

New Privacy Laws



**Company Accountants Special
Interest Group**



**Incident
Response**

FORENSIC & CYBER



Agenda

Implementing a cybersecurity and privacy framework

Preparing incident response plans and playbooks

Responding to a privacy breach and
Notifying the Office of the Privacy
Commissioner of a privacy breach

Privacy Act 2020

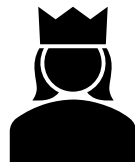
The Privacy Act replaces 27 year old legislation and implements a number of the changes adopted in comparable jurisdictions, such as the EU, Australia, and various US states.

These significant reforms will change the way organisations in New Zealand manage privacy issues and data security.

***Mandatory
notifications for
privacy breaches***



***Increased powers for
the Privacy
Commissioner***



***Controls on
disclosure of
information
overseas***



Criminal offences



***Extra-territorial
scope***



Serious Harm

113 Assessment of likelihood of serious harm being caused by privacy breach

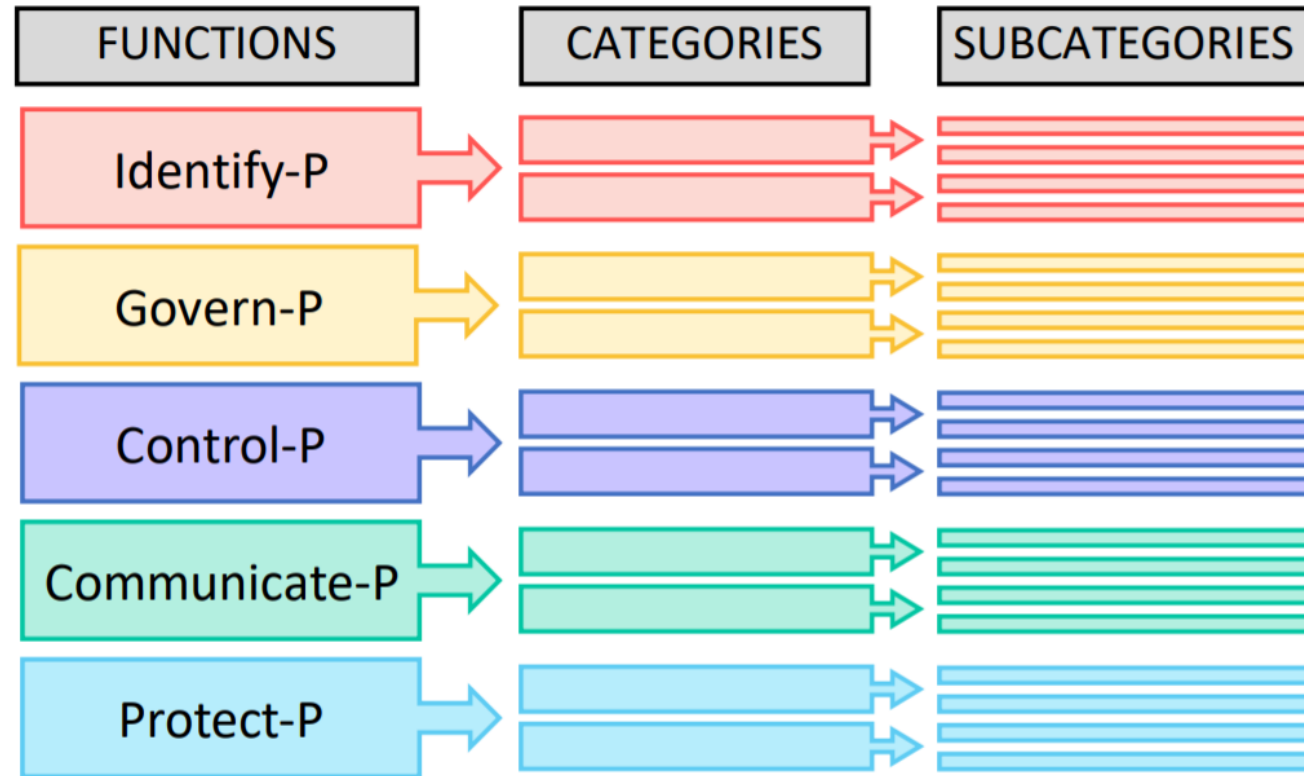
When an agency is assessing whether a privacy breach is likely to cause serious harm in order to decide whether the breach is a notifiable privacy breach, the agency must consider the following:

- (a) any action taken by the agency to reduce the risk of harm following the breach:
- (b) whether the personal information is sensitive in nature:
- (c) the nature of the harm that may be caused to affected individuals:
- (d) the person or body that has obtained or may obtain personal information as a result of the breach (if known):
- (e) whether the personal information is protected by a security measure:
- (f) any other relevant matters.

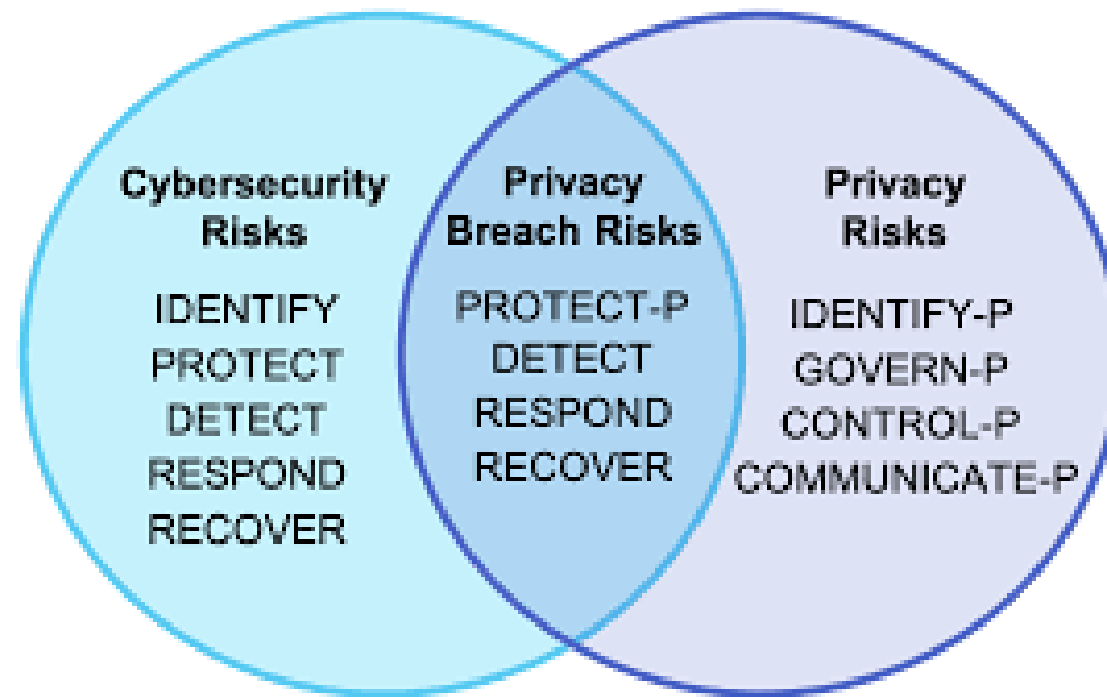
NIST CSF Framework



NIST Privacy Framework



Combined Frameworks



Privacy Framework Categories

Function Unique Identifier	Function	Category Unique Identifier	Category
ID-P	Identify-P	ID.IM-P	Inventory and Mapping
		ID.BE-P	Business Environment
		ID.RA-P	Risk Assessment
		ID.DE-P	Data Processing Ecosystem Risk Management
GV-P	Govern-P	GV.PO-P	Governance Policies, Processes, and Procedures
		GV.RM-P	Risk Management Strategy
		GV.AT-P	Awareness and Training
		GV.MT-P	Monitoring and Review
CT-P	Control-P	CT.PO-P	Data Processing Policies, Processes, and Procedures
		CT.DM-P	Data Processing Management
		CT.DP-P	Disassociated Processing
CM-P	Communicate-P	CM.PO-P	Communication Policies, Processes, and Procedures
		CM.AW-P	Data Processing Awareness
PR-P	Protect-P	PR.PO-P	Data Protection Policies, Processes, and Procedures
		PR.AC-P	Identity Management, Authentication, and Access Control
		PR.DS-P	Data Security
		PR.MA-P	Maintenance
		PR.PT-P	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Completing the Framework

CATEGORY - Inventory and Mapping (ID.IM-P)

Data processing by systems, products, or services is understood and informs the management of privacy risk.

ID.IM-P1: Systems/products/services that process data are inventoried. *

	1	2	3	4	
Strongly Disagree	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Strongly Agree

ID.IM-P2: Owners or operators (e.g., the organisation or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried. *

	1	2	3	4	
Strongly Disagree	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Strongly Agree

ID.IM-P3: Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried. *

	1	2	3	4	
Strongly Disagree	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Strongly Agree

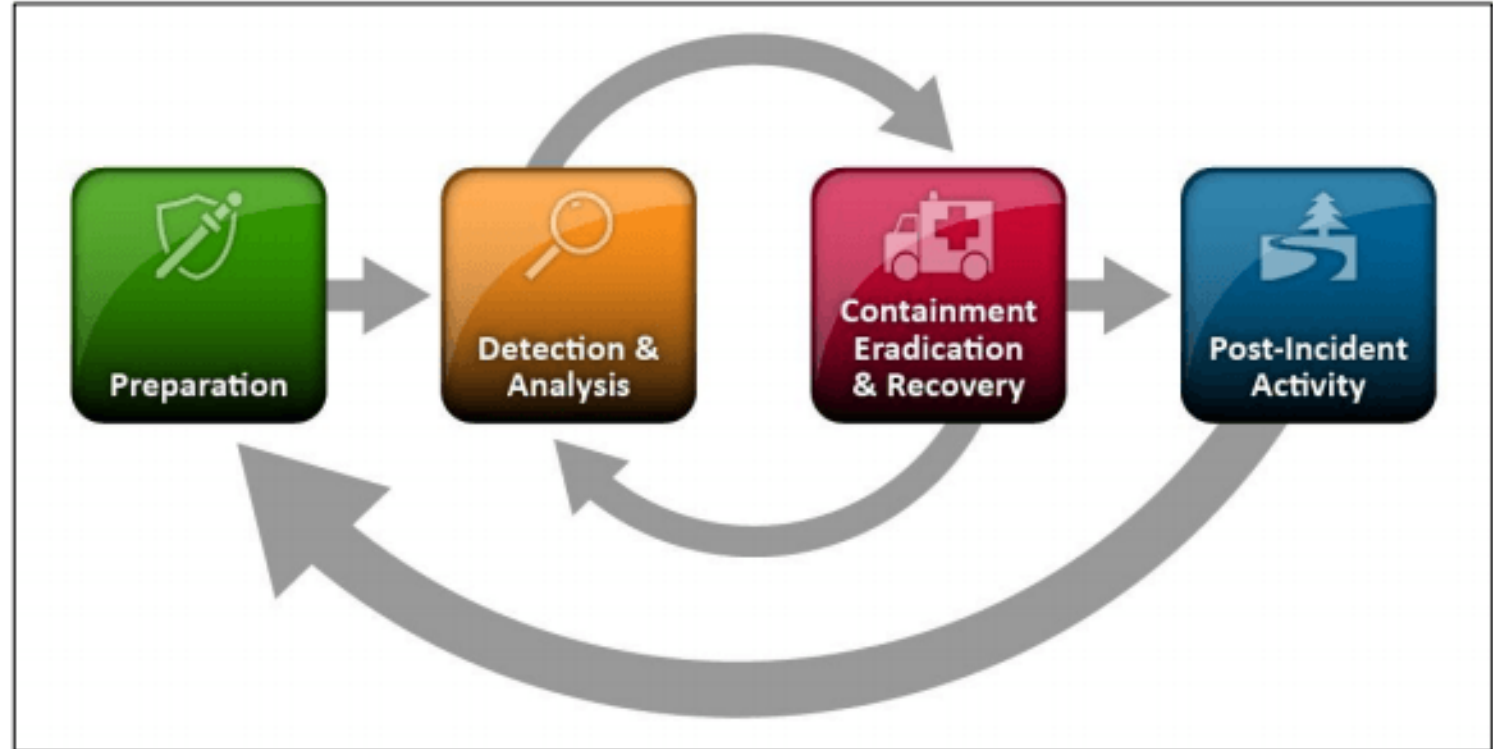
Completed Framework Example

Sample Report 3: Current Profile v Target Profile + Risk Gap

Function	1 Identify-P	2 Govern-P	3 Control-P	4 Communicate-P	5 Protect-P	Current Profile	Target Profile	Risk Gap
Cat.01 - Inventory and Mapping (ID.IM-P)	3.9					3.9	4 -	0.1
Cat.02 - Business Environment (ID.BE-P)	3.0					3.0	4 -	1.0
Cat.03 - Risk Assessment (ID.RA-P)	3.0					3.0	3 -	-
Cat.04 - Data Processing Ecosystem Risk Management (ID.DE-P)	3.2					3.2	4 -	0.8
Cat.05 - Governance Policies, Processes, and Procedures (GV.PO-P)		2.5				2.5	3 -	0.5
Cat.06 - Risk Management Strategy (GV.RM-P)		2.3				2.3	3 -	0.7
Cat.07 - Awareness and Training (GV.AT-P)		2.3				2.3	3 -	0.8
Cat.08 - Monitoring and Review (GV.MT-P)		2.9				2.9	3 -	0.1
Cat.09 - Data Processing Policies, Processes, and Procedures (CT.PO-P)			1.8			1.8	2 -	0.3
Cat.10 - Data Processing Management (CT.DM-P)			3.2			3.2	4 -	0.8
Cat.11 - Disassociated Processing (CT.DP-P)			3.2			3.2	4 -	0.8
Cat.12 - Communication Policies, Processes, and Procedures (CM.PO-P)				1.5		1.5	2 -	0.5
Cat.13 - Data Processing Awareness (CM.AW-P)				1.9		1.9	2 -	0.1
Cat.14 - Data Protection Policies, Processes, and Procedures (PR.PO-P)					2.3	2.3	3 -	0.7
Cat.15 - Identity Management, Authentication, and Access Control (PR.AC-P)					2.3	2.3	3 -	0.7
Cat.16 - Data Security (PR.DS-P)					2.5	2.5	3 -	0.5
Cat.17 - Maintenance (PR.MA-P)					3.5	3.5	4 -	0.5
Cat.18 - Protective Technology (PR.PT-P)					1.5	1.5	2 -	0.5
Grand Total	3.3	2.5	2.7	1.7	2.4	2.6	3.1 -	0.5

Preparation

Your Incident Response processes should analyse privacy incidents to learn how to prevent future breaches and attempt to protect your data.



Preparation

Manage the risk posed by privacy breach and support your organisation's coordinated and efficient response to a breach.

Create, maintain, and exercise a basic cyber incident response plan (and playbooks) and associated communications plan that includes response and notification procedures for a privacy incident.

Run regular cyber simulations to evaluate the effectiveness of the incident response plan, and drill the training into the CSIRT team.

Clearly define and allocate roles and responsibilities in advance, and have a backup option for each.

Roles and Responsibilities

An incident response plan clearly sets out the roles and responsibilities of those involved in the incident response.

Privacy officer

Information security and ICT

Legal

Communications

Risk and assurance

Service delivery/operations

Senior leadership team

Responding to a Privacy Breach


privacy.org.nz/privacy-for-agencies/privacy-breaches/notify-us

Do I need to notify

If you are unsure whether your organisation must notify its privacy breach to us, use our self-assessment tool to help you work it out.

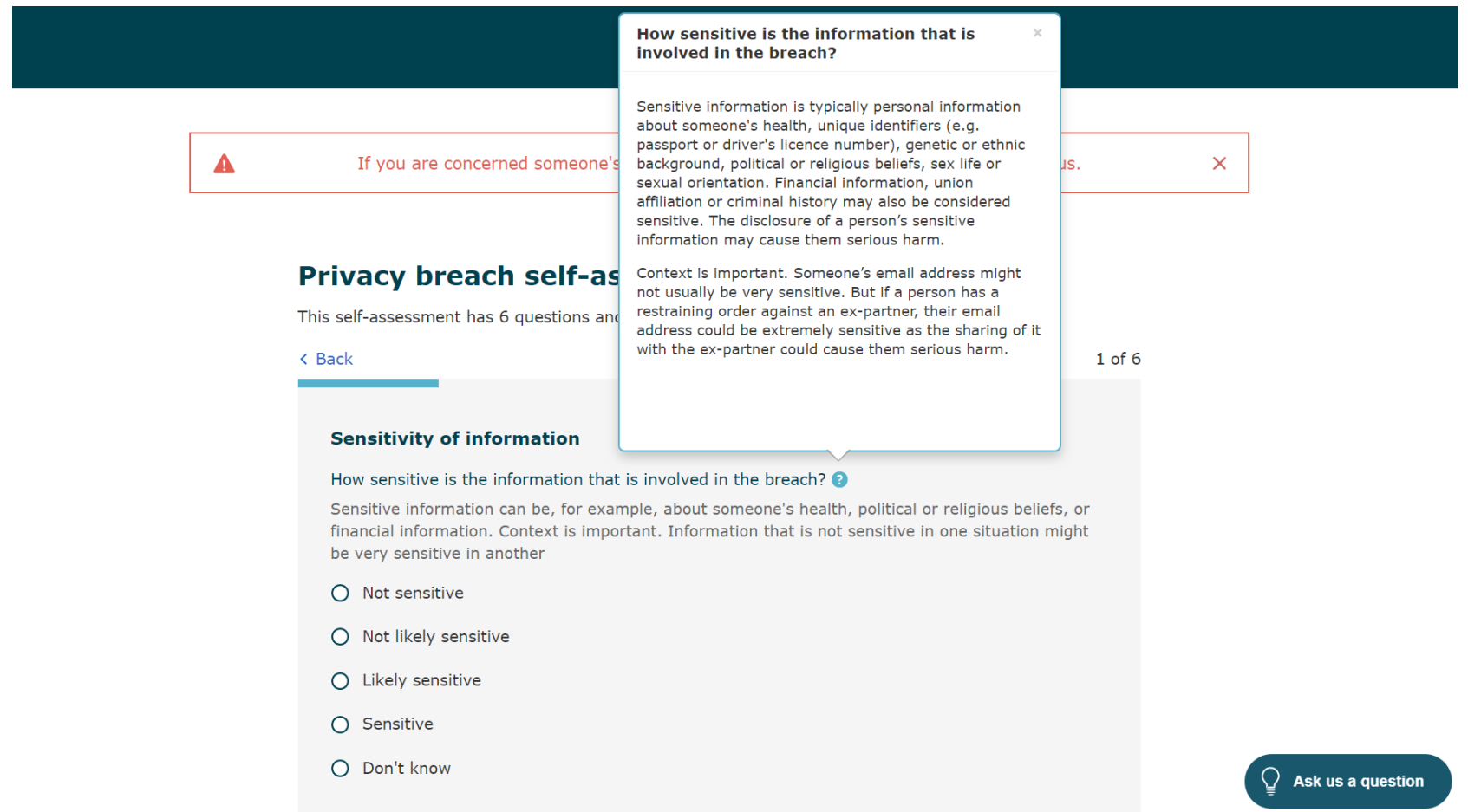
Note: No information you enter is sent to us, unless you elect to go on to submit a privacy breach notification. None of the information entered is stored on our website.

Take self-assessment →

If your organisation has already determined that its privacy breach is notifiable, or wish to notify us in any case, click on the button below to report the breach. You can see a checklist of what information is required  [here](#).

Report a breach →

Self Assessment



Reporting a Breach

Privacy breach notification form

- ✓ Contact details
- ✓ Timeline
- ✓ About the breach
- ✓ Likely harm
- ✓ Notifying Affected People
- ✓ Other Organisations
- Almost done**

Almost done

Please provide any other information you think may be relevant to the breach, or steps you have taken or intend to take in response. (This is an optional field.)


You can upload any attachments here (e.g. copy of any public notice if applicable). The total size limit is 7MB. (This is an optional field.)

Do not provide us with copies of the information involved in the breach.

Choose files

Review and submit

Financial
Context

An abstract background featuring vibrant red and blue light streaks and bokeh effects, creating a sense of motion and depth.

Cyber and
the CFO

Key Findings from the CAANZ Report

- 54% were either not aware of whether their organisation had suffered an attack or thought they had not been.
- In just 8% of organisations, the CFO was responsible for the strategic direction of cyber security.
- The annual cost of cybercrime to the global economy will double from US\$3 trillion in 2015 to \$US6 trillion in 2021.
- Many organisations pinpoint cybercrime as one of their most significant threats.
- There are key reasons for the CFO to step up and play a leading role in cyber security.

Thank you

Campbell McKenzie

0800 WITNESS

campbell@incidentresponse.co.nz

incidentresponse.co.nz

We help you Prepare, Respond and Recover
from **Forensic** and **Cyber** Incidents

