus, Greece, Ireland, Italy, Portugal and Spain



Source: European Election Database (EED) corroborated with external sources
 Left includes communist and ecologist parties; Centre-left includes social democratic parties; Centre-right includes Christian democratic, conservative and European liberal parties; Right includes libertarian and nationalist parties. (U)

Mainstreaming the right

3. The 6(a) image of right-wing parties is also undergoing a shift. 6(a) groups like Golden Dawn in Greece, Jobbik in Hungary and Attack in Bulgaria are the exception rather than the norm. Right-wing groups are rebranding themselves with centrist and even left-wing policies and flavouring them with protectionism and nationalism. The leader of the **Dutch** Party for Freedom (PVV) Geert Wilders has fashioned himself as a defender of gay rights and gender equality. He justifies his anti-Islam stance by the threat it poses to western liberal values and is a staunch supporter of Israel, 6(a) making his anti-Islam stance more plausible. In **France**, the National Front's (FN) leader Marine Le Pen has been trying to distance the FN from the radical 6(a) reputation of her holocaust-denying father Jean-Marie. Marine is pro-choice and economically interventionist. Like Wilders, she has also successfully repackaged the FN's anti-immigration and anti-Islam stance as a battle to uphold France's secular democracy. (U)

4. While far-right parties are dressing up their policies with a moderate tone to try to capture a wider electoral base, mainstream parties are failing to challenge the racist stereotypes of the right's 6(a) politics.³ They are also reacting with anti-

³ 6(a)

immigrant (and anti-Islam) rhetoric, to some extent further normalising the right-wing and what they represent. In 2010, former **French** President Sarkozy tried to convince the French public of his right-wing credentials with the large-scale deportations of Roma camps around Paris. In the 2012 election Sarkozy's proposed immigration policies took a right-ward turn once again which was interpreted as a response to the newfound success of Marine Le Pen and the FN. And the Roma deportations continue under the current socialist administration of President Hollande. (U)

5. In the **Netherlands**, the Liberal-Christian Democrat alliance with the PVV before the government fell planned to introduce a general ban on burkas and other face-covering clothing and to restrict dual nationality. The same alliance also proposed to withdraw residence permits of migrants who did not take obligatory Dutch language courses and those who failed the civic integration examination. In **Britain**, the threat of the UK Independence Party has pushed the ruling Conservative party further to the right on immigration and on the UK's relationship with the EU. The government recently introduced a new immigration bill which requires private landlords to confirm the immigration status of tenants and contains proposals to make temporary migrants pay a levy to use the National Health Service. (U)

Europe's anti-establishment trend

6. The only significant gain over the past four years has been for special issue and protest parties such as Italy's Five Star Movement which took a quarter of the popular vote in the 2013 election. Such parties are equally fierce in their demands to change the way politics is conducted, but they lack the strong anti-capitalist and racist undertones that would allow them to be easily pigeon holed as left or right on the political spectrum. Left-wing parties have also managed to hang on to votes over the past decade and in some cases, like Greece's SYRIZA party, are polling significantly higher than the mainstream centre-left parties. What left, right and protest parties share in common is disillusionment with the policy convergence of mainstream centre left and right parties. They are anti-establishment and increasingly anti-EU. (U)

Implications for the European Union

7. The European Parliament (EP) has steadily been gaining powers. And under the Lisbon Treaty of 2009, it now has equal say on the vast majority of European laws on economic governance, immigration, energy, transport, the environment and consumer protection. But EP elections are typically viewed by EU citizens as an

opportunity to lodge a protest vote against mainstream national parties. Eurosceptic parties currently have a presence in the EP and their numbers could swell after the 2014 EP election with the addition of left-wing, right-wing and protest parties that share the anti-EU stance. While it is highly unlikely that parties from both ends of the political spectrum will cooperate with each other, their combined anti-EU presence in the EP could challenge EU processes and act as a strong headwind in the face of further integration. And even if pro-EU parties continue to form the majority at the national and EU level, their room to manoeuvre on European policy shrinks if they also feel the need to respond to nationalist and anti-EU parties. (R)

Implications for New Zealand

8. The EU sets policy in key areas like trade, investment and immigration. If far-right, protest and left-wing anti-establishment parties are successful in shifting the debate at the national and EU level, it could impact on New Zealand's interests. (R)

6(a)



* * * * *

AR 54/2013-14 DISTRIBUTION LIST

Hard Copy Distribution

Ministers

Rt Hon John Key	(via Mr B King)
Hon Murray McCully	(via Mr J Fepuleai)
Hon Dr Jonathan Coleman	(via GCSB Reader Service)

Department of the Prime Minister & Cabinet

Ms R Kitteridge

NAB

Registry copy

Electronic Distribution (via NZICnet and/or MFAT Merlin)

CTAG

DPMC (CEO, FPA, PAG, NCPO, SRG & ICG)

DDI

GCSB

Immigration Intelligence Unit

NZSIS

Ministry of Foreign Affairs and Trade

Ministry of Defence

New Zealand Customs Service

New Zealand Police (NIC)

This document is the property of the
Government of New Zealand and is to be handled
as provided for in the official publication entitled
Security in the Government Sector.



Summary of New Zealand's Terrorism Risk Profile

Introduction

This document summarises the content of New Zealand's Terrorism Risk Profile, which was developed in June 2019 by New Zealand Security Intelligence Service, New Zealand Police, and the Department of the Prime Minister and Cabinet. While the Terrorism Risk Profile is classified, this document provides a comprehensive summary of the content of the profile. The full Terrorism Risk Profile is a classified document to ensure methods, techniques and capabilities are protected.

Risk profiles are documents produced by government agencies to support the National Security System's awareness and decision making on nationally significant hazards and threats. The two Officials Committee for Domestic and External Security Coordination (ODESC) Boards; the Hazard Risk Board and Security and Intelligence Board; use risk profiles to strategically govern risks that could have a significant impact on New Zealand's security.

The Hazard Risk Board and Security Intelligence Board use risk profiles to examine how effectively risks are being managed, and provide direction about what steps could be taken to improve our management of risks and strengthen New Zealand's resilience. Risk profiles are reviewed on a regular basis and updated when appropriate.

The Terrorism Risk Profile was updated in the aftermath of the 15 March 2019 terrorist attack on Christchurch mosques, to capture the shifts in agencies' understanding of this risk in New Zealand. Since this Risk Profile was produced, the Royal Commission of Inquiry into the attack on Christchurch masjids on 15 March 2019 has presented its findings in its Report: *Ko tō tātou kāinga tenei*. This Report is available online at: <https://christchurchattack.royalcommission.nz/>.

Our national approach to countering terrorism and violent extremism is set out in [New Zealand's Counter-Terrorism Strategy](#)¹, with an aim of bringing our nation together to protect all New Zealanders from terrorism and violent extremism of all kinds. This strategy prioritises prevention – focusing on increasing understanding, working collectively, building resilient communities, and addressing the underlying causes of violent extremism – whilst ensuring systems and capabilities are in place to act early and to respond whenever needed.

The Terrorism Risk Profile is a key document that underpins this strategy, by supporting awareness and decision-making to manage the risk as effectively as possible.

¹ Available online at <https://dpmc.govt.nz/our-programmes/national-security-and-intelligence/national-security/counter-terrorism/new-zealands>

Terrorism Risk Profile Summary: June 2019

Risk Description

Under New Zealand law, a terrorist act is defined as an ideologically, politically, or religiously motivated act – including those causing death or serious bodily injury – intended to induce terror in the population, or to compel the government to do or not do certain things.

The Terrorism Risk Profile considers the risk of a terrorist attack in New Zealand, and a terrorist attack off-shore impacting New Zealanders (e.g. while travelling, living/working off-shore or attending an international event). The scope of the Risk Profile includes violent extremism in so far as it is a precursor to, or supportive of, terrorist activity.²

Context

On 15 March 2019, New Zealand experienced its most significant terrorist attack. Two Christchurch mosques were targeted, killing 51 people and seriously injuring dozens more. This attack was undertaken by an individual assessed to adhere to a violent extreme right-wing ideology, who live-streamed the attack on social media.

Due to the unprecedented nature of the Christchurch terrorist attack, it will take time to fully understand the long-term impacts on New Zealand's terrorism threat environment. However, the impact is likely to be wide-ranging, significant and enduring.

The Christchurch terrorist attack had a significant impact domestically and internationally, and has received a considerable amount of international attention. The Risk Profile assessment recognises that this event could potentially inspire a retaliatory or copycat attack in New Zealand or off-shore, and may be a motivating or radicalising event for years to come.

New Zealand's national terrorism threat level

The Combined Threat Assessment Group (CTAG), an autonomous inter-agency group hosted by New Zealand Security Intelligence Service, is responsible for reviewing and recommending the national terrorism threat level. New Zealand's national terrorism threat level is continuously monitored and can change at short notice.

The Risk Profile acknowledges the shift in New Zealand's terrorism threat environment following the Christchurch terrorist attack, reflecting the CTAG's assessment of the terrorism threat level from LOW to HIGH in the aftermath of the Christchurch attack, which was then reduced to MEDIUM³ in April 2019.

Since this Risk Profile was completed in June 2019, the terminology generally used by New Zealand government agencies to describe terrorist and violent extremist ideologies has been updated.

² In the absence of a formal legal definition, violent extremism as described in the national Counter-Terrorism Strategy is the justification of violence with the aim of radically changing the nature of government, religion or society. This violence is often targeted against groups seen as threatening violent extremists' success or survival or undermining their world view. Pathways to radicalisation are also relevant to this risk profile, particularly in the context of managing the risk of terrorism.

³ Terrorism threat levels are a statement about the likelihood of a terrorist attack occurring based on the intent and capability of actors. Medium means a terrorist attack is assessed as feasible and could well occur.

Sources of terrorism

The Risk Profile outlines three sources of the terrorism threat, in no particular order, using the terminology that was in use at the time⁴:

- **Violent right-wing extremism** - Violent right-wing extremism referred to the beliefs and actions of people who support or use violence to achieve their extreme right-wing goals, which may include terrorism.⁵
- **Violent Islamist extremism** - Islamist extremism was defined as a revolutionary political ideology, the goal of which is to remove existing social and political systems, and impose a single system based on an extremist interpretation of the Qur'an. Violent Islamist extremism refers to the beliefs and actions of people who support or use violence to achieve these ideological goals, which may include terrorism.
- **Other types of violent extremism** – This includes other terrorist groups, and other issue-motivated groups and individuals who may conduct terrorist acts.

CTAG assessed it was probable there were individuals in New Zealand with an extreme right-wing ideology with the intent and capability to conduct a terrorist attack who have not come to the attention of security agencies. Further, the Risk Profile highlights that right-wing extremism in New Zealand is generally fragmented in nature and has a significant presence online.

The Risk Profile notes that New Zealand agencies are aware of a small number of Islamist extremists in New Zealand who were of security concern and who had the capability to commit an unsophisticated terrorist attack. There have been numerous calls of encouragement over many years from the Islamic State of Syria and the Levant (ISIL) and al-Qai'da, and their support to conduct attacks targeting the West. Since the Christchurch terrorist attack, calls of encouragement have specifically mentioned New Zealand.

Risk Drivers

International political and social drivers will have an impact on both the international and domestic threat environment, although when and how is difficult to predict. Terrorism is driven and exacerbated by a range of social, religious, ideological and political factors. Radicalisation pathways vary widely between individuals, however, there are certain identifiable patterns.

Known risk drivers include:

- The internet and social media
- Radicalising and mobilising influences
- Changing demographics
- Individual and group dissatisfaction and grievance
- Ideology
- High profile conflicts and extremist flashpoints.

⁴ As at May 2021, the NZSIS uses the following terminology when referring to extremist ideology:

- Faith-Motivated Violent Extremism (FMVE): promoting the use of violence to advance one's own spiritual or religious objectives;

- Identity-Motivated Violent Extremism (IMVE): promoting the use of violence to advance one's own perception of identity and/or denigrate others' perceived identities;

- Politically-Motivated Violent Extremism (SMVE): promoting the use of violence to achieve a desired outcome to a specific issue; and

- White Identity Extremism (WIE): describes extremely radical ideologies and beliefs that are focussed on real or perceived threats to concepts of a white or ethnic-European culture and identity.

⁵ Right-wing extremism encompasses a broad umbrella of beliefs and ideologies, including, but not limited to, racism, Islamophobia, anti-Semitism, homophobia, sexism, authoritarianism, anti-immigration and anti-democratic views. Adherents may strongly espouse some or all of these views.

Risk Analysis

Each nationally significant risk on the National Risk Register is assessed using a standardised methodology. These assessments are undertaken by subject matter experts and informed by our current understanding of the risk.

Nationally significant risks are assessed using a "maximum credible event" scenario; a plausible worst-case scenario that could occur in the next five years which could have significant negative impacts on New Zealand and would require significant coordination by government. Looking at the risk in this way helps agencies to plan and be prepared for the worst-case-scenario, if it were to play out.

The overall risk rating is derived from an assessment of the likelihood and consequence of the maximum credible event, with the results of the analysis recorded in the Risk Profile.

There are a wide range of scenarios by which terrorism could occur, which vary in target, method and number of casualties. The Terrorism Risk Profile includes an assessment of three plausible worst-case scenarios for a terrorist attack in New Zealand. All scenarios would require a degree of planning, preparation, capability and coordination.

Likelihood

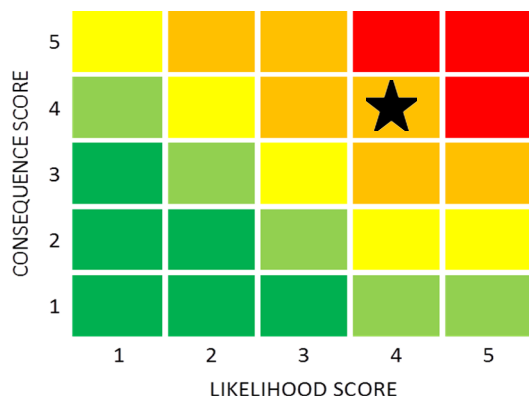
The likelihood of the three scenarios occurring was assessed by subject matter experts as LIKELY; "likely to occur, regular recorded events and strong anecdotal evidence; once per 1-10 years".

Terrorist attacks and plots can be difficult to detect due to their generally covert nature, and can occur with little or no forewarning. Prevention and security activities by a range of agencies help reduce the likelihood of an attack, but there will always be some risk.

Consequences

The consequence of the scenarios was assessed as MAJOR; "Multi-functional, multi-regional specialised management required, national agencies involved, of interest to international institutions and partner states".

A significant terrorist attack could have wide-ranging impacts, such as death, physical and psychological injuries, eroded public perceptions of safety, and exacerbation or creation of divisions in society along social, ethnic, religious or other lines. Other consequences could include damage to built infrastructure, erosion of confidence in government and institutions; and pressure for policy change.



Based on the analysis above, the overall risk rating for Terrorism was assessed as 'Very High'. The national risk rating for Terrorism differs to the national terrorism threat level administered by CTAG (which at the time was MEDIUM). CTAG's terrorism threat levels are a statement about the current likelihood of a terrorist attack occurring. They reflect the assessment of CTAG on the intent and capability of actors to conduct terrorist attacks in New Zealand. National risk assessments capture the likelihood and consequence of a potential worst-case scenario occurring in the next five years.

Risk Management

New Zealand actively seeks to reduce the threat of terrorism, both globally and at home. Our counter-terrorism system and related activities aim to protect New Zealanders and support the global effort to counter terrorism and violent extremism. The range of counter-terrorism activities can be organised into categories broadly reflecting their place on a terrorism prevention spectrum. The risk management activities below are highlighted in the Risk Profile:

Understand the threat

Understanding the threat of terrorism is critical as it informs and enables all other counter-terrorism activities. Example of risk management activities in this space include:

- the National Security and Intelligence Priorities (NSIPs), which provide high level direction for agencies involved in counter-terrorism to influence resourcing and prioritisation of intelligence and assessment effort
- the delivery of CTAG's annual strategic terrorism threat assessment
- New Zealand's national terrorism threat level system
- terror-related communication and public awareness, including on the role of the public in helping to counter the threat.

Reduce the threat (globally and at home)

Global initiatives include:

- supporting and implementing various counter-terrorism-related United Nations resolutions and conventions, and participating in a growing number of international fora, committees and working groups focussed on countering terrorism and violent extremism
- maintaining and fostering strong international relationships
- the 'Christchurch Call' and related efforts to tackle and eliminate extremist content online.

Domestic risk management activities include:

- social initiatives which support vulnerable communities and enhance social inclusion
- intervention, monitoring and disengagement activities by agencies for specific persons of concern
- combating violent extremist content online within New Zealand's jurisdiction, supported by the Films, Videos, and Publications Classification Act 1993
- limiting access to resources used to conduct terror activities (such as weapons and finances), through legislative change (amendments to the Arms Act 1983) and New Zealand's ongoing commitment to anti-money laundering and countering terrorist financing (AML/CFT).

Address vulnerabilities
<p>New Zealand has in place a range of precautionary measures and activities intended to protect the public through strengthening potential vulnerabilities or ensuring the integrity of critical systems. These include:</p> <ul style="list-style-type: none"> • the Crowded places strategy • aviation and maritime security efforts • improving information-sharing between border agencies.
Prevent and disrupt extremist activity
<p>New Zealand agencies engage in legal, operational policy and security activities that target specific terrorist and violent extremist threats. These activities range from the designation of terrorist groups and the administration of terrorism-related legislation, to passport cancellations, the disruption of extremist propaganda channels, operational investigations and plot disruption, through to terrorism-related criminal prosecutions. The ability to prevent and disrupt terrorist activity relies heavily on counter-terrorism legislation.</p> <p>Examples of activity in this area includes:</p> <ul style="list-style-type: none"> • the review of counter-terrorism legislation • Responding to the Law Commission's report <i>The Crown in Court: A Review of the Crown Proceedings Act and National Security Information in Proceedings</i> 14 December 2015 (NZLC R135).
Remain ready to respond and recover
<p>There is an ongoing requirement for New Zealand's national security system and its agencies to be ready to respond to, and recover from, a terrorist attack. Activities in this area include:</p> <ul style="list-style-type: none"> • the framework of the ODESC system whereby the threat, risk, mitigations and response are escalated through Watch Groups, the ODESC Board and ministers as deemed necessary • tactical response planning, training and exercising, such as counter-terrorism exercises conducted as part of the National Exercise Programme (NEP) • ongoing review of agency responses to the Christchurch terror attacks.



NATIONAL
ASSESSMENTS
BUREAU
Te Ranga Tātari Take

DEPARTMENT OF THE PRIME MINISTER AND CABINET

Wellington, New Zealand

AR 31A/2018-19
Assessment Report

14 September 2018


2018 GLOBAL TERRORISM UPDATE

6(a), 6(b)(i)

6(a), 6(b)(i)


Two pages removed from document - withheld under sections 6(a) and 6(b)(i) of the Act

6(a), 6(b)(i)



* * * * *

6(a), 6(b)(i)



Annex 2: Extreme-right terrorism

Although the most prominent threat is currently from jihadist terrorism, this is not the only form of violent extremism. One notable example of this is extreme-right terrorism, and the rising global trends of right wing groups using violence to further their aims. Between 12 September 2001 and 31 December 2016 in the United States, there were more extreme-right incidents than Islamist terrorist incidents resulting in fatalities. (R)

There has been an emerging threat from extreme-right terrorism for some time, but groups are fragmented and there is limited coordination internationally. Although far right extremism is not limited to anti-Islamism, Islamist extremist attacks have provoked retaliatory attacks, including from extreme right-wing groups. (R)

Extreme-right wing groups are present in New Zealand and have an online presence, but have not been active. Extreme-right groups differ from far right groups in the fact that the extreme-right is willing to use terrorism to further their aims. There has been no evidence to suggest New Zealand-based far right groups have the intent or capability to promote their ideology by an act of terrorism. (R)

New Zealand Counter-terrorism Strategic Framework 2018

Approved by the Security and Intelligence Board, September 2018

Counter-terrorism strategic framework

This strategic framework covers the fundamental aspects of New Zealand's approach to counter terrorism (CT), including our guiding objectives and principles, main activities, key system pillars and system organisational arrangements.

This framework supports a consistent understanding of our counter-terrorism approach and counter-terrorism system across government, as well as supporting the consistent articulation of that system to stakeholders. This framework is also a reference when considering counter-terrorism system priorities.

While the focus of this Framework is on the CT activities of government agencies, it is acknowledged that non-government, community and private sector organisations also played important roles.

The framework sits alongside and supports other key counter-terrorism system and strategic documents, including the terrorism risk profile. It has been produced on behalf of the Counter-Terrorism Coordination Committee (CTCC) and the Security and Intelligence Board (SIB).

The Strategic Framework is comprised of 4 sections:

- Terrorism threat environment
- Objectives and key principles
- Activities and key enablers
- System organisation and governance

DEFINITIONS

Terrorism - Under New Zealand law, terrorism is defined as an ideologically, politically, or religiously motivated act intended to induce terror in the population or coerce a government or other authority.

Violent Extremism - There is no legal or single international definition of violent extremism. But for the purpose of this Strategic Framework it can be understood as concerning the beliefs or ideas that underpin terrorist intent.

Terrorism threat environment

Terrorism is a pervasive international threat reaching across geographic distance and national boundaries. It is a threat that involves extreme violence and the threat to life. It has the potential for significant psychological and socially destabilising outcomes. For all of these reasons, it is a threat that New Zealand actively confronts, both globally and at home.

The emergence and expansion of ISIL and other Islamist extremist groups has consolidated a truly global brand of terrorism. While the territorial caliphate ISIL sought to build in Iraq and Syria has been reversed, ISIL's narrative endures and its broader strategy of directing, enabling and inspiring foreign attacks will continue to be felt throughout the Western world and in our region. Terrorism should not be characterised as an Islamist extremist threat alone, but this is the form of terrorism and violent extremism that currently represents the most significant threat to New Zealand and New Zealanders.

Almost every country is exposed to the threat of violent extremism. New Zealand has its own geographic, socio-cultural profile. However, we remain vulnerable to terrorism for reasons shared by many other countries: the ubiquity of the internet, the connectedness of international travel and trade systems, regional extremism, as well as the presence within all societies of disconnected or vulnerable individuals susceptible to extremist messaging or ideology.

New Zealanders are global citizens who travel widely for lifestyle, leisure and work. As such, New Zealanders face the threat of terrorism and violent extremism whilst travelling or living in other countries. New Zealand citizens have been killed, injured and deeply impacted by terrorist attacks in various parts of the world.

A terrorist attack in this country cannot be discounted. There are individuals in New Zealand who subscribe to extremist narratives and are consuming extremist material online. This includes propaganda that aims to enable and inspire attacks. There are almost certainly individuals in New Zealand that have not yet come to the attention of intelligence and law enforcement agencies. A very small number of New Zealanders of security interest have travelled to join or support terrorist groups offshore, and could return to New Zealand.

Objectives and key principles

COUNTER-TERRORISM OBJECTIVE

Our counter-terrorism system and related activities aim to protect New Zealanders and support the global effort to counter terrorism and violent extremism.

COUNTER-TERRORISM KEY PRINCIPLES

Underpinning principles guide our approach in pursuing this objective.

1. **We aim to take a holistic and strategic approach to the threat of terrorism.** This approach stretches across the 4Rs (reduction, readiness, response, recovery), consistent with New Zealand's approach to other national security threats and hazards. We strive to be proactive and place an especially high priority on reduction activity across a broad risk and prevention spectrum. This includes tackling the root causes of violent extremism (both globally and in New Zealand), as well as activities that address more immediate extremist and terrorist threats. In addition, we maintain a keen vigilance and seek to be ready to respond to, and recover from, a terrorist attack.
2. **We recognise the global threat of terrorism in the New Zealand context.** We recognise the highly global, cross-border nature of the threat of terrorism and New Zealand's exposure to globally-driven terrorism, as well our role as a responsible global citizen in tackling terrorism at the global level. At the same time, we make sure our approach is calibrated to the particular threat faced by New Zealand and the nature of our own domestic environment.
3. **We act in proportion to the risk faced by New Zealand consistent with New Zealand values.** Sometimes the government will need to use intrusive powers and capabilities to deal with threat of violent extremism and terrorism. These powers and capabilities need to be exercised in a manner that's in proportion to the particular risk, consistent with the law, and in line with New Zealand's commitment to a free, open and democratic society.

Activities and key enablers

COUNTER-TERRORISM ACTIVITIES

New Zealand government agencies are engaged in a wide range of activities intended to counter terrorism and violent extremism. Non-government organisations, private sector and community organisations, also play an important role in some areas.

The range of counter-terrorism activities can be organised into categories broadly reflecting their place on a terrorism prevention spectrum. Collectively, these activities support New Zealand to:

- understand the threat
- reduce the threat (globally and at home)
- address vulnerabilities
- prevent and disrupt extremist activity
- remain ready to respond.



ACTIVITY	OBJECTIVE	KEY AGENCIES	DESCRIPTION
Threat awareness	Understand the threat	NZSIS, GCSB, CTAG, DPMC, NZ Police, MFAT, NZDF, MoD	At the strategic level, threat awareness involves the ongoing collection and assessment of intelligence and information about the terrorism threat environment, both at the global and domestic level. At a more tactical level, it includes threat surveillance, monitoring high risk actors, intelligence support for deployments and operations or threat assessments for major events. Communications also play a part in raising threat awareness at the public level.
Global contribution	Reduce the threat (at the global level)	MFAT, NZDF, MoD, NZ Police, NZSIS, GCSB	New Zealand contributes to the global effort to reduce the threat of terrorism on a number of fronts. This includes the implementation of terrorism-related United Nations resolutions, terrorist designations, collaboration with partners and the international community, capacity building and training, off-shore deployments, and the disruption of terrorist financial channels.
Risk reduction and prevention	Reduce the threat (at the domestic level)	NZ Police, Corrections, MSD, MoH, DIA, NZSIS	Risk reduction and prevention involves a broad and important spectrum of activity. At one end of the risk reduction spectrum, it includes social programmes and initiatives that strengthen social inclusion (and will also support the country's ability to recover from a terrorist attack). At the other end, it includes interventions, monitoring and disengagement activity in relation to specific individuals of concern to authorities or communities.
Precautionary measures	Address vulnerabilities	Customs, MBIE, NZ Police, CAA, MoT, DPMC, NZSIS, CTAG, private sector	New Zealand has in place a range of precautionary measures and activities intended to protect the public through strengthening potential vulnerabilities or ensuring the integrity of critical systems. Often, these measures and activities involve in the flow of people and goods. These activities include major event planning and risk management, aviation security measures, pre-border screenings, immigration vetting.
Disruption and law enforcement	Disrupt extremist activity	NZ Police, NZSIS, DIA, MoJ, MFAT, Customs	New Zealand agencies engage in legal, operational policy and security activities that target specific terrorist and violent extremist threats. These activities range from the designation of terrorist groups and the administration of terrorism-related legislation, to the disruption of extremist propaganda channels, operational investigations and plot disruption, through to terrorism-related criminal prosecutions.
Planning and training	Be ready to respond	NZ Police, DPMC, NZSIS, NZDF, MoD, MFAT, Customs, CAA, MoT	In addition to efforts to reduce and disrupt the terrorism threat, there's ongoing activity focused on ensuring agencies are prepared to respond to a terrorism incident. This includes tactical response planning, training and exercising.

COUNTER-TERRORISM SYSTEM ENABLERS

The effectiveness of New Zealand's counter-terrorism activities depends on the strength of key enablers.

- **Governance and coordination**

The cross-agency, international and domestic nature of terrorism and counter-terrorism activities heightens the need for good governance and coordination at strategic and operational levels of risk management.

- **Information, intelligence, awareness**

Comprehensive understanding of the threat environment, the ability to identify specific threats and disrupt extremist activity depends heavily on quality information, intelligence and the ability to assess it. Knowledge and expertise is also especially important to risk reduction activity, including the effectiveness of different approaches overseas and within New Zealand.

- **Relationships and partnerships**

New Zealand relies on relationships and strong networks across almost every aspect of the counter-terrorism effort. We require relationships with partners and the international community to get threat intelligence and participate effectively in international efforts. On the domestic front, strong relationships across government agencies, trusted relationships with community groups (and private sector organisations) enable much more effective risk identification, risk reduction and precautionary activity.

- **Legislative frameworks**

Many of the risk mitigation activities necessary for dealing with terrorist threats rely on legislative powers and mandate. This includes efforts to disrupt terrorist financial channels, contain the travel of foreign fighters, monitor high-risk individuals, disrupt plots and effectively prosecute terrorist offences.

- **Capability and preparedness**

The appropriate mix and level of capability to deliver effective counter-terrorism activities will change as the threat environment changes, including our ability to implement successful risk-reduction activities, provide timely intelligence and investigate. Our ability to respond successfully to a terrorist attack will be enhanced if we can instil a constant state of readiness.

System organisation and governance

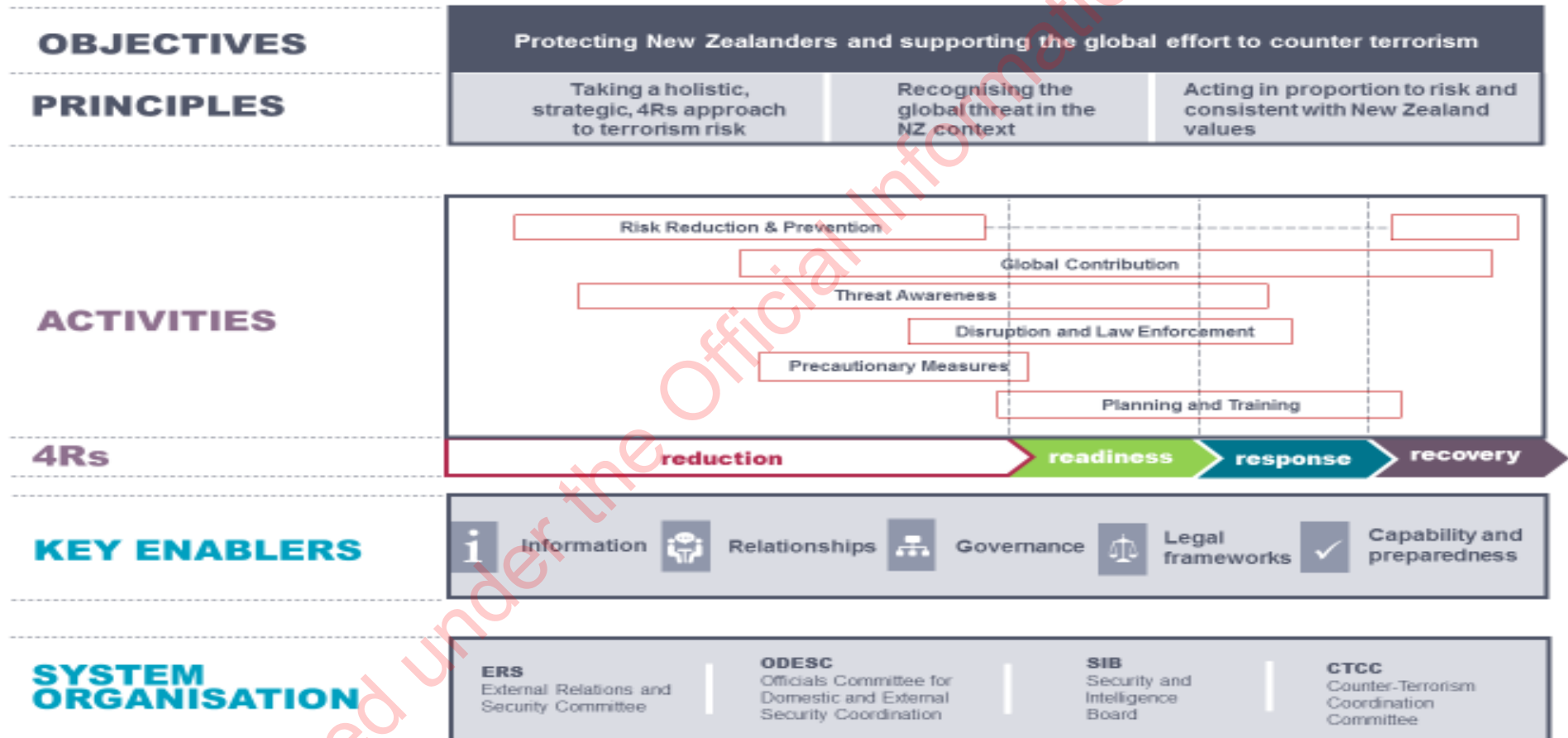
There are many agencies that contribute to New Zealand's counter-terrorism effort. Some agencies perform relatively narrow roles, while others, such as NZ Police, undertake activities right across the counter-terrorism system.

Operational coordination is a critical requirement of much counter-terrorism activity. It happens on a business-as-usual, daily basis – whether at the border (in relation to our international effort), pursuing investigations or engaging with communities.

NATIONAL SECURITY SYSTEM

- The **External Relations and Security Committee (ERS)** sits at the peak of the system. ERS has oversight of the national intelligence and security sector, including policy and legislative proposals relating to the sector. It's made up of key ministers, including the Prime Minister.
- The **ODESC** national security system sits across the inter-agency counter-terrorism arrangements and multi-agency activity. ODESC is responsible for national security governance, risk management and operational coordination in relation to significant events or operations. This system operates at several levels. (Refer to the *National Security System handbook* for more detail.)
- The **Security and Intelligence Board (SIB)** supports ERS. The board builds a high performing, cohesive and effective security and intelligence sector. SIB focuses on external threats and intelligence issues, including terrorism. It's made up of chief executives from a number of agencies and chaired by the Deputy Secretary, Security and Intelligence, Department of the Prime Minister and Cabinet.
- The **Counter-Terrorism Coordination Committee** reports to SIB. The committee coordinates and risk manages counter-terrorism activity, specifically the counter-terrorism system. Various cross-agency groups are also involved in coordination at an operational level.

Strategic Framework Overview





ODESC

*Officials' Committee for Domestic
and External Security Coordination*

Counter-Terrorism Coordination Committee

ctcc@dpmc.govt.nz

Countering Terrorism and Violent Extremism

System Capability Review

Paper 1: Capability landscape and development opportunity themes

June 2020

Contents

Executive summary.....	3
1 Introduction	4
1.1 Purpose.....	4
1.2 Approach.....	4
2 Capability landscape	5
2.1 Modelling approach	5
2.2 Capability landscape.....	6
3 Opportunity themes.....	7
3.1 Public communication and engagement.....	7
3.2 Inter-agency collaboration	9
3.3 Workforce development.....	10
3.4 Information access and sharing.....	11
4 Next steps	13
Annex 1 : System context	14
Annex 2 : Capability descriptions	16

Figures

Figure 1: Updated stage approach.....	4
Figure 2: Capability-strategy relationship.....	5
Figure 3: CT / CVE system capability landscape.....	6
Figure 4: Candidate next steps.....	13
Figure 5: CT system governance.....	14
Figure 6: Risk reduction-focused strategy.....	15

Executive summary

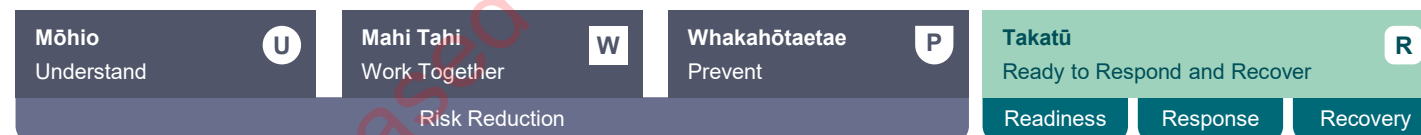
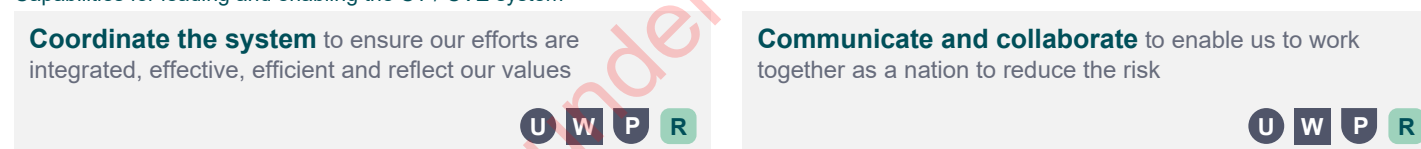
'Business capabilities' are expressions of what organisations must be able to do in order to implement their strategies and deliver target outcomes. This paper presents a system view comprising 9 headline and 37 second-order capabilities, then proposes areas for further investigation and evaluation.

Capability landscape – headline level

Core capabilities for countering terrorism and violent extremism



Capabilities for leading and enabling the CT / CVE system



Development opportunities

Strengthening shared foundations

- What **Better connect information, expertise and effort**, both within government and more widely...
- How ...through **increasing engagement, understanding and collaboration**...
- Why **...to enhance the inclusiveness and effectiveness of our work to protect our communities from terrorism and violent extremism**

Key opportunity themes:

- stakeholder relationship management
- public communication
- capability management and joint ventures
- threat assessment, discovery and investigation
- community understanding and representation in the workforce
- workforce CT / CVE awareness
- information access and sharing

Next steps

Apply a structured approach to evaluate existing capabilities and the nature of challenges, then set out development objectives (3-4 year horizon).

1 Introduction

1.1 Purpose

The Counter-Terrorism System Capability Review ('the review') was commissioned to provide the Counter-Terrorism Coordination Committee (CTCC) with:

- a high-level view of system capabilities for countering terrorism and violent extremism (CT / CVE)¹
- options for enhancing those capabilities.

The review's objectives are to:

- support the CTCC to ensure CT / CVE capabilities across government are integrated, effective, efficient and reflect New Zealand's values
- inform the CTCC's response to the findings of the Royal Commission of Inquiry into the Attack on Christchurch Mosques^[2]
- inform future versions of the CTCC's annual work programme
- potentially, provide agencies with information to support the development of investment cases and Budget bids, in particular to demonstrate alignment to system priorities.

This paper presents a system view of capabilities and proposes candidates for development.

It has been kept at the RESTRICTED level to facilitate sharing. In some areas this has meant limiting the amount of detail presented.

Further context is provided in Annex 1.

¹ Terrorism and violent extremism are not conflated here. Terms are linked because the capabilities required to counter them are essentially the same.

1.2 Approach

The review began in February 2020. A structured approach was adopted to help ensure a balanced range of views is represented, including those of agencies not traditionally seen as central to countering terrorism and violent extremism.

Progress was disrupted by the Covid-19 lockdown, ongoing challenges in engaging with agency representatives who were working on Covid response, and the second extension of the time available for the Royal Commission of Inquiry. In response, consultation was limited to agency representatives and the approach was adjusted to refocus this stage and paper on:

- developing, for the first time, a shared view across all capabilities required to counter terrorism and violent extremism
- identifying shared priorities for development.

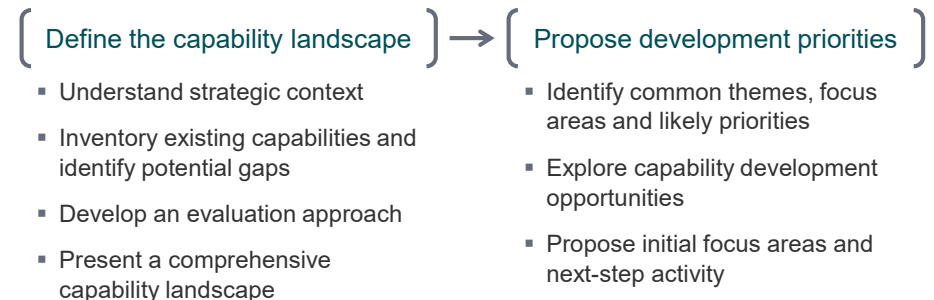


Figure 1: Updated stage approach.

A working group representing a subset of CTCC and social sector agencies was convened to support opportunity identification.

^[2] christchurchattack.royalcommission.nz

2 Capability landscape

The model presented in this section is designed to inform system-level decisions on capability investment and management, both now and into the future.

2.1 Modelling approach

‘Business capabilities’ are expressions of what^[3] organisations must be able to do to implement their strategies and deliver target outcomes. They may be:

- deployed individually or in combination to fulfil business functions
- defined to multiple levels of detail. Modelling in this paper is limited to two tiers so as to maintain its focus at the system level.

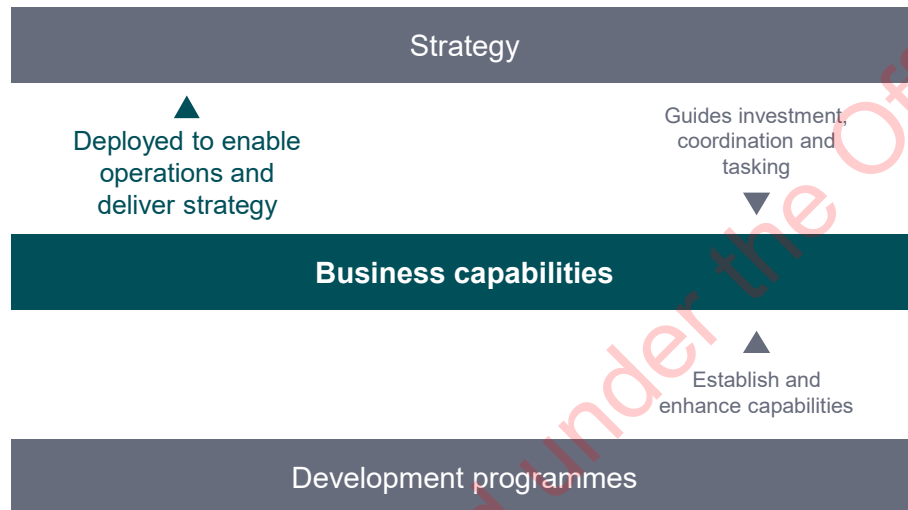


Figure 2: Capability-strategy relationship.

^[3] Rather than *how* functions are delivered.

In order to deliver value successfully and sustainably, capabilities:

- require a well-understood stakeholder and ‘customer’ base that is effectively supported to derive value from them
- must be comprehensive and coherent, effectively integrating people, competencies, processes, information, technology, facilities, equipment and other resources
- should be operated by the parties best placed and most appropriate to deliver them
- require active governance and coordination.

Capability modelling is an appropriate approach for establishing a system-level view of CT / CVE activity as capability-based design:

- recognises capabilities may be deployed for different purposes at different times, supporting agencies to be flexible to respond to evolving priorities in line with New Zealand’s ‘all hazards, all risks’ approach to national security risk management
- supports capability sharing in a range of forms and degrees of formality
- facilitates the identification of opportunities and priorities for enhancement, including where partners can assist each other.

The modelling approach aligns to commonly accepted standards for business capability architecture, with some adjustments to support shared understanding across the range of agencies working in different parts of the system. These include:

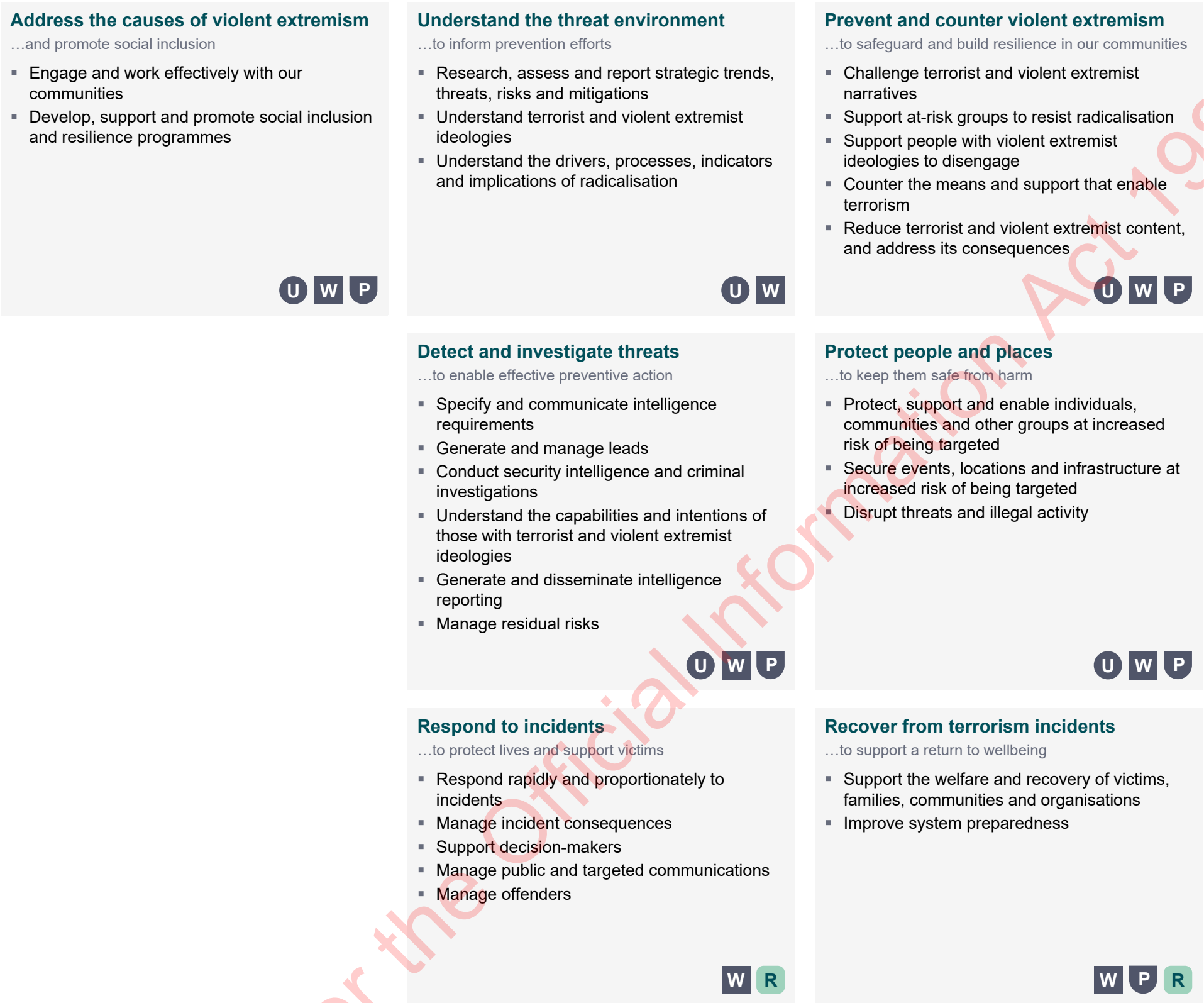
- emphasising the use of plain-English, objective-focused labelling
- allowing repetition to support clarity.

2.2 Capability landscape

Figure 3 presents the proposed system capability model. Each component is described further in Annex 2.

Core capabilities: Countering terrorism and violent extremism

We have capabilities to...



Enabling capabilities: Leading and enabling the CT / CVE system

We have capabilities to...

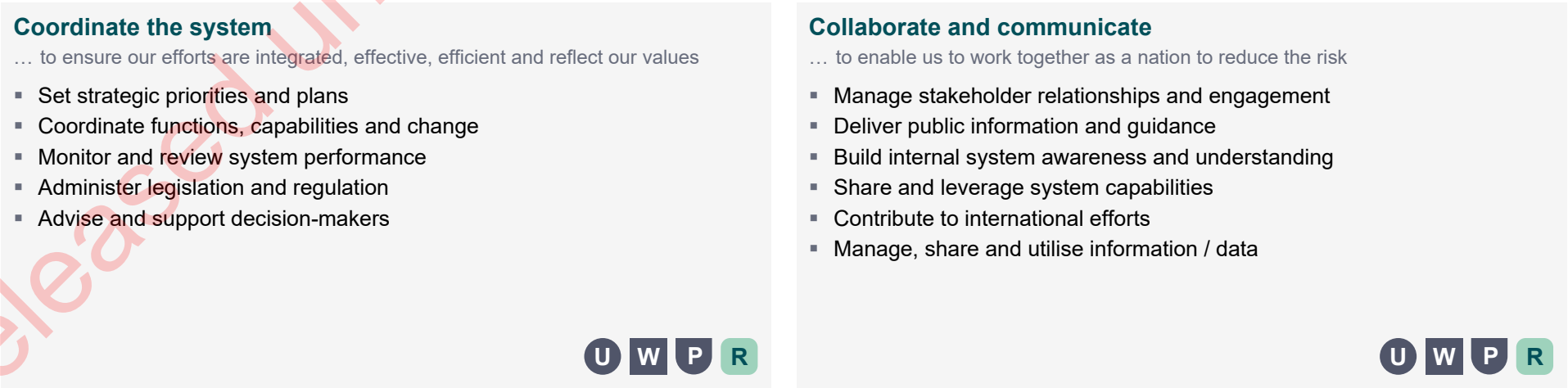
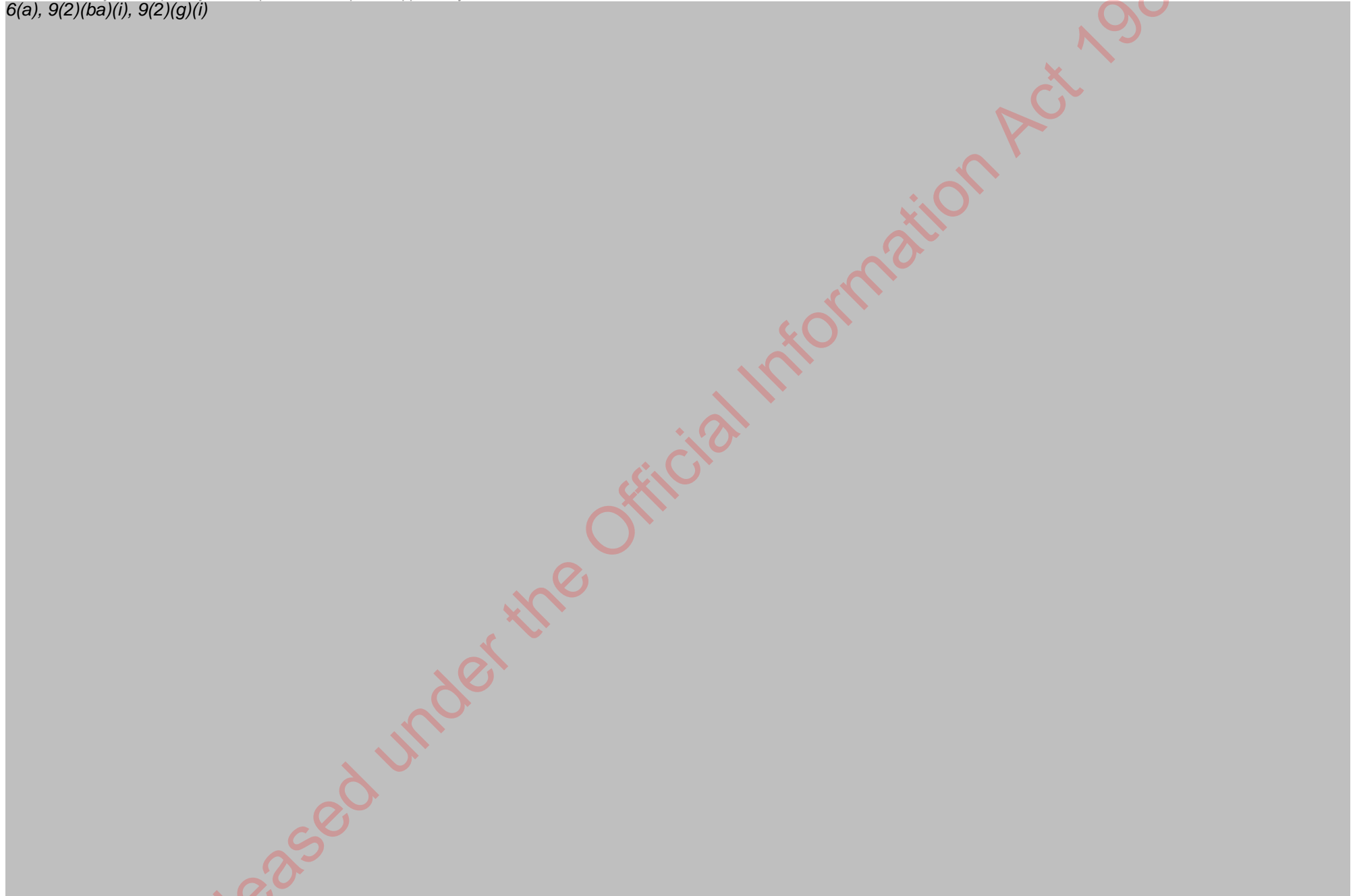


Figure 3: CT / CVE system capability landscape.

CT / CVE system capability landscape and development opportunity themes
6(a), 9(2)(ba)(i), 9(2)(g)(i)

Released under the Official Information Act 1982

CT / CVE system capability landscape and development opportunity themes
6(a), 9(2)(ba)(i), 9(2)(g)(i)

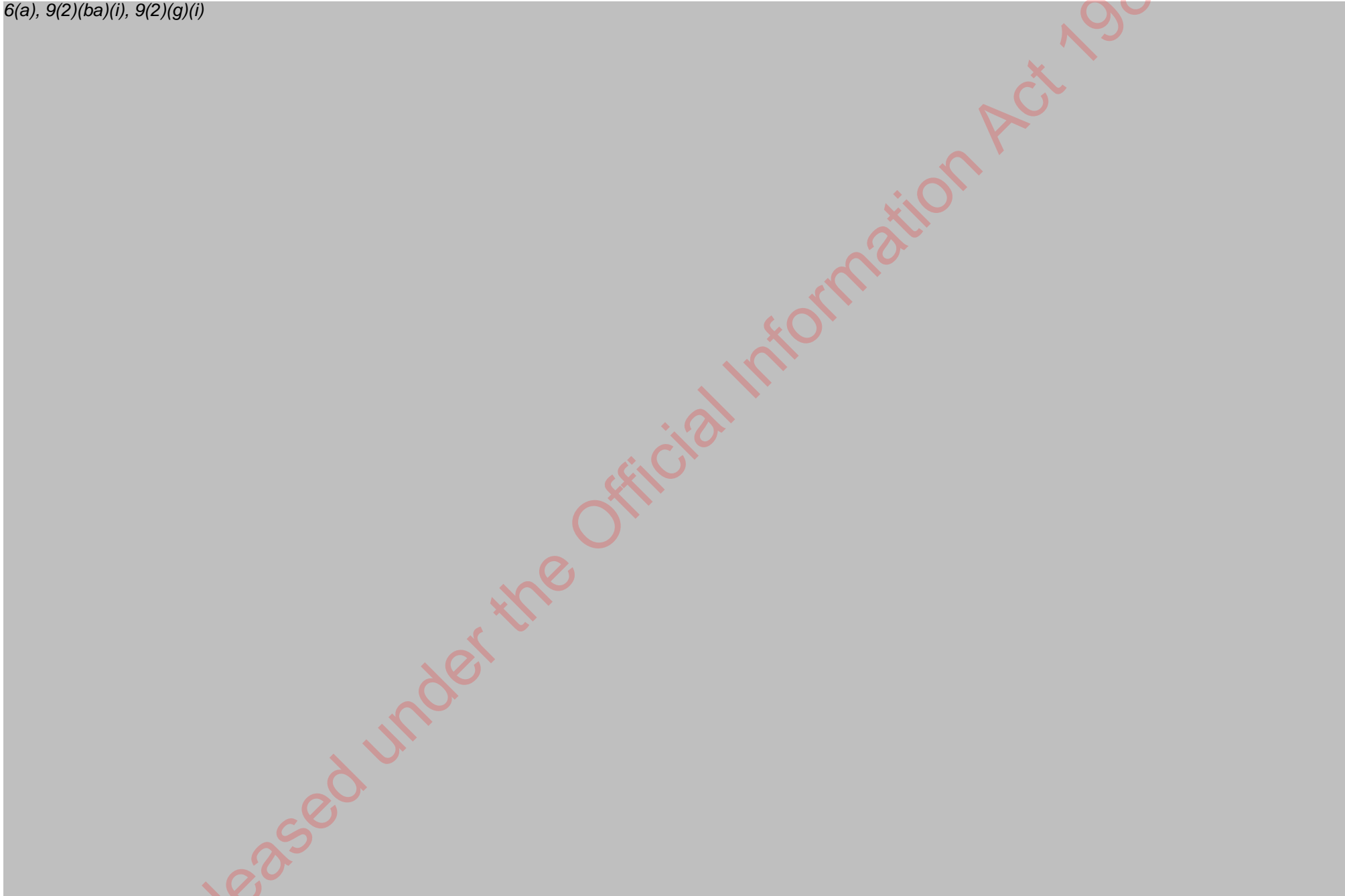


CT / CVE system capability landscape and development opportunity themes
6(a), 9(2)(ba)(i), 9(2)(g)(i)

Released under the Official Information Act 1982

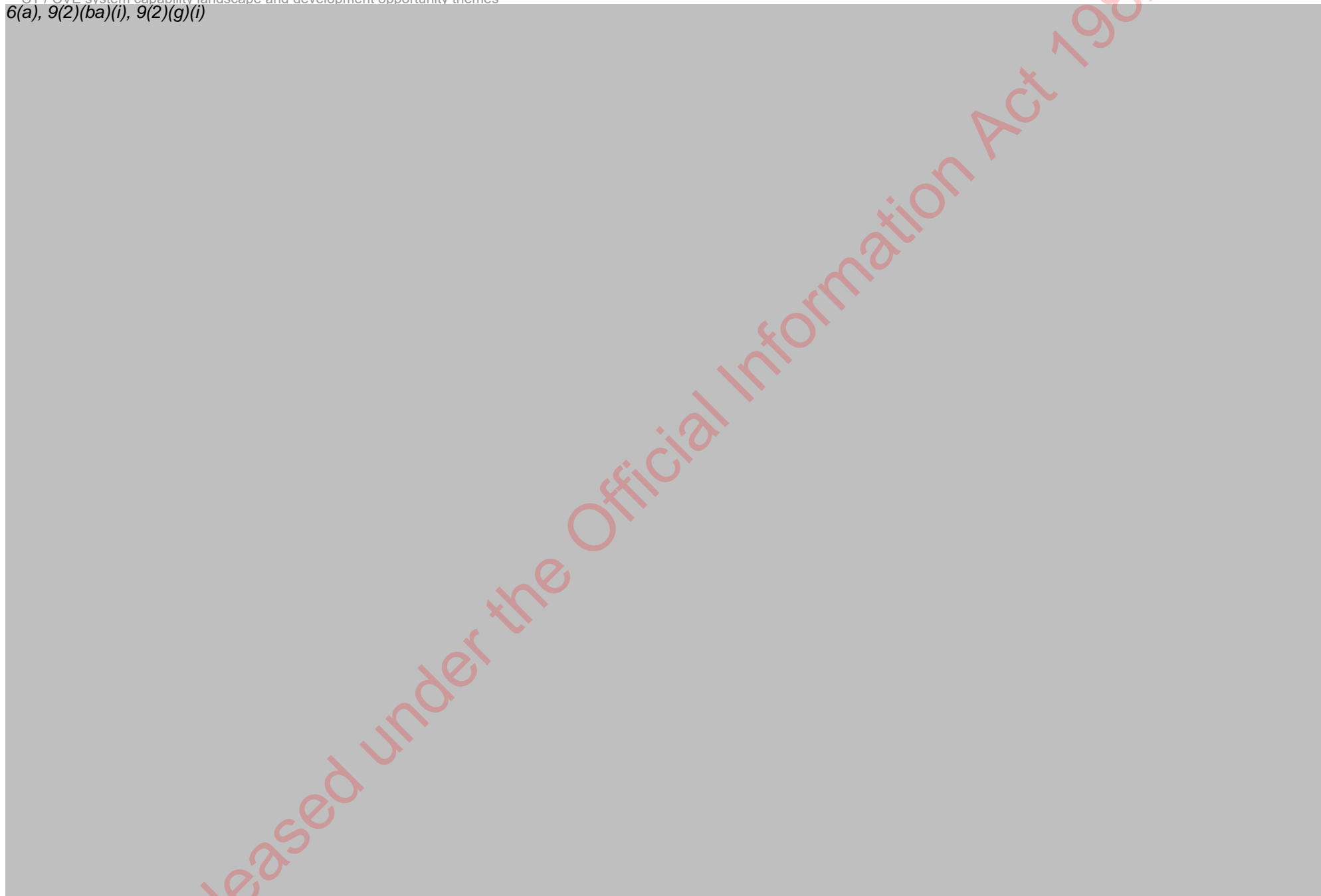
CT / CVE system capability landscape and development opportunity themes

6(a), 9(2)(ba)(i), 9(2)(g)(i)




CT / CVE system capability landscape and development opportunity themes

6(a), 9(2)(ba)(i), 9(2)(g)(i)

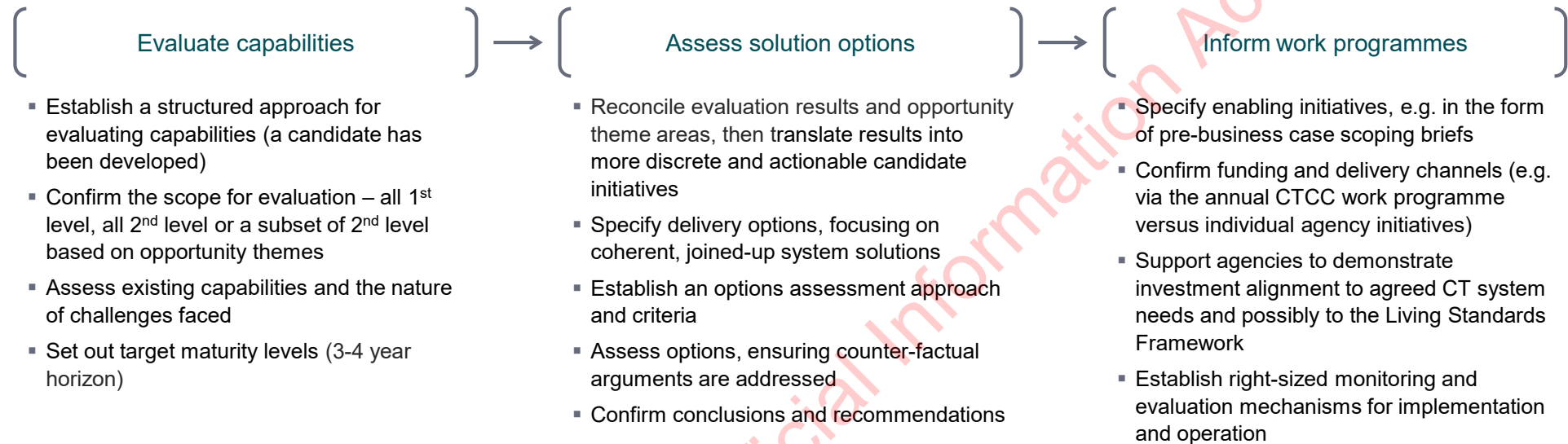


CT / CVE system capability landscape and development opportunity themes

6(a), 9(2)(ba)(i), 9(2)(g)(i)



4 Next steps



When evaluating capabilities and options consider...

Oversight responsibilities

Who needs to be involved and supported in governance and oversight? Who is responsible for day-to-day leadership across system components? Are mandates and role boundaries clear? How (and how well) does the authorising environment work?

Key relationships

What partners, suppliers and other parties are needed to make the capability work?
What activities do they perform?

Key activities

What enabling and supporting activities must be performed?

Key resources

What competencies and capacity do we need to possess or have access to?
What are our most important process, infrastructure, tool and resource needs?
How do we source other resources?

Core functions

What key functions must be performed to create value and achieve target objectives and outcomes?

Goals

What are our system objectives and outcomes?
Who benefits from functions? What are their needs?

How do we package capabilities and services?

What channels do we use to reach people?

How do we maintain relationships, including to understand needs?

Operating responsibilities

Who has responsibility for day-to-day operational activity? What other parties have related responsibilities? What agreements are required? How will responsibilities be integrated?

Figure 4: Candidate next steps.

Annex 1: System context

National security system

New Zealand takes an 'all hazards, all risks' approach to managing all types of national security risks. Known as the 4Rs, this approach encompasses:

- **Reduction.** Identifying and analysing long-term risks and taking steps to eliminate them if possible, or if not, to reduce their likelihood and the magnitude of their impact.
- **Readiness.** Building operational response systems and capabilities before an emergency happens.
- **Response.** Taking action immediately before, during or directly after a significant event.
- **Recovery.** Using coordinated efforts and processes to bring about immediate, medium-term and long-term regeneration.

Relevant integrated control frameworks include the:

- **Coordinated Incident Management System.** New Zealand's modular framework of principles, structures, functions, processes and terms for coordinating and controlling the response to natural disasters and other emergencies of any scale.^[6]
- **National Security System Handbook.** Sets out arrangements regarding the governance of national security and for responding to a potential, emerging or actual national security crisis.^[7]
- **Counter-Terrorism Handbook.** Guides the initial 'response' phase following a terrorism incident.^[8]

Cabinet's **External Relations and Security Committee** (ERS) oversees the national intelligence and security sector.

The **Officials' Committee for Domestic and External Security Coordination** (ODESC) is responsible for governance, risk management and operational coordination of national security in its broad sense.

The ODESC **Security and Intelligence Board** (SIB) supports the ERS, working to build a cohesive and effective security and intelligence sector.

The SIB's **Counter-Terrorism Coordination Committee** coordinates and risk manages CT / CVE activity, primarily through:^[9]

- supporting strategic CT decision-making and action
- coordinating and driving inter-agency CT work, particularly through the national CT work programme.

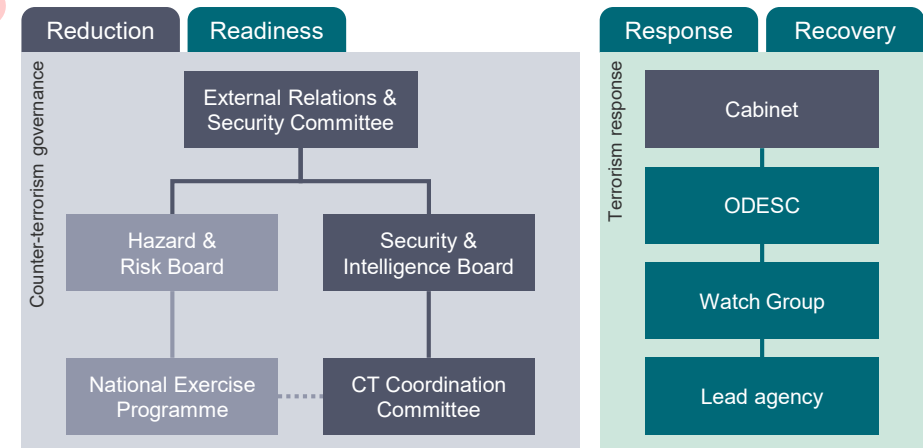


Figure 5: CT system governance.

^[6] *Coordinated Incident Management System*, 3rd Edition, NEMA, August 2019, UNCLASSIFIED.

^[7] *National Security System Handbook*, DPMC, August 2016, UNCLASSIFIED.

^[8] *Counter-Terrorism Handbook*, DPMC, October 2019, RESTRICTED

^[9] *Counter-Terrorism Coordination Committee Terms of Reference*, October 2019, IN-CONFIDENCE.

National counter-terrorism strategy

The national counter-terrorism strategy^[10] and supporting work programme emphasise threat reduction whilst also preparing for incident response.



Figure 6: Risk reduction-focused strategy.

A range of traditional (e.g. law enforcement, security intelligence, safety regulators) and non-traditional agencies (including from the social, health and education sectors) are partnering to deliver the strategy.

^[10] *Countering Terrorism and Violent Extremism: National Strategy Overview*, September 2019, UNCLASSIFIED.

Annex 2: Capability descriptions

The descriptions presented here were developed to:

- help clarify capability scope and boundaries (they are illustrative and not necessarily complete)
- inform ongoing evaluation and prioritisation.

Core capabilities

Seven core capability areas are presented. The first – *address the causes of violent extremism* – includes capabilities most often led by agencies in the social sector (though not always – for instance the NZ Police is active in this space). While CT / CVE benefits should accrue from work in this area, they will often be secondary to other social outcomes being sought and may not be made explicit. The remaining six areas are more often deployed directly towards countering terrorism and violent extremism.

Address the causes of violent extremism

Engage and work effectively with our communities

The ability to (see also page 22):

- understand community views, needs and expectations of government and the CT / CVE system
- build and maintain social licence to operate in this often sensitive domain, including through being seen to deliver on commitments
- provide communities with the information they need to engage with the system, and support them to do so
- maintain the trust and confidence required for individuals and communities to feel safe and willing to proactively engage with agencies, for example when they observe concerning behaviours.

Develop, support and promote social inclusion and resilience programmes

The ability to identify, develop, deliver, evaluate and / or support (e.g. through funding) social inclusion and community resilience initiatives that will help address causes of violent extremism, including through:

- fostering recognition, acceptance, participation and positive interactions
- addressing prejudice, unfairness and discrimination.

Understand the threat environment

Research, assess and report strategic trends, threats, risks and mitigations

The ability to:

- develop, maintain, evaluate and share baseline views of the terrorism and violent extremism threat-scape both within and relevant to New Zealand
- plan, direct and conduct strategic CT / CVE analyses, including of historic cases and outcomes to help inform future investigation targeting
- research and forecast 'over the horizon' threat sources and vectors before they manifest
- identify, assess, reassess and communicate threat types and their implications as they emerge over time
- research, develop and share information on effective counter-measures
- explore and review information requirements to support the above
- effectively manage risk frameworks, individual risks, and associated communication and effort integration
- provide threat and risk assurance information.

Understand terrorist and violent extremist ideologies

The ability to identify and assess existing, emerging and evolving ideologies. This includes understanding ideological 'cultural' elements such as sources of inspiration, phraseology, symbology and modes of dress.

Understand the drivers, processes, indicators and implications of radicalisation

The ability to inform threat and risk management through understanding:

- behavioural and other indicators associated with violent extremism
- motivations and pathways to radicalisation and mobilisation
- links between radicalisation risk and potentially related vulnerability factors, for example mental illness
- the practical implications of offshore influences on radicalisation
- relationships between crime, criminal relationships and violent extremism.

Prevent and counter violent extremism

Challenge terrorist and violent extremist narratives

The ability to work with, within and on behalf of communities to challenge terrorist and violent extremist ideologies and hate speech (links to the capability to eliminate relevant objectionable content – see page 18), and to promote social inclusiveness.

This includes the ability to identify, develop and utilise appropriate communication content, channels and spokespeople (links to enabling communications management capabilities – see page 22).

Support at-risk groups to resist radicalisation

The ability to identify, educate and support individuals and groups who may be vulnerable to self-radicalisation or targeted for recruitment by terrorist or violent extremist groups. This includes the ability to:

- identify, design and implement effective resilience support mechanisms in cooperation with communities
- manage the risk of inadvertent alienation and / or stigmatisation.

Support people with violent extremist ideologies to disengage

The ability to identify, design and apply appropriate tailored interventions and case management to support the disengagement, rehabilitation and community reintegration of individuals known to follow extremist ideologies. This includes the ability to assess the nature and degree of risk posed by such individuals (links to the ability to conduct investigations – see page 18).

Counter the means and support that enable terrorism

The ability to detect and neutralise access to mechanisms, training and materiel enabling terrorism, for example through anti-money laundering controls, border controls and firearm access controls.

This includes the ability to:

- identify and formally designate terrorist entities to enable the criminalisation and disruption / suppression of recruitment, participation and support activities, including in accordance with foreign policy and international obligations
- administer and disseminate designation information
- exercise powers pursuant to the formal designation of terrorist entities.

Reduce terrorist and violent extremist content, and address its consequences

The ability to identify, detect and prevent the dissemination of, or otherwise limit exposure to, objectionable material relevant to terrorism and violent extremism.

The ability to identify and evaluate actual and anticipated consequences of hate speech and violent extremist content, then to design, apply and evaluate interventions to address those consequences (may link to social inclusion and resilience programmes – see page 16).

This may also include supporting activities such as liaison, monitoring, assessment, case management and enforcement.

Detect and investigate threats

Specify and communicate intelligence requirements

The ability to identify, prioritise and communicate clear and actionable requirements that drive and inform criminal and security intelligence discovery, investigation and analysis.

Generate and manage leads

The ability to effectively generate, record and triage enquiry and lead information:

- proactively, e.g. through focused discovery initiatives
- reactively, e.g. as a result of border screening, reporting by the public, or reporting by partner agencies (domestic or international)
- on a 24*7 basis when necessary, e.g. due to international travel or in reaction to social media activity suggesting an attack is imminent.

This includes, or will be dependent on, supporting capabilities to:

- develop lead source channels and triggers (links to collaboration and communication capabilities – see page 22)
- source, manage and analyse information, including complex datasets (see page 23).

Conduct security intelligence and criminal investigations

The ability to manage full investigation lifecycles from lead development, prioritisation and tasking through to reporting and potential handover for disruption and / or prosecution – all in a timely and efficient manner. This includes supporting capabilities such as:

- overt and covert information and evidence collection methods, e.g. observation, liaison, interviewing, surveillance, technical operations, online operations, forensics, research and more
- processing, analysis and decision-making – including in specialist domains such as financial intelligence
- case management and record-keeping
- compliance monitoring and management.

Understand the capabilities and intentions of those with terrorist and violent extremist ideologies

The ability to evaluate and report on the influences, capabilities, motivations and intentions of individuals and groups identified as following or espousing terrorist or violent extremist ideologies. This includes threats within New Zealand and threats to New Zealanders and New Zealand's interests overseas.

Generate and disseminate intelligence reporting

The ability to generate and deliver reporting that:

- has impact, i.e. it meets well-understood audience needs and is clear and actionable
- is timely and delivered via appropriate channels to all those with a valid need-to-know – this includes the ability to generate and disseminate threat warnings on a 24*7 basis when necessary
- is appropriately access controlled.

Manage residual risks

The ability to ensure individuals and groups assessed as being of interest / concern are not permanently 'forgotten' once an investigation is complete, including through maintaining records and incorporating appropriate triggers to inform future lead discovery work – all within the bounds of legislation and policy governing the retention and management of historic / closed records.

The ability to ensure residual risk management is well integrated with wider CT / CVE threat and risk management (see page 16).

Protect people and places

Protect, support and enable individuals, communities and other groups at increased risk of being targeted

The ability to:

- understand who may be at increased risk domestically and offshore, including through ensuring there are effective channels for managing incoming information
- develop and issue relevant advice, guidance and direct interventions (e.g. funding community-led initiatives) through appropriate channels and with understanding of audiences and their needs (see page 22)

- provide protective security measures when it is appropriate to do so directly
- review and adjust protective measures over time.

Secure events, locations and infrastructure at increased risk of being targeted

The ability to mitigate risk through identifying, assessing, prioritising and addressing factors making events, places and infrastructure (physical and digital) vulnerable to, and / or targets for, attack. Examples include crowded places, major events, transport systems, utilities and border control spaces.

This includes the ability to collaborate and share vulnerability and response information with all parties having protective security responsibilities, including those in the community and private sectors.

Disrupt threats and illegal activity

The ability to perform law and regulatory enforcement activities, e.g.:

- monitoring and enforcing compliance, e.g. with control orders
- issuing warnings
- exercising statutory powers of detention and arrest
- disrupting and prosecuting criminal activities, e.g. relevant acts of preparation, planning, recruitment, participation in a terrorist group (including international travel in order to participate) financing terrorism, etc.

This capability is closely related to the countering of means and support for terrorism (see page 17) and the elimination of objectionable material (page 18).

Respond to incidents

Respond rapidly and proportionately to incidents

The ability to effectively sustain an agreed level of capacity and readiness to respond to suspected or known terrorist attacks how, when, where and at the scale required. This includes testing plans and demonstrating preparedness through inter-agency personnel mobility (supporting surge capacity), scenario planning, cross-training and exercises (links to system monitoring – see page 21).

The ability to immediately respond to a terrorism incident in one or more locations in order to:

- preserve life and safety
- develop situational awareness
- prevent escalation, neutralise threats and apprehend offenders
- contain situations, e.g. via evacuation, fire management, hazardous material identification and neutralisation, location security, tightened border controls...

This includes the ability to rapidly assess needs, to structure, manage and integrate a response, and to equip and scale it up as required.

Manage incident consequences

The ability to understand and manage the immediate consequences of an incident, possibly while elements of the initial response continue. This may include, for example, the ability to:

- treat and / or identify victims
- extend physical security measures
- address the risk of follow-up, copycat and / or revenge attacks
- restore essential services and ensure their continuity
- shelter, feed and support displaced people (welfare management, logistics management)
- provide support to New Zealanders overseas

- coordinate offers or requests for international support
- inform and support foreign missions to fulfil their obligations to their nationals affected by an incident in New Zealand.

Support decision-makers

The ability to provide information, advice and support that enables right-sized governance and oversight of the response to an incident, including in accordance with the Coordinated Incident Management System, National Security System and National CT Handbook as applicable.

Manage public and targeted communications

The ability to, in a timely fashion:

- coordinate the provision of appropriate and clear information and safety messages to the public through suitable channels
- identify, engage and communicate with groups requiring additional information and support, in particular those targeted by an attack
- monitor media activity and liaise with media organisations
- monitor and manage communications through diplomatic channels and international media.

Manage offenders

The ability to:

- build and prosecute criminal cases (links to the ability to conduct investigations – see page 18)
- manage suspects in custody and monitor those released subject to conditions.

Recover from terrorism incidents

Support the welfare and recovery of victims, families, communities and organisations

The ability to understand the needs of affected individuals, communities and organisations, and to work appropriately with and for them, in order to:

- support them to navigate the aftermath of an incident
- address longer-term physical, psychological, social, financial, economic and / or environmental consequences.

Effective support should also prevent further victimisation and / or address the risk of survivors themselves becoming radicalised.

Improve system preparedness

The ability to review and apply experience to improve the CT / CVE system. This includes ensuring learnings inform policies, processes, doctrine, education, incident readiness (see page 20) and future system reviews (see below).

Enabling capabilities

Enabling capabilities are foundational. They may be deployed to manage the system or in support of any core capability.

Coordinate the system

Set strategic priorities and plans

The ability to develop, test, consult on, approve, report and evaluate strategic priorities, risk thresholds and plans (e.g. incident response and recovery plans) across the CT / CVE system.

Coordinate functions, capabilities and change

The ability to:

- plan, coordinate and integrate functions and capabilities at the system level
- agree how agencies will work together and with community groups and other organisations to manage prevention, protection and response work appropriately and effectively
- define, agree, communicate and operationally manage agency responsibility boundaries and transition / handover points
- collectively set expectations and share information between agencies on an ongoing basis to help manage the risk activities come into conflict or that capabilities are unnecessarily duplicated
- identify inter-organisational and international collaboration, secondment and training / cross-training needs and opportunities (links to shared capability operation – see page 23)
- plan, deliver and integrate new capabilities and capability enhancements, both through incremental improvement and more substantial / structured change initiatives
- ensure system-level coordination is right-sized and does not impose unnecessary overheads on agencies.

Monitor and review system performance

The ability to:

- specify, track and report appropriate success criteria and assurance information
- inform and support oversight bodies
- plan, run and review exercises (links to maintaining response readiness – see page 20)
- translate learnings into system improvements.

Administer legislation and regulation

This includes the implementation and proactive stewardship of legislative and regulatory frameworks to provide assurance they uphold the rule of law, remain fit-for-purpose and are consistent with democratic rights and freedoms.

Advise and support decision-makers

The ability to provide policy, legal and technical advice that is timely, evidence-based and of high quality. This includes ensuring there is consistency with:

- the Treaty of Waitangi
- human rights, criminal justice and cyber security policy
- New Zealand's international obligations.

Collaborate and communicate

Manage stakeholder relationships and engagement

The ability to:

- identify, develop and manage enduring and effective domestic and international partnerships and stakeholder relationships across the public (central and local government), community, academic and private sectors
- understand stakeholder information and support needs
- understand how stakeholders may contribute to countering terrorism and violent extremism, including parties not traditionally seen as working in this domain
- establish and manage formal agreements where these are appropriate
- effectively and sustainably coordinate engagement and consultation, demonstrating openness, accountability and system integration.

Deliver public information and guidance

The ability to sustainably identify, develop and deliver (through appropriate channels, including via third parties) appropriate audience-specific and public communications and guidance regarding, for example (not limited to):

- the domestic and international threat environment
- how to stay safe
- how to respond to incidents
- accessing assistance
- recognising signs of radicalisation
- how to report concerns
- protective security obligations and solutions, including educating people for whom parties have a duty of care.

Build internal system awareness and understanding

The ability to ensure agencies possess the awareness and capability (including cultural and diversity competencies and representation) required to:

- design and deliver public services that are inclusive, respectful, relevant to community needs, informed by Te Tiriti o Waitangi, and reflect New Zealand's values
- work sensitively and effectively with and on behalf of communities, for example (not limited to) ethnic, faith and LGBTQI+ communities
- build baseline understanding of CT / CVE issues within the government workforce.

Share and leverage system capabilities

The ability to:

- share knowledge of agency capabilities that may be made available to others
- share expertise and resources across the system, including to help meet surge demand
- establish, provision, manage and govern capabilities as shared services when appropriate, to drive system effectiveness and / or efficiency improvements.

Contribute to international efforts

The ability to lead or otherwise meaningfully contribute to international CT / CVE initiatives that align to New Zealand's values, including via:

- engagement, cooperation and advocacy, including through participation in multi-lateral fora
- meeting United Nations reporting requirements
- secondments and deployments
- providing and / or funding capability development programmes.

Manage, share and utilise information / data

The ability to:

- identify information requirements and sources
- secure and manage holdings
- maintain appropriate cross-system awareness of available holdings
- manage appropriate access, collaboration, sharing and transfer within and between domestic and international organisations
- agree and utilise standards to support cross-system understanding and sharing
- link, 'mine' and analyse large and complex datasets.

CT / CVE System Capability Landscape

Core: Countering terrorism and violent extremism

We have capabilities to **address the causes of violent extremism** and promote social inclusion

- Engage and work effectively with our communities
- Develop, support and promote social inclusion and resilience programmes

U W P

We have capabilities to **understand the threat environment**, to inform prevention efforts

- Research, assess and report strategic trends, threats, risks and mitigations
- Understand terrorist and violent extremist ideologies
- Understand the drivers, processes, indicators and implications of radicalisation

U W

We have capabilities to **prevent and counter violent extremism**, to safeguard and build resilience in our communities

- Challenge terrorist and violent extremist narratives
- Support at-risk groups to resist radicalisation
- Support people with violent extremist ideologies to disengage
- Counter the means and support that enable terrorism
- Reduce terrorist and violent extremist content, and address its consequences

U W P

We have capabilities to **detect and investigate threats**, to enable effective preventive action

- Specify and communicate intelligence requirements
- Generate and manage leads
- Conduct security intelligence and criminal investigations
- Understand the capabilities and intentions of those with terrorist and violent extremist ideologies
- Generate and disseminate intelligence reporting
- Manage residual risks

U W P

We have capabilities to **protect people and places**, to keep them safe from harm

- Protect, support and enable individuals, communities and other groups at increased risk of being targeted
- Secure events, locations and infrastructure at increased risk of being targeted
- Disrupt threats and illegal activity

U W P

We have capabilities to **respond to incidents**, to protect lives and support victims

- Respond rapidly and proportionately to incidents
- Manage incident consequences
- Support decision-makers
- Manage public and targeted communications
- Manage offenders

W R

We have capabilities to **recover from terrorism incidents**, to support a return to wellbeing

- Support the welfare and recovery of victims, families, communities and organisations
- Improve system preparedness

W P R

Enabling: Leading and enabling the CT / CVE system

We have capabilities to **coordinate the system**, to ensure our efforts are integrated, effective, efficient and reflect our values

- Set strategic priorities and plans
- Coordinate functions, capabilities and change
- Monitor and review system performance
- Administer legislation and regulation
- Advise and support decision-makers

U W P R

We have capabilities to **collaborate and communicate**, to enable us to work together as a nation to reduce the risk

- Manage stakeholder relationships and engagement
- Deliver public information and guidance
- Build internal system awareness and understanding
- Share and leverage system capabilities
- Contribute to international efforts
- Manage, share and utilise information / data

U W P R

Mōhio
Understand

U



Mahi Tahi
Work Together

W



Whakahōtaetae
Prevent

P



Takatū
Ready to Respond and Recover

R










Readiness

Response

Recovery

Reduction

Counter-Terrorism Work Programme 2021

INITIATIVE	OVERVIEW	LEAD(S)	KEY WORKSTREAMS	RCOI RECS	NEXT KEY MILESTONE
 Increase direct engagement and public communications	<p>Lift capability and increase efforts to work with, within and on behalf of communities. Successful engagement and communication on matters relating to terrorism and violent extremism:</p> <ul style="list-style-type: none"> Helps agencies build the trust and confidence that underpins our social licence to operate in often highly sensitive situations. Increases public understanding of the nature of threats and what people can do to protect themselves and others. 	<p>DPMC to lead strategic approach.</p> <p>CTCC agencies to lead public engagement and communication.</p>	<ul style="list-style-type: none"> RCOI engagement (DPMC) Advisory Group on CT (DPMC) Publish indicators and risk factors (NZSIS) National Centre of Excellence (DPMC) Coordinated public information (DPMC) Annual CT Hui (DPMC) 	<p>-</p> <p>Rec 7</p> <p>Rec 13</p> <p>Rec 14</p> <p>Rec 15</p> <p>Rec 16</p>	9(2)(f)(iv)
 Enhance stewardship of the CT / CVE system	<p>Expand capability coordination and outcomes management:</p> <ul style="list-style-type: none"> Enhance the identification, coordination and deployment of capabilities across the system to support efficient use of what are often specialist competencies and limited resources. Extend the CTCC work programme's Learning System workstream (including extending CT exercise programmes) to enhance system testing, reflection and lesson management. 	DPMC to lead, through CTCC.	<ul style="list-style-type: none"> New Intelligence and Security Agency (DPMC) Clearer system roles and responsibilities (DPMC) 	<p>Rec 2</p> <p>-</p>	
 Grow workforce awareness and diversity	<p>Continue and expand work to:</p> <ul style="list-style-type: none"> Build baseline understanding of CT / CVE issues within the wider public sector, and depth of CT expertise across the workforce. Support and promote diversity, inclusion and cultural awareness within the national security workforce. 	DPMC to lead, with diversity aspects led through National Security Workforce (NSW) programme.	<ul style="list-style-type: none"> Grow workforce CT awareness (<i>TBD</i>) Papa Pounamu (PSC) NSW Programme (DPMC) 	<p>Rec 9</p> <p>Rec 33 & 34</p> <p>-</p>	
 Enhance threat discovery and assessment	<p>Expand capabilities and integration to:</p> <ul style="list-style-type: none"> Assess and communicate the CT / CVE threatscape and associated vulnerabilities. Generate and investigate 'high quality' leads. 	NZSIS / CTAG to lead.	<ul style="list-style-type: none"> Threat discovery and leads (NZSIS) Joint online threat discovery (NZSIS) Single accessible reporting system (NZP) Te Raranga (NZP) 	<p>-</p> <p>-</p> <p>Rec 12</p> <p>Rec 42</p>	
 Enhance information access, sharing and analysis	<p>Enhance access to information to support threat identification and assessment, the provision of protective security advice, and the evidence used to inform investigations and interventions.</p> <p>[This initiative is significantly broader than CT / CVE. It encompasses aspects across the national security system and the public sector, including the GCDO and GCISO roles.]</p>	Recommend this requires stand-alone review / project sponsored by SIB.	<ul style="list-style-type: none"> Amend ISA wrt direct access agreements (DPMC) Security clearances and access to information systems (NZSIS / GCSB) 	<p>Rec 10</p> <p>Rec 11</p>	
 Extend and support PCVE programmes	<p>Develop a strategic approach to Preventing and Countering Violent Extremism (PCVE) with a focus on prevention and disengagement initiatives, then implement action plan across targeted areas.</p>	<p>DPMC to lead development of strategic approach.</p> <p>CTCC agencies to implement.</p>	<ul style="list-style-type: none"> P/CVE Strategic Framework (DPMC) CVE online (DIA) Disengagement (NZP) 	<p>Rec 4</p> <p>Rec 41</p> <p>-</p>	
 Enhance protection of people and places	<p>Continue and expand work to protect people and places, including enhancing CT legislation, addressing gaps in intervention capabilities, and building on the Crowded Places Strategy and Safer Communities Fund.</p>	Lead(s) per key workstreams, including MOJ, NZ Police and DIA.	<ul style="list-style-type: none"> Strengthen NZ's CT laws (MOJ) Change hate speech legislation (MOJ) Crowded Places Strategy (NZP) Extend Safer Communities Fund (DIA) 6(a) 	<p>Rec 18</p> <p>Rec 40</p> <p>-</p> <p>-</p> <p>-</p>	
<i>Under-pinned by</i>	Social cohesion	<i>Existing work programme underway, under separate governance arrangements.</i>	<i>MSD lead through Social Cohesion Oversight Group.</i>	<ul style="list-style-type: none"> <i>[Per social cohesion work programme]</i> 	<i>[Various]</i>

CT STRATEGY IMPLEMENTATION PLAN - 2020

Counter-terrorism Coordination Committee							Alert Level 4 Level 3												TODAY		
ctcc@dpmc.govt.nz							Q3 2019/20			Q4 2019/20			Q1 2020/21			Q2 2020/21					
Work Stream		Goal		Lead	CTCC Review	Status	Risk / Issues & Comments		JANUARY	FEBRUARY	MARCH	APRIL	MAY	JUNE	JULY	AUGUST	SEPTEMBER	OCTOBER	NOVEMBER	DECEMBER	
Mōhio - Understand		We detect and understand the threat, while our people look out for each other and we all know what to do when something happens.								★ CTCC 14 Feb		★ CTCC 27 Mar	★ CTCC 9 May	★ CTCC 19 June	★ CTCC 31 July	★ CTCC 11 Sept		★ CTCC 23 Oct	★ CTCC 4 Dec		
Information Access and Sharing		Appropriate information is available to agencies to proactively identify terrorist and violent protest threats and manage residual risk.		NZSIS & DPMC	TBD		DPMC / NZSIS-led information gathering underway (delayed due to COVID-19).				Information gathering										
Public Information		New Zealanders have the information they need to be aware, engaged, and know what to do to stay safe.		DPMC	TBD		CT Comms Working Group established to manage action plan, and coordinating with RCOI Response Steering Group (RSG). DPMC comms staff in place.							CT Public Information Review							
Strategic Threat Assessment		CTAG to develop and introduce an annual New Zealand Terrorism Threat Environment assessment, to inform priority and risk discussions.		CTAG	-	Complete	Published Dec 2019, unclassified version to be published in the NZSIS Annual Report.														
CT NSIP Implementation		Fully implement the structures to support the implementation of the CT NSIP under the updated framework.		DPMC	Post RCOI		NSIP Qs agreed, SCG last met in March. Light touch NSIPs review is underway, CT will be considered as part of this after RCOI report.				★ CT SCG meeting										
Risk Profile		Update the Terrorism Risk Profile.		DPMC	2021	Complete	Signed off by SIB in June 2019.														
Mahi Tahi - Work Together		We work collectively as a nation to reduce and mitigate the risk.																			
CT System Capability Review		Review of cross-system CT capabilities to inform the CT Work Programme and capability development options.		DPMC	Jun-20		DPMC-led review delayed due to COVID-19 but initial phase scheduled to complete at end of June. Ongoing agency input required.				Develop capability landscape										
Christchurch Call		Lead the Christchurch Call to Action to eliminate terrorist and violent extremist content online.		MFAT	TBD		Priorities are engaging with newly independent GIFCT, crisis response mechanisms, understanding algorithmic outcomes and research landscape.						Assess current and target state								
International CT Engagement and Posture		Support the efforts of the international community to counter terrorism and violent extremism at the global, regional and national levels.		MFAT	TBD		Heavy COVID-19 impact. Some forums now being held virtually, potentially in person in coming months. Risk for NZ if unable to contribute appropriately.							★ First GIFCT Independent Advisory Committee meeting (25 June)	★ GIFCT 2020 Summit (23 July)	★ Advisory Network meeting (RightsCon) (27-31 July)					
International Deployments		Cabinet to confirm Middle East and other deployments.		NZDF & MFAT	TBD		Defeat ISIS Cabinet paper approved. CTIF Cabinet paper scheduled for Cabinet in August 2020.				★ Cabinet (D-ISIS)				★ UN 2020 Counter-Terrorism Week	★ Cabinet Committee (CTIF)		★ ANZCTC meeting (25 Nov, Wellington)			
Whakahōtaetae - Prevent		We focus our efforts and capabilities on effective, long-term prevention.																			
Reduce the Threat																					
Disengagement and MACIP		Establish a broader, more structured inter-agency model / programme for the case management of violent extremism risk individuals.		NZP	TBD		First inter-agency workshop held. Key milestones: establish criteria, approve case management pilot, explore risk assessment tool benefits.				★ NZ Police lead appointed				★ Initial inter-agency workshop						
CVE Online		Deliver CVE online content work programme via operational improvements, legislative change, and media content regulatory review.		DIA	TBD		Bill introduced on 26 May. DIA team established, key positions being filled, inter-agency planning underway. Research contract signed.								★ Films, Videos and Publications (Urgent Interim Classification...) Amendment Bill				★ CVE Cabinet paper (TBD)		
Social Inclusion		Progress and strengthen connections of government actions to build social inclusion.		MSD	TBD		Report-back on improving social inclusion lodged for consideration at Cabinet Social Wellbeing Committee (SWC) on 17 June.								★ SWC Cabinet Committee						
Community Engagement		[TBD]		DPMC	TBD		Establishment of CTCC Community Engagement Subgroup agree at 19 June meeting.														
Control Orders		Terrorism Suppression (Control Orders) Act passed in late 2019. Expand control orders to terrorism-related offenders (including FVPCA offenders).		MOJ	TBD		Policy development underway to expand control orders. Will be taken to Cabinet following the formation of the next Government.												★ ERS / LEG (TBC), as part of legislative amendments		
FTF Planning		Agree policy and operational frameworks for managing New Zealand FTFs. Determine repatriation options.		DPMC	TBD	Complete	Frameworks agreed, but situation remains volatile. Limited repatriation options and no further planning will be undertaken at this stage.								★ Embassy Baghdad closure						
Hate Speech		Ensure the incitement provisions in the Human Rights Act 1993 provide for adequate protection against hate speech.		MOJ	TBD		Policy development underway, decisions yet to be taken on possible timing for consultation on proposed changes.														
Major Events		Support the Major Event Security Committee (MESC) to monitor and enable security planning by lead agencies.		DPMC	TBD	Ongoing	Focus is currently on the 2020 general election, America's Cup, and APEC 2021.					★ ANZAC Day					★ General Election				
Address Vulnerabilities																					
Crowded Places		Develop and role out a Crowded Places Strategy and guidelines for owners and operators.		NZP	TBD		Strategy developed and Crowded Places Advisory Group (CPAGNZ) established. Public engagement started, launch delayed by COVID-19.								★ Crowded Places Strategy launch (TBD)						
Transport Security		Develop and implement work programme to address key security risks and vulnerabilities across the transport sector.		MOT & Sector	TBD		9(2)(f)(iv)					6(a)				6(a), 9(2)(f)(iv)					
Drones		Implement effective legislative framework and capability to intervene in relation to unlawfully operated drones.		MOT & CAA	TBD		Policy work progressing well, but Civil Aviation Bill intro delayed (COVID-19). Being managed within wider Civil Aviation Bill project.				★ Drone intervention power agreed by Cabinet (now reviewing offences under civil aviation)			★ W-ECM policy decisions (TBD, possibly deferred)				★ Bill introduction (TBD, deferred from April)			
Border Systems		Use of border data (goods and passenger) to inform CT targeting and threat discovery. Procurement of technology/tools and trialling collaborative initiatives.		INZ & NZCS	TBD		COVID19 has hindered work in the passenger space, however has allowed for shift in focus to goods space.														
Firearms Reform		Implement updated legislative framework to regulate the use and possession of firearms.		NZP	TBD		Arms Amendment Act and buy-back operation complete. Arms Legislation Bill in progress.														
Disrupt Violent Extremist Activity																					
CT Legislation (new offences; definition; extended COs)		Review of Counter Terrorism legislation to ensure offences and definition of terrorist offence are workable and fit for purpose		MOJ	TBD		Policy devt and Bill drafting underway. Cabinet policy decisions and intro of Bills to the House will follow formation of a new government.			★ Offences briefing to Minister	★ Targeted engagement on definitions				★ Definitions briefing to			ERS / LEG (TBC), as part of legislative amendments package	★ Bill introduction		
Terrorist Designations		Review and update as appropriate the terrorist designations framework and processes.		NZP	TBD		Review of framework at very early stages. Designation of Christchurch attacker under consideration by working group - advice to SIB in July.														
Immigration National Security Screening (INSS) Project		Re-engineer National Security Screening to provide an agile system where risks from migrants can be tracked, measured and controlled.		INZ	TBD		Business case co-presented to INZ Business Change Board on 10 June.								★ Chch attacker designation advice to SIB						
NSI Proceedings		Create a new regime for managing how national security information is used in proceedings		MOJ	TBD		Bill being drafted, though delayed due to competing priorities in PCO. Intro to the House will follow formation of a new government.												★ Bill introduction		
Terrorist Financing		Agree AML/CFT National Strategy and participate fully in FAFT mutual evaluation process in 2019-20.		MOJ	TBD		AML/CFT National Strategy released in December 2019. Feedback provided on first draft of FATF report - final due in February 2021				FAFT meetings										
Takatū - Ready to Respond and Recover		We take a victim-centred approach, responding swiftly to protect lives and working in partnership to ensure recovery.																			
Learning System		Respond to RCOI recommendations. Incorporate CT elements into any NSS centralised lessons management system. Run effective CT exercises.		DPMC	TBD		RCOI report delayed until 31 July. No progress on lessons management system. Ex RESOLUTION postponed due to COVID-19.				★ Ex RESOLUTION (to be rescheduled)				★ Royal Commission of Inquiry report			Response to RCOI			
NZDF Support to Agencies		Clarify NZDF CT support to agencies under the Defence Act in the event of a terrorist incident.		MOD, NZDF & NZDF	TBD		Currently working to understand gaps and opportunities.														
CT Handbook Refresh		Review and publish the CT Handbook.		DPMC	-	Complete	Refresh completed in October 2019 and disseminated to agencies.														
Threat Level System		Confirm changes to national terrorism threat level processes and decision-making.		DPMC & NZSIS	-	Complete	Signed off by Cabinet in Sept 2019.														
PUBLIC COMMS DATES										★ ISC	★ CT Strategy				★ Crowded Places Strategy launch (TBD)						
KEY MILESTONE DATES											★ 15 March Commemorations				★ Royal Commission of Inquiry report	★ General Election					
OTHER KEY DATES											★ Easter	★ Ramadan	★ ANZAC Day			★ Yom Kippur		★ Hanukkah	★ Christmas		
							Alert Level 4 Level 3														

Key Principles:

- Reflecting NZ threat context, proportionate
- Building on strengths, current approach
- Proactive, reduction-focused

DRAFT ONLY**Proposed National Security Sector Action****National security sector****Social sector**

More tactical
Narrower in objectives
Threat oriented
Focus on individuals

Bespoke mitigation of violent extremist risk*via ...*

Inter-agency case management of risk individuals, supported by capability investment and external relationships

Build

Build/establish an inter-agency model for end-to-end, holistic and outcomes-focused case management of risk individuals (working closely with social sector partner agencies).

Strong, trust-based community relationships*via ...*

Broad-based, enduring engagement with diverse communities and investment in cultural capability

Invest

Community facing national sector agencies to continue investing in community engagement and cultural capability aligned to more diverse demographic, cultural, ethnic profile (and support similar investment by social sector partner agencies).

More strategic
Broader in objectives
Risk oriented
Focus on communities

Underlying community strength and resilience*via ...*

Continued all-of-government investment in social inclusion, promotion of cultural/religious awareness, diversity and tolerance

Support/advocate

Lend advocacy support to activity that supports national security via strengthening social inclusion, inter-community relationships, community resilience and by promoting key values such as tolerance and diversity.

Released under the Official Information Act 1982

[This document has been removed as it is now subject to a Non-Publication Order by the Coroner. If requested now, section 18(c)(ii) of the Act would apply]