Office of the Victorian Information Commissioner

INFORMATION FOR AGENCIES and BODIES

1300 00 6842 | ovic.vic.gov.au

How-to: A guide to the Multi-Organisation Attestation Reporting Model and Process

Freedom of Information | Privacy | Data Protection

Document Details

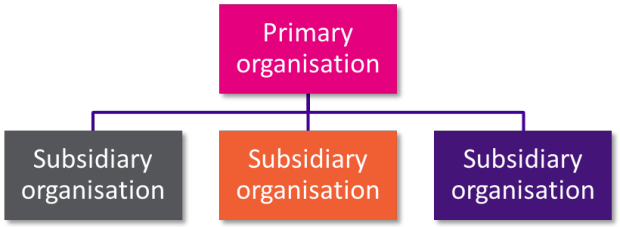
How-to: A guide to the Multi-Organisation Attestation Reporting Model and Process		
Protective Marking		OFFICIAL
Approved for unlimited public release		Yes – Authorised for release
Release Date		February 2023
Review Date		January 2024
Document Version		1.0
Authority		Office of the Victorian Information Commissioner (**OVIC**)
Author		Information Security Unit - OVIC
Version control		
Version	Date	Key Changes
1.0	March 2022	Original version – using How-to: A guide to the Multi-Organisation PDSP Reporting Model and Process as basis

Contents

Introduction

What is the Multi-Organisation reporting model?

The multi-organisation reporting model is designed to support scenarios where subsidiary organisations have equivalent risk profiles (including appetite and tolerance), risk references, control environments, implementation statuses, completion dates for the Victorian Protective Data Security Standard elements, and maturity levels to those of a primary organisation. In these scenarios the subsidiary effectively operates as a business unit of the primary organisation.

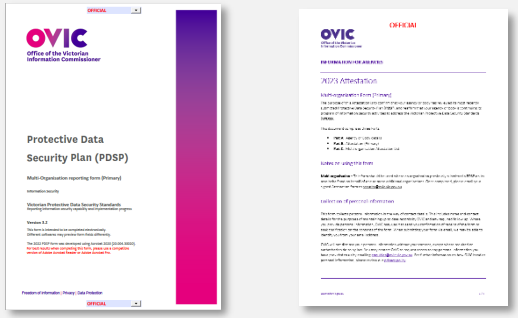


Strengthening the Multi-Organisation reporting model

Following analysis of the 2018 and 2020 multi-organisation Protective Data Security Plan (**PDSP**) submissions, OVIC identified a range of issues relating to the identification and management of information security risks of subsidiary organisations versus those of a primary organisation. These issues included different control environments which, in some cases, were not reflected in multi-organisation PDSPs.

To address these issues, in 2022 OVIC implemented a strengthened multi-organisation reporting model. This model requires all organisations (primary and subsidiaries) seeking to use a multi-organisation PDSP to meet certain reporting criteria before proceeding.

Primary organisation PDSP and Attestation



Subsidiary organisation(s) PDSP and Attestation

Refer to OVIC's How-to: A guide to completing the PDSP form for detailed guidance on Part A and B of the PDSP form

Is the Multi-Organisation reporting model appropriate for my scenario?

In the first instance, each subsidiary organisation should liaise with their primary organisation to determine whether the multi-organisation reporting model would be supported. This includes confirming shared criteria with the primary organisation, i.e., that each proposed subsidiary organisation will attest to having equivalent:

a. risk profiles (including appetite and tolerance);
b. control environments;
c. implementation statuses for the elements (including completion dates for VPDSS);
d. risk references; and,
e. maturity levels.

This shared criteria must be met for the subsidiary organisation(s) to be comfortable with their representation on the primary organisation's Attestation form that will be submitted to OVIC.

Should you require further guidance, members of the Information Security Unit are available to discuss. Contact security@ovic.vic.gov.au

When is the Multi-Organisation Attestation due?

A consolidated submission of the primary organisation and subsidiary organisation(s) Attestation is due to OVIC by **31 August 2023**. Refer to the Submission and Next Steps section of this guide for submission options.

Steps and Actions Required

STEP	ACTION REQUIRED		
	PRIMARY ORG	SUBSIDIARY ORG	OVIC INFORMATION SECURITY UNIT (ISU)
1	Collaborate to review and reaffirm that the shared reporting criteria is met by all organisations (primary and subsidiary), and each subsidiary organisation's risks and controls are reflected on the primary organisation's current PDSP. This includes confirming that each proposed subsidiary organisation can attest to having equivalent: a. risk profiles (including appetite and tolerance); b. control environments; c. implementation statuses for the elements (including completion dates for VPDSS); d. risk references; and, e. maturity levels. This could be undertaken in conjunction with each organisation's Security Risk Profile Assessment (**SRPA**) process. ⚠ *Where any subsidiary organisation is unable to attest to all shared reporting criteria, the multi-organisation reporting model process is no longer appropriate. In this instance, the subsidiary organisation should contact OVIC's Information Security Unit for further guidance.*		

STEP	ACTION REQUIRED		
	PRIMARY ORG	**SUBSIDIARY ORG**	**OVIC INFORMATION SECURITY UNIT (ISU)**
2	Advise the ISU of the intention to use the Multi-Organisation reporting model (*use email template provide on page 9 of this guide*). This includes providing: • formal confirmation that each proposed subsidiary organisation can attest to the shared reporting criteria • details of each subsidiary, including the: – organisation name – public sector body Head's name – public sector body Head's position title – public sector body Head's email address.		
3			1. Create a **tailored primary organisation Attestation** form using the subsidiary organisation(s) details provided. 2. Send a copy of the tailored primary organisation Attestation and **the subsidiary organisation Attestation form(s)** to all organisations via email. ⚠ *This correspondence will be one email sent to all organisations listed on the primary Attestation, and outlines who is responsible for completing the required documentation and submission to OVIC.*

STEP	ACTION REQUIRED		
	PRIMARY ORG	SUBSIDIARY ORG	OVIC INFORMATION SECURITY UNIT (ISU)
4	Populate the primary Attestation form.	Populate and sign the subsidiary organisation Attestation form and provide a signed copy to the primary organisation.	
5	Collate all signed subsidiary Attestation forms (primary and subsidiary organisation Attestation forms).		
6	Finalise and sign the tailored primary organisation Attestation form.		
7	Submit collated (primary and all subsidiary Attestations) submission to OVIC by 31 August 2023 via email, including in CC any subsidiary organisations.		
8			Confirm receipt of the Attestations with the primary organisation and subsidiary organisations.
Each organisation satisfies their reporting obligations for 2023.			

Email Template for Primary Organisation to send to ISU (step 2 of Multi-Organisation reporting process)

TO:	security@ovic.vic.gov.au
CC:	***[include any relevant contacts]***
SUBJECT:	Intention to use Multi-Organisation Attestation reporting model in 2023
CONTENT:	**Attention**: Information Security Unit I am confirming that ***[insert primary organisation name]*** and ***[insert subsidiary organisation name(s)]*** intend to use the Multi-Organisation reporting model in 2023. 1. I can confirm that each subsidiary organisation listed below (in point 2) can attest to having equivalent: a. risk profiles (including appetite and tolerance); b. control environments; c. implementation statuses for the elements (including completion dates for VPDSS); d. risk references; and e. maturity levels. 2. Details of each subsidiary organisation: • Subsidiary organisation name: ***[Insert subsidiary organisation name]*** • Public sector body Head's name: ***[insert name of public sector body head of the subsidiary organisation]*** • Public sector body Head's Position title: ***[insert title of public sector body head of the subsidiary organisation]*** • Public sector body Head's email address: ***[insert email address of public sector body head of the subsidiary organisation]*** ***[If you need to add additional subsidiaries, please copy and paste item 2 and complete the corresponding details]*** ***[Ensure you include your email signature with your contact details and role title should the ISU have any follow up questions]***

Submission and Next Steps

Options for submission

When all mandatory fields on the Attestations have been completed and public sector body Heads have reviewed and signed off their respective organisation's form, the primary organisation **submits a copy** of the collated Attestations to OVIC via one of the options below.

Please note: A prior appointment must be made with a member of OVIC's Information Security Unit for option 3.	**Option 1**	Soft copy	Send a copy of the completed, signed and dated Attestations to security@ovic.vic.gov.au (either from the public sector body Head's email address, or the Information Security Lead's email address)
	Option 2	Hard copy	Post the Attestations in a single opaque envelope with no protective marking labelled on the outside to: PO Box 24274 Melbourne VIC 3001
	Option 3	Hard copy	Hand deliver the Attestations to: Attention: OVIC, Level 34 121 Exhibition Street Melbourne VIC 3001

Next steps

After submitting the collated Attestations to OVIC, each organisation will receive an email confirming receipt by OVIC's Information Security Unit within 1-15 business days.

Between now and the next OVIC reporting period, all organisations represented on the primary organisation Attestation form must continue to:

- monitor their organisation's information security risks;
- alert OVIC to any significant changes to their organisation's information security risks and/or operating environment;
- notify OVIC of any changes to their organisation's information security lead and/or public sector body Head; and
- report information security incidents through the Incident Notification Scheme.