Office of the Victorian
Information Commissioner

Standard 10 of the Victorian Protective Data Security Standards

Audit of the pre-engagement phase of personnel security under section 8D(2)(b) of the Privacy and Data Protection Act 2014 (Vic)

Disclaimer

The information in this document is general in nature and does not constitute legal advice.

Copyright

You are free to re-use this work under a Creative Commons Attribution 4.0 licence, provided you credit the State of Victoria (Office of the Victorian Information Commissioner) as author, indicate if changes were made and comply with the other licence terms. The licence does not apply to any branding, including Government logos. Copyright queries may be directed to communications@ovic.vic.gov.au

Table of Contents

Foreword

The Victorian Public Sector (**VPS**) employs thousands of personnel across multiple organisations, carrying out a wide array of functions. These personnel hold positions of trust as custodians of vast volumes of public sector information, much of which includes high-value information assets.

It is important that these personnel are eligible and suitable to have access to government assets. In instances where unsuitable or ineligible personnel have access to public sector information, there are significant risks – including possible fraud and corruption.

Under Standard 10 of the Victorian Protective Data Security Standards (**VPDSS**), public sector organisations must establish, implement, and maintain personnel security controls addressing all persons' continuing eligibility and suitability to access public sector information.

This audit focussed on the pre-engagement phase of the personnel lifecycle. That is, the time between completion of a merit selection process, and a new employee commencing in the organisation.

OVIC sought to determine whether the four organisations have in place appropriate policies, procedures, and practices addressing the pre-engagement phase of personnel security. This includes verifying a person's identity, and undertaking appropriate screening checks to assess suitability and eligibility of prospective staff.

The report reflects that none of the organisations fully met the criteria for any of the four questions tested in the audit. However, they were all rated as either 'partially meets' or 'substantially meets' across each of the audit questions – meaning that all audited organisations have the foundations necessary to ensure effective pre-engagement screening. At the same time, the report also finds that there is considerable scope for the audited organisations to improve their practices across all tested criteria.

All Victorian government organisations are encouraged to consider the report, reflect on their current approach to personnel screening, and consider scope for better practice improvements.

I thank the four organisations for their cooperation and participation in this audit. They invested a considerable amount of time in evaluating their own performance against Standard 10 and have indicated that they will continue to strengthen their implementation of the VPDSS.

Rachel Dixon

Privacy and Data Protection Deputy Commissioner

2 April 2024

Executive Summary

Introduction

The Victorian public sector (**VPS**) comprises nine major government departments and numerous other organisations which together employ or engage many thousands of personnel responsible for delivering services and carrying out a wide array of functions.

These personnel hold positions of trust. They are custodians of vast volumes of public sector information, much of which includes high-value information assets, and they should have the appropriate qualifications, skills, experience, qualities and values[1] to properly perform their duties.

In instilling public trust, VPS organisations should therefore implement appropriate personnel security[2] measures to ensure that personnel who have access to government assets are eligible and suitable to do so.

This report focuses on the pre-engagement phase of the personnel lifecycle, meaning the time before personnel commence work with the organisation. Appropriate screening in this phase is a critical aspect of personnel security. Organisations should meet their recruitment responsibilities by developing and implementing thorough, consistent, and fit-for-purpose personnel screening policies and procedures.

If organisations fail to manage their workforces at the pre-engagement phase, it exposes them to risks to their information and other resources, including fraud and corruption risks. It can also undermine public confidence and trust in government and the services it delivers.

Audit of the pre-engagement phase of personnel security under Standard 10 of the VPDSS

The Victorian Protective Data Security Framework (**VPDSF**) and accompanying Victorian Protective Data Security Standards (**VPDSS**) were released in 2016.[3] The VPDSS contain 12 standards that all VPS agencies must adhere to.[4]

[1] The Victorian Public Sector values are responsiveness, integrity, impartiality, accountability, respect, leadership and human rights.

[2] The management of personnel across multiple phases, including: pre-engagement (eligibility and suitability); engagement (ongoing and re-engagement); and separation (permanently or temporarily). Victorian Protective Data Security Standards – Glossary V 2.1, January 2022.

[3] OVIC website, https://ovic.vic.gov.au/information-security/standards/ .

[4] Adherence to the Standards is mandatory for all organisations within the scope of Part 4 of the Privacy and Data Protection Act 2014. This includes a public sector agency, a body that is a special body within the meaning of section 6 of the Public Administration Act 2004, and a body declared under subsection (3) to be a body to which Part 4 applies. It does not apply to local councils, universities and public hospitals and health services.

Standard 10 deals with personnel security. It covers policies and practices to ensure the continued eligibility and suitability of people accessing public sector resources.

There are eight elements underpinning Standard 10. This audit focuses on four of these elements relating to the pre-engagement phase of the personnel security lifecycle. The pre-engagement phase is the period between a merit selection process being concluded but before new personnel commence in the role.

The Office of the Victorian Information Commissioner (**OVIC**) selected this focus because pre-engagement activities, such as identity verification and pre-engagement screening checks (including security clearances where relevant), are the first line of defence in mitigating organisations' personnel security risk. This is also an area where OVIC frequently sees gaps and risks in organisations' information security programs.

Audit Questions

To reach an audit conclusion, OVIC assessed the organisations against four audit questions:

1. Do the organisation's personnel security policies and procedures address the pre-engagement (eligibility and suitability) phase?
2. Does the organisation verify the identity of its personnel?
3. Does the organisation undertake pre-engagement screening of all personnel?
4. Does the organisation undertake additional pre-engagement screening of personnel that is commensurate with the risk profile of their roles?

Audit Criteria

The criteria tested to answer the above are set out in the sections covering each of the four questions, and in Annexure A.

Summary of OVIC's assessment of each organisation

Each organisation was rated against the audit questions using the following rating scale:

- **Yes** – the organisation fully meets the audit criteria

- **Substantially** – the organisation meets most of the audit criteria
- **Partially** – the organisation meets some of the audit criteria
- **No** – the organisation does not meet the audit criteria.

Table 1 Summary of audit assessment by agency and criteria

Audit Question	CCYP	DPC	VFMC	VMIA
1. Policies and procedures	Partially	Partially	Substantially	Partially
2. Identity verification	Partially	Partially	Partially	Partially
3. Pre-engagement screening	Substantially	Partially	Substantially	Substantially
4. Additional pre-engagement screening commensurate with risk	Partially	Substantially	Partially	Partially

Question 1 – Pre-engagement screening phase in policies and procedures

Question 1 sought to answer whether the audited organisations' personnel security policies and procedures adequately address the pre-engagement (eligibility and suitability) phase of personnel security.

Organisations must set out adequate pre-engagement screening requirements in easy-to-follow policy and procedure documents. This helps to ensure that the commensurate checks are carried out for each role at the appropriate time, in a consistent and thorough manner.

While none of the audited organisations have a single overarching personnel security policy or procedure(s) covering pre-engagement, all could point to a suite of documents that address personnel security activities related to the pre-engagement stage. However, OVIC found that generally, policies and procedures did not adequately capture all pre-engagement screening requirements in a coherent and consistent way, or sufficiently reflect best practice.

The main flaws in policy and procedure documents included:

- gaps, duplication, inaccuracies, or outdated content across documents
- insufficient coverage of all personnel, particularly temporary resources and contractors
- inconsistent or inappropriate timing for conducting pre-engagement screening checks, meaning some crucial checks are not conducted until after commencement in the role.

The level of pre-engagement screening undertaken by an organisation should be commensurate with the level of risk (posed by the functions associated with a role), organisational objectives, processes, and assessment of business impact. Different functions performed by different roles are likely to attract different levels of risk. Given this, a one-size-fits-all approach to pre-engagement screening is generally not appropriate. As such, understanding the risk profile of the workforce is an important foundational step required to properly inform an organisation’s policies and procedures. None of the audited organisations demonstrated that they have achieved this.

Given the above deficiencies, OVIC rated three of the organisations as partially meeting the audit criteria, with VFMC substantially meeting the criteria.

To assist in meeting the requirements associated with Question 1, OVIC recommends that all audited organisations review their existing personnel security related policies and procedures, with a view to developing a single, comprehensive personnel security policy and associated procedure(s) covering pre-engagement screening, that incorporates better practice activities and techniques.

Further, audited organisations should undertake a review of their workforce to determine the risk profile of the various roles and associated functions, to ensure that personnel security policies and procedures contain adequate pre-engagement requirements for both general and high-assurance roles.

Question 2 – Identity verification

Question 2 sought to answer whether the audited organisations verify the identity of their personnel to an appropriate standard.

An identity check helps to establish confidence in a person’s identity, ensuring that the candidate is the person they claim to be.

The VPDSS points to the Protective Security Policy Framework (**PSPF Policy 12**) as best practice. PSPF Policy 12 states that entities must verify their personnel to Level of Assurance 3 (**LOA 3**) of the National Identity Proofing Guidelines (**NIPG**). They must also use the Document Verification Service (**DVS**) to verify documents for Australian issued primary identification documents.

None of the audited organisations had clear policies and procedures on how to undertake identity verification to the appropriate standard. All four submitted that in practice, they conduct identity verification via a Nationally Coordinated Criminal History Check (National Police Check), conducted by third-party providers. However, organisations were generally unaware of the process and requirements for identity verification within the National Police Check, and therefore did not have sufficient assurance that identity verification conducted by third parties meets the required level of assurance. They gained a better appreciation of this during the audit.

Given the above gaps in policies and procedures, the audited organisations were assessed as only partially meeting the recommended standard for verifying all prospective personnel's identity.

To assist in meeting the requirements associated with Question 2, OVIC recommends that policies and procedures relating to pre-engagement screening explicitly articulate requirements and processes for verifying identity (to a particular level of assurance), and that they encapsulate these in future service agreements or contracts with third party service providers.

Question 3 – Pre-engagement screening of general workforce

Question 3 sought to answer whether the audited organisations carry out adequate pre-engagement screening measures to assess whether prospective personnel are eligible and suitable to access public sector information. This question focused on the typical pre-engagement screening checks that organisations carry out for general roles across an organisation's workforce.

The VPDSS points to PSPF Policy 12, which recommends a range of minimum pre-employment screening checks. It recommends that entities undertake pre-engagement screening to Australian Standard 4811: 2022 Workforce Screening (**AS 4811**) requirements. It also recommends conducting entity-specific checks to mitigate particular security threats applicable to the entity that are not addressed by minimum pre-engagement screening checks.

The audited organisations each conduct most of the mandatory and recommended pre-engagement checks as set out in PSPF Policy 12. However, some important checks are not conducted by all organisations – notably, the residential history check, conflict of interest declarations, and statutory declaration confirming the content of the application is truthful and complete.

However, three organisations reported undertaking entity-specific checks. These were Commission for Children and Young People (**CCYP**) which undertakes child safety-related checks as well as Victorian Funds Management Corporation (**VFMC**) and Victorian Managed Insurance Authority (**VMIA**) which conduct specific financial checks.

All organisations use third-party service providers to undertake at least some of their pre-engagement screening checks. It was notable during the audit, however, that the organisations needed to seek advice from their third-party service providers about the nature of checks they undertake. This was particularly the case for identity checks.

In conclusion, three audited organisations were assessed as substantially satisfying the criteria that supported Question 3, mainly due to the range of pre-engagement screening checks undertaken, and the requirement that a satisfactory outcome from these checks is a condition of employment with the audited organisations. The Department or Premier and Cabinet (DPC) was rated lower than the other organisations as it conducts a narrower range of checks for its general workforce. In contrast, the entity-specific checks undertaken by CCYP and VFMC contributed to their higher ratings.

To assist in addressing the criteria associated with Question 3, OVIC recommends that organisations review the suite of pre-engagement checks they undertake for their general roles. Additionally, organisations should liaise with third-party providers to clearly define and document the requirements of any pre-engagement screening checks they have them perform on the organisation’s behalf, with a view to ensuring that all checks are undertaken consistently and meet all the relevant standards.

Question 4 – Additional pre-engagement screening commensurate with risk

Question 4 sought to answer whether organisations undertake additional pre-engagement screening of personnel that is commensurate with the risk profile of their roles. It considered whether organisations carry out additional pre-engagement screening measures for high-assurance roles, beyond standard pre-engagement checks conducted for general roles.

This question reflected the varying information security risks that different roles carry, and that a one-size-fits-all approach to pre-engagement screening is often not appropriate.

As mentioned in Question 1, none of the audited organisations demonstrated a thorough, systemic approach towards understanding the risk profile of their workforce. However, DPC goes some way towards this, through its identification of certain positions requiring security clearances. In contrast, CCYP, VFMC and VMIA provided explanations as to why security clearances are not relevant to their organisational context, and/or the reasons they do not conduct security clearances.

However, despite its conduct of security clearances, DPC does not have clear policies, processes and procedures relating to additional pre-engagement screening checks for high-assurance roles. It is also unclear what assurance DPC has that additional pre-engagement screening checks are conducted to an appropriate standard, given the age of the agreement currently in place with a third-party provider, and the lack of currency of the content of that agreement.

OVIC is also concerned that aspects of the other three organisations’ pre-engagement screening are currently inadequate, as their policies and procedures do not cover additional pre-engagement checks for high-assurance roles, including those with access to security classified information and systems.

Nonetheless, CCYP, VFMC and VMIA showed some appreciation of the fact that particular roles can attract increased risk, even where they do not involve access to information assets rated as PROTECTED or above.

In summary, the lack of identification of positions requiring additional forms of pre-engagement screening, together with the lack of registers of such positions, demonstrates that the audited organisations have not fully satisfied the criteria addressing this audit question.

Given the above deficiencies, only DPC was assessed as substantially meeting the criteria, while CCYP, VMIA and VFMC were assessed as partially meeting the criteria.

To assist in meeting the requirements associated with Question 4, OVIC recommends that DPC update its documentation to reflect current expectations of, and services provided by, the third-party service provider which performs vetting assessments on its behalf, together with processes for ensuring that service provider carries out security clearance assessments to the appropriate standard.

OVIC also made a series of subsequent recommendations to all audited organisations, including those who are not currently undertaking security clearances. They include, after undertaking a workforce review (recommended in Question 1) organisations should consider defining and strengthening pre-engagement screening measures for high-assurance roles, creating a register of positions requiring security clearances (if relevant), and making sure that third-party providers who undertake personnel security vetting checks have appropriate agreements and supporting processes in place to ensure security clearances are undertaken to an appropriate standard.

OVIC also recommended that all audited organisations improve their understanding of the security value of their information holdings and workforce risk profiles, as a critical input into an informed workforce review.

Recommendations

Recommendation 1 to CCYP, DPC, VFMC, VMIA

Review existing personnel security policies and procedures with a view to:

- Producing a clear, comprehensive and cohesive personnel security policy and associated procedures covering pre-engagement screening for all personnel and positions.
- Clearly articulating the eligibility and suitability requirements that apply to contractors and other temporary or short-term staff.
- Integrating the most recent personnel security measures, including updated practices set out in the PSPF, VPDSS and guidance, and AS 4811.
- Clearly defining roles, responsibilities and accountabilities for pre-engagement screening.
- Creating clear linkages between personnel security policies and procedures, and the organisation’s broader security policies, human resources policies, and its risk management framework.
- Specifying the timing of pre-engagement checks.
- Integrating clear personnel eligibility and suitability requirements into human resource management documentation.

- Implementing a policy review cycle for personnel security documentation.

Recommendation 2 to CCYP, DPC, VFMC, VMIA

Conduct an updated review of their workforce to:

- Determine the risk profile of the various roles across the organisation (including identification of general roles and high-assurance roles).
- Review personnel security policies and procedures to ensure they set out adequate pre-engagement requirements for both general and high-assurance roles.

Recommendation 3 to CCYP, DPC, VFMC, VMIA

Review existing identity pre-engagement screening policies and procedures with a view to:

- Updating content and aligning the organisation's practices with those set out in the NIPG, including identity verification to at least LOA 3 of the guidelines.
- Using the DVS for Australian issued primary identification documents.
- Providing clear instructions to authorised personnel (including third parties) on their role in undertaking identity verification.

Recommendation 4 to CCYP, DPC, VFMC, VMIA

When engaging with a third-party service provider to undertake identity verification on the organisation's behalf:

- Ensure that the service agreement or contract clearly specifies the requirements around meeting LOA 3 of the NIPG, including use of the DVS.
- Obtain ongoing assurance that the service provider meets the requirements of at least LOA 3 of the NIPG, including use of the DVS.

Recommendation 5 to CCYP, DPC, VFMC, VMIA

Review the suite of pre-employment checks they undertake against best practice material, with a view to including relevant checks that are not currently undertaken.

Recommendation 6 to CCYP, DPC, VFMC, VMIA

Liaise with their third-party service providers to understand and document the requirements of each pre-engagement screening check, with a view to ensuring that all checks meet the relevant standards outlined in PSPF Policy 12, NIPG and AS 4811, or equivalent.

Recommendation 7 to DPC

Update documentation regarding security clearances to reflect the current expectations of, and service provided by, the third-party service provider, together with processes for ensuring the service provider carries out security clearances to the appropriate standard.

Recommendation 8 to CCYP, DPC, VFMC, VMIA

After conducting the workforce review referred to in Recommendation 2:

- consider strengthening pre-engagement screening measures for high-assurance roles; and
- establish and maintain a register of positions that require security clearances, including when the need for a security clearance will be assessed.

Recommendation 9 to CCYP, DPC, VFMC and VMIA

Ensure that for any position identified as requiring a security clearance, the security clearance process is undertaken by an authorised vetting agency, with appropriate processes in place to ensure the vetting agency carries out security clearances to the appropriate standard.

Recommendation 10 to CCYP, DPC, VFMC and VMIA

Improve organisational understanding of the security value of the information holdings and risk profiles associated with the various roles and functions across the workforce, as a critical input into an informed workforce review.

Background

The VPDSS

2. The VPDSF and accompanying VPDSS were released in 2016. Section 88 of the *Privacy and Data Protection Act 2014* (**PDP Act**) sets out that organisations which are bound by Part 4 (**organisations**) of the Act must comply with the VPDSS.

3. The VPDSS are consistent with national and international standards and describe the Victorian Government's approach to protecting public sector information and systems[5]. The risk management approach adopted by the VPDSS empowers organisations to identify and manage their unique risks.

4. OVIC has published implementation guidance to assist organisations to implement the VPDSS. The implementation guidance includes elements underpinning each standard as well as primary source material based on best practice.[6]

Purpose of the audit

5. The audit was carried out under section 8D(2)(b) of the PDP Act, to ascertain whether the four organisations subject to the audit have policies, procedures, and practices that adequately address personnel security in the pre-engagement phase of the personnel lifecycle. For the purpose of this audit, the pre-engagement phase includes the merit selection process being concluded up until new personnel commence in a role or take on a new function.

6. OVIC focused on pre-engagement activities, as they often act as the first line of defence in mitigating agencies' personnel security risk. This is also an area where OVIC frequently sees gaps and risks to public sector resources.

Standard 10

7. The audit sought to assess VPS organisations' practices against pre-engagement aspects of Standard 10, with reference to specific audit criteria, to express an opinion about the effectiveness of those organisations in ensuring the eligibility and suitability of all personnel. Standard 10 sets out the following requirement in relation to personnel security:

[5] The term 'public sector information' is used in this report as having the same meaning as 'public sector data'. 'Public sector data is defined in section 3 of the PDP Act as 'any information (including personal information) obtained, received or held by an agency or body to which Part 4 applies, whether or not the agency or body obtained, received or holds that information in connection with the functions of that agency or body'.

[6] OVIC website, https://ovic.vic.gov.au/wp-content/uploads/2023/10/VPDSS-V2.0-Implementation-Guidance-V2.2_web-version.pdf .

An organisation establishes, implements and maintains personnel security controls addressing all persons' continuing eligibility and suitability to access public sector information.

8. The objective of Standard 10 is to mitigate an organisation's personnel security risks and provide a consistent approach for managing all persons with access to public sector information.

Standard 10 elements and primary source material

9. There are eight elements[7] underpinning Standard 10. The following four elements were relevant to this audit:

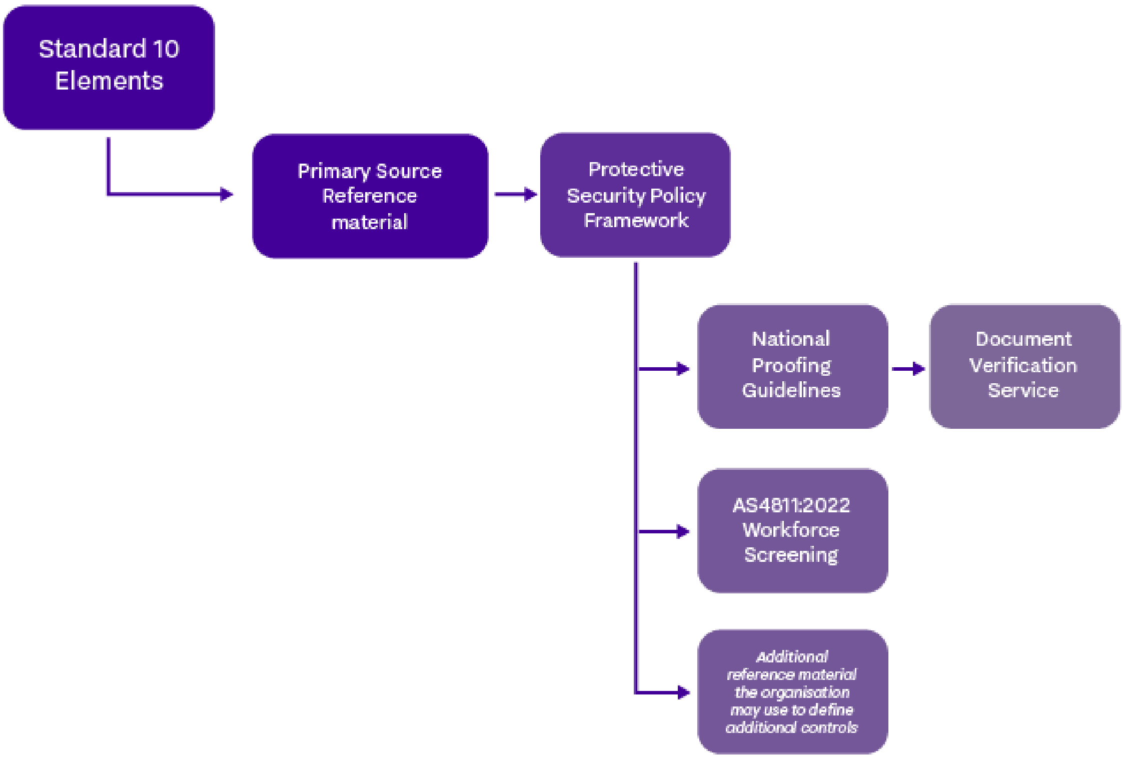
   - E10.010 The organisation's personnel security policies and procedures address the personnel lifecycle phases of:
     - Pre-engagement (eligibility and suitability)
     - Engagement (ongoing and re-engagement)
     - Separating (permanently and temporarily).
   - E10.020 The organisation verifies the identity of personnel, re-validates, and manages any changes as required.
   - E10.030 The organisation undertakes pre-engagement screening commensurate with its security and probity obligations and risk profile.
   - E10.070 The organisation undertakes additional personnel screening measures commensurate with the risk to support roles requiring high-assurance and/or handling security classified information.

10. OVIC's implementation guidance for the VPDSS identifies primary sources for each element within each Standard. A primary source is the reference point from where the element has been primarily derived. References are intended to provide implementation advice and point to best practice, including Australian and International Standards, federal and state government guidance, and tailored guides developed by OVIC.

11. **Figure 1** shows the relationship between Standard 10 Elements and the primary source reference material applicable in this audit.

[7] Elements are security measures that modify risk. Elements often depend on a supportive control environment to be effective. A control environment can be a set of standards, processes and structures, authorities, funds, and resources that provide the basis for applying controls across the organisation.

Figure 1: Relationship between Standard 10 Elements and the primary source reference material


Standard 10 Elements
Primary Source Reference material
Protective Security Policy Framework
National Proofing Guidelines
Document Verification Service
AS4811:2022 Workforce Screening
Additional reference material the organisation may use to define additional controls

Protective Security Policy Framework

12. The key primary source relevant to this audit is PSPF Policy 12.[8]

13. The PSPF is an Australian Government framework that seeks to assist Australian Government entities to protect their people, information and assets. It sets out government protective security policy and supports entities to effectively implement the policy across the following outcomes: security governance; information security; personnel security; and physical security.[9]

14. PSPF Policy 12 covers the eligibility and suitability of personnel. In turn, PSPF Policy 12 refers to some further reference material that also apply to this audit, notably:

- NIPG: a robust, yet flexible risk-based approach to identity proofing[10]

[8] While PSPF Policy 12 is an Australian Government framework, it applies to the VPS organisations audited because they have selected it in their control libraries for implementation of Standard 10.

[9] Australian Government, Protective Security Policy Framework, https://www.protectivesecurity.gov.au/about .

[10] Attorney-General's Department, National Identity Proofing Guidelines, https://www.ag.gov.au/national-security/publications/national-identity-proofing-guidelines .

- DVS: checks whether the personal information on a range of Australian government identity documents matches the original record, making it harder for people to use fake identity documents[11].

AS 4811

15. A second significant primary source for this audit is AS 4811. The objective of this document is to 'set out requirements and guidance for the development of organisational specific workforce screening policies and processes'.[12]

Definition of 'personnel'

16. For the purposes of this audit, 'personnel' includes full-time or part-time employees and trainees.

17. It also includes 'contractors' – these are individuals who carry out work on a non-permanent basis and who are not directly employed by a VPS organisation. They are often engaged through a labour hire agency for reasons such as providing specialised skills, working on a particular project, or covering temporary absences of ongoing staff.

18. For the purposes of this audit the term 'personnel' does not include consultants.

How we conducted the audit

19. The audit method involved:

    - Issuing a self-assessment questionnaire to audited organisations, which asked for organisation responses to detailed audit questions, along with submission of supporting evidence

    - Reviewing initial submissions and issuing each audited organisation with a tailored set of questions relating to their submission and evidence provided

    - Speaking with audited organisation personnel where relevant or requested

    - Issuing a preliminary assessment of proposed findings, conclusions and recommendations to each organisation

    - Reviewing organisations' responses to the preliminary assessment and any supplementary evidence provided

[11] ID Match website, https://www.idmatch.gov.au/ .

[12] Standards Australia Store, https://store.standards.org.au/product/as-4811-2022 .

- Producing a final audit report and inviting a formal response from the audited organisations. These responses are included at **Annexure C** of this report.

How we assessed the organisations

20. To reach an audit conclusion, OVIC assessed the organisations against four audit questions and associated criteria:

1. Do the organisation's personnel security policies and procedures address the pre-engagement (eligibility and suitability) phase?
2. Does the organisation verify the identity of its personnel?
3. Does the organisation undertake pre-engagement screening of all personnel?
4. Does the organisation undertake additional pre-engagement screening of personnel that is commensurate with the risk profile of their roles?

21. All audit criteria are set out at **Annexure A** to this report, and are referenced against each of the corresponding questions, and explained in subsequent sections of this audit report.

22. Each organisation was rated against the audit questions using the following rating scale:

- **Yes** – the organisation fully meets the audit criteria
- **Substantially** – the organisation meets most of the audit criteria
- **Partially** – the organisation meets some of the audit criteria
- **No** – the organisation does not meet the audit criteria.

Organisations selected for the audit

23. The audited organisations were selected for inclusion in the audit based on the following characteristics and criteria:

- Organisations that handle information at Business Impact Level (**BIL**)[13] 3 or above (see below)

- Organisations' self-reported maturity rating of 'core' or 'managed' for Standard 10 as reported by the organisations on their 2022 Protective Data Security Plan (**PDSP**)

- Organisations that indicated they have implemented the relevant elements of Standard 10

- The number of employees (with the view to auditing organisations of different sizes)

- The significance or importance of the organisations' operations to the social, economic or physical environments

- The likely sensitivity of information assets held by the organisations.

Protective Data Security Plans

24. Every two years, certain organisations must submit to OVIC a PDSP. A PDSP is a document that outlines an organisation's plan to address the VPDSS and elements applicable to the organisation.

25. As part of the PDSP, organisations are asked to provide a breakdown of the organisation's information assets, against the following protective markings and corresponding BIL rating reflecting the outcomes of a confidentiality assessment:

• BIL 1	OFFICIAL
• BIL 2	OFFICAL: Sensitive
• BIL 3	PROTECTED
• BIL 3-4	Security classification // Cabinet-in-Confidence
• BIL 4	SECRET
• BIL 5	TOP SECRET

26. Organisations' assessment and assignment of a protective marking for their information is important because it provides an indication of the sensitivity of the material handled by an organisation, and guidance on the expected controls to maintain the confidentiality of the information. These controls include personnel security measures, extending to the type and extent of pre-engagement screening to help facilitate authorised access to eligible and suitable personnel.

[13] See OVIC Practitioner Guide: Assessing the security value of public sector information, on OVIC website: https://ovic.vic.gov.au/information-security/practitioner-guide-assessing-the-security-value-of-public-sector-information-v2-0/.

27. While shortlisting criteria for the audit included audited organisations' 2022 PDSP's reporting information assets at BIL 3 (PROTECTED) or higher, VFMC advised OVIC auditors that it had subsequently reassessed its information assets to BIL 2 or below.

28. VFMC explained that its assessment of the information assets at a BIL of 3 had been overly conservative. VFMC remained in the audit on the basis that at the time of assessing its assets, appropriate pre-engagement screening measures should have been required for relevant staff accessing and handling those assets.

29. The remaining three agencies reported holding information assets as PROTECTED: CCYP (34%), DPC (5%) and VMIA (11%). Additionally, DPC assessed 10 per cent of its assets as CABINET-in-CONFIDENCE and one per cent as SECRET and CCYP assessed one per cent as CABINET-in-CONFIDENCE.

Organisation profiles

Purpose of audited organisations

30. The broad purpose of each of the selected organisations is:

- **CCYP:** An independent statutory body that promotes improvement in policies and practices for the safety and wellbeing of children and young people in Victoria, with a particular focus on those who are vulnerable.[14]

- **DPC:** The Victorian Government department that leads whole-of-government policy and performance.

- **VFMC:** A public authority responsible for investing for the benefit of Victorians. It manages over $71 billion for 31 Victorian public authorities and related organisations.

- **VMIA:** The Victorian Government's insurer and risk adviser. Its clients include cultural institutions, major infrastructure, public schools, hospitals, emergency services, and not-for-profit organisations. In 2021–22 VMIA insured $224 billion in public assets.

Recruitment activity of the audited organisations

31. **Table 2** shows the number of staff employed by each agency, as at June 2023, while **Table 3** shows the number of new staff recruited during 2022–23.

32. Together, the tables show that recruitment activity was significant across all organisations audited when accounting for the size of the existing workforces. This emphasises the need for organisations to

[14] Of relevance to this audit, CCYP has a Memorandum of Understanding with the Department of Families, Fairness and Housing (DFFH) for support in 11 areas, including HR, IT services, and information and record management. This arrangement means that CCYP will need to work closely with DFFH to implement some of the recommendations outlined in this report.

have in place sound policies and procedures for ensuring all personnel's eligibility and suitability for the role.

Table 2: Staff numbers as at June 2023

Organisation	Ongoing full-time staff	Ongoing part-time staff	Fixed-term / casual staff	Total staff
CCYP	43	14	23	80
DPC	332	74	154	560
VFMC	89	10	25	124
VMIA	171	28	56	255

Table 3: Recruitment activity during 2022–23

Organisation	Ongoing full-time staff	Ongoing part-time staff	Fixed-term / casual staff	TOTAL staff	Contractors
CCYP	4	2	14	20	3
DPC	178	3	336	517	87
VFMC	16	3	11	30	5
VMIA	65	3	45	113	9

Question 1 - Do the organisation’s personnel security policies and procedures address the pre-engagement (eligibility and suitability) phase?

Criteria tested for Question 1

33. Audit Question 1 sought to answer whether audited organisations’ personnel security policies and procedures address the pre-engagement (eligibility and suitability) phase.

34. Organisations must set out adequate pre-engagement screening requirements in easy-to-follow policy and procedure documents. This ensures that the appropriate types of checks are carried out for each role at the appropriate time – in a consistent and thorough manner.

35. The criteria tested for this audit question were that the organisation has:

    a. personnel security policies and procedures that contain requirements that address pre-engagement screening

    b. personnel security policies and procedures that clearly articulate eligibility and suitability requirements for personnel

    c. personnel security policies and procedures that address all forms of personnel

    d. personnel security policies and procedures that require pre-engagement screening checks of all personnel to be undertaken prior to commencement in the role

    e. personnel security policies and procedures that contain adequate requirements / directions for general roles across the workforce and high-assurance roles that require additional forms of assurance

    f. personnel security policies and procedures reflective of the risk profile of their workforce.

OVIC’s assessment against Question 1

36. **Table 4** shows how OVIC assessed the organisations’ performance against Audit Question 1.

Table 4 OVIC assessment against Question 1

Organisation	OVIC's assessment
CCYP	Partially – the organisation meets some of the audit criteria
DPC	Partially – the organisation meets some of the audit criteria
VFMC	Substantially – the organisation meets most of the audit criteria
VMIA	Partially – the organisation meets some of the audit criteria

Observations against Question 1

Policies and procedures addressing pre-engagement screening

37. AS 4811 sets out that 'workforce screening policy and processes shall be developed, addressing accountability and responsibility, transparency and consistency, in order to provide effective and efficient workforce screening of candidates'. It goes on to outline aspects of what the policies and processes should include – such as information on timing, sequencing and roles and responsibilities.[15]

38. None of the audited organisations have an overarching personnel security policy, plan, procedures, or similar documentation covering the pre-engagement phase of the personnel security lifecycle. Responses from some of the audited organisations explained that such documentation is not necessary given the size, complexity and context of their organisation.

39. However, in the absence of a standalone personnel security policy, all organisations could point to a suite of documents that address personnel security factors related to the pre-engagement stage.

40. VFMC said that rather than creating standalone documentation, the structures, policies and practices comprising the personnel security framework are contained within a range of other organisational

[15] See section 2.8.2, AS 4811:2022 Workforce Screening.

documents, particularly the Recruitment and Selection Policy, Fit and Proper Policy, Code of Conduct Policy, and the Fraud, Corruption and Other Losses Policy.

41. CCYP considers that its Recruitment and Selection Policy and supporting documentation from the Department of Families, Fairness and Housing (**DFFH**) (consisting of a Pre-employment safety screening policy document and a Pre-employment safety screening procedures document) along with CCYP's Information Management and Data Security Framework, sets out its policies and procedures for pre-engagement screening. CCYP explained that it has a Memorandum of Understanding (**MOU**) in place with DFFH, under which most tasks relating to the pre-engagement phase are managed by DFFH through its human resources and payroll functions.

42. VMIA's Employee Lifecycle Policy outlines the requirements for pre-engagement screening checks and other selection assessments.

43. DPC has a range of policies and procedures addressing pre-engagement screening. They include a Pre-employment Screening Policy, Personnel Screening Policy, Personnel Screening Procedure, Personnel Screening Guidelines, and an Evidence of Identity Policy and Procedure.

Policies and procedures that articulate eligibility and suitability requirements

44. Under PSPF Policy 12, organisations must ensure the **eligibility** of their personnel who have access to government resources by:

- Verifying a person's identity using the DVS
- Confirming a person's eligibility to work in Australia.

45. All the audited organisations include reference to the requirement to have the right to work in Australia in their policies and procedures. However, this is not the case with respect to identity verification (see Question 2 for detailed analysis of the audited organisations' approaches to identity verification).

46. Under PSPF Policy 12, organisations must also obtain assurance about the **suitability**[16] of personnel to access government resources by carrying out the following checks as recommended under the Policy:

- Employment history
- Residential history
- Referees

[16] Similar suitability considerations are also set out in AS 4811.

- Nationally Coordinated Criminal History Check (**National Police Check**)[17]
- Credit history
- Conflict-of-interest declaration
- Qualifications
- Entity-specific checks.

47. All the audited organisations have human resources documentation that identifies a range of suitability checks for general roles, the most common being reference checks, qualifications and National Police Checks. Additionally, CCYP's suitability checks include a Working With Children Check (**WWCC**), while VFMC and VMIA identify a range of financial checks relevant to their organisational context. (see Question 3 for detailed analysis of the audited organisations' approaches to suitability checks for general roles across their workforces).

48. In general, the audited organisations do not have adequate documented processes or procedures underpinning their policies relating to pre-engagement screening, such as a step-by-step guide, checklist, roles and responsibilities table, or a detailed flowchart outlining who completes which tasks, when and how. However, three of the organisations presented aspects of this within their suite of documents.

49. CCYP provided a copy of DFFH's Pre-employment Screening Procedures which outline the processes for conducting a range of checks, including qualifications, right to work in Australia, National Police Check, and misconduct verification.

50. DPC has sporadic examples of 'how to' procedures, including the Employee Security and Screening Guidelines and the Reference Check Guide and Template.

51. VFMC's Recruitment and Selection Policy includes a table setting out a broad overview of steps and responsibilities during the recruitment and job offer processes. It allocates the responsibilities between the recruiting manager, people team, and recruitment partner. VFMC also has a new starter checklist which contains a detailed list of actions, along with responsibilities.

52. VMIA did not submit documents detailing the processes for conducting pre-engagement screening.

Policies and procedures addressing coverage and timing of pre-engagement screening

53. Broad coverage of personnel types within organisations' policy and procedure documentation is important, as all forms of personnel have access to organisational resources. This does not necessarily mean that all personnel types are subject to the same pre-engagement screening processes. The key

[17] While Nationally Coordinated Criminal History Check has been the official name for these checks since 2018, the term 'National Police Check' remains commonly used and is used in this report for ease of understanding.

requirement is that policies and procedures explicitly capture all forms of personnel and set out the pre-engagement screening process which applies to each of these.

54. DPC's Pre-employment Screening Policy states that it applies to all ongoing, fixed term and casual appointments, graduates, internships, youth employment trainees and work placements in excess of six weeks. It also covers labour hire workers and independent contractors.

55. CCYP's Recruitment and Selection Policy identifies ongoing, fixed term and casual employees, while VFMC's Recruitment and Selection Policy states that the policy applies to the recruitment of all resources at VFMC, including permanent and contractor positions.

56. VMIA's Employee Lifecycle Policy does not identify which personnel types its screening requirements apply to, but appears to be for any role longer than 6 months – as it references a Temporary People Resources Policy that applies to roles of less than 6 months.

57. However, whilst contractors and other short-term resources are mentioned in policy and procedure documents across the audited organisations, the documents contained insufficient information about the application of eligibility and suitability requirements to these personnel types.

58. Such roles are usually dealt with in policy and procedure documentation as being subject to differing recruitment processes – mainly through the use of external recruitment agencies, but there is a lack of detail across the audited organisations on whether differing pre-engagement screening requirements will also apply.

59. While CCYP and VFMC's recruitment and selection policies state that they apply to all recruitment, the documents contain sections describing specific recruitment arrangements for contractors. These sections do not explicitly set out whether differing eligibility or suitability requirements apply or not.

60. The DFFH Pre-employment Screening Policy (which applies to CCYP) requires that while the misconduct process is not mandatory for non-advertised or short-term roles of six months or less, consideration should be given to the level of risk inherent in the role to determine whether it is necessary for preferred applicants in these roles.

61. VMIA's Temporary People Resources Policy notes that 'appropriate reference checks, employment checks and other certifications as reasonably requested must be provided' without further detail on what checks are appropriate for certain roles, or the process for carrying out or verifying these checks.

62. DPC's Pre-employment Screening Policy specifically references requirements around police checks for labour hire workers and independent contractors, but does not cover other checks that may be required for these types of personnel.

63. Similarly, for those suitability checks that are specifically referenced for contractor roles, these are not accompanied by a clear and unambiguous procedure for ensuring these are consistently implemented.

64. For example, DPC's policy states that police checks for independent contractors can be undertaken by requesting the relevant recruitment agency or provider to perform a standardised check, or by

instructing the People and Culture branch to undertake the check. The lack of clarity here around process, responsibility, and verification that checks have been undertaken (and to what standard), introduced risks.

65. There were different approaches amongst the audited organisations in terms of addressing the timing of conducting pre-employment screening checks.

66. According to PSPF Policy 12, pre-employment screening should be conducted and finalised after the conclusion of the merit selection process but prior to an offer of employment or contract. Where checks are not completed prior to engagement, the PSPF recommends that organisations make the employment or contract conditional on satisfying the required checks within a reasonable timeframe.

67. CCYP's Recruitment and Selection Policy states that the offer of employment is conditional upon and subject to the satisfactory completion of the pre-employment checks outlined in the policy, namely reference checks, safety screening (WWCC and police check), misconduct screening, and working rights.

68. VMIA's Employee Lifecycle Policy similarly states that all candidates are required to complete probity checks prior to commencing employment, including the right to work in Australia, employment history, academic credentials check, police check and, for applicable roles, financial background checks.

69. VFMC's Recruitment and Selection Policy states that all offers of employment are subject to receipt of at least two satisfactory references. However, it does not state when the remaining background checking should be completed. VFMC advised OVIC that screening is commenced but not necessarily concluded before the joining date, with the exception of police checks which must be completed before the joining date.

70. DPC's Pre-employment Screening Policy states that misconduct screening checks must be verified by the recruitment team prior to an offer of employment being made. Notably, however, the same policy states that the National Police Check can be completed within three months of the start date. DPC advised the audit team that police checks can take anywhere from one to eight weeks, so it is not feasible to withhold progressing with an offer on this basis.

71. According to the Australian Criminal Intelligence Commission (ACIC) website, around 70 per cent of National Police Checks are completed in real-time, with results being returned to the requesting organisation within minutes. Around 30 per cent of checks are referred to one or more police agencies because a 'potential match' is found, of which 87 per cent will be processed within 15 business days.[18]

[18] Australian Criminal Intelligence Commission website, https://www.acic.gov.au/services/national-police-checking-service/find-out-more-information/how-service-works .

Policies and procedures reflective of risk profiles of workforce - containing adequate requirements for both general roles and high-assurance roles

72. In line with AS 4811, the level of screening conducted on a candidate should be commensurate with the level of risk posed by that particular role, to organisational objectives, processes and business impact (such as reputation damage, financial loss or harm to individuals).

73. Different roles are likely to attract different levels of risk, so a one-size-fits-all approach to pre-engagement screening is generally not appropriate. For example, there should be different pre-engagement screening requirements for a junior staff member who has limited access to information that does not go beyond BIL 2, compared to a senior executive who has access to information rated at BIL 4 and who has significant financial delegations.

74. As such, understanding the risk profile of the workforce is an important foundational step required to properly informing an organisation's policies and procedures relating to pre-engagement screening. The risk profile of a workforce may be informed by the:

    - Various roles across the organisation
    - Associated functions of each role
    - Security value of information and systems each role has access to
    - Level of influence of each role
    - Current control environment of the organisation.

75. The workforce risk profile should then be reflected in relevant policy and procedure documentation that explains which roles are deemed to be general, which roles are high-assurance[19], and the differing pre-engagement screening requirements that apply to different categories of roles (see Question 4 for detailed analysis of the audited organisations' approaches to conducting additional pre-engagement screening for high-assurance roles).

76. None of the audited organisations demonstrated that their policies and procedures covering pre-engagement screening were informed by a thorough, systematic approach towards understanding the risk profile of their workforce. Instances of policies and procedures reflecting an understanding of differing risk profiles for general and high-assurance roles were largely sporadic and vague.

77. VMIA's Cyber Security Policy states that background verification checks should be proportional to the classification of information the candidates will have access to but does not give any further detail beyond this.

[19] *High-assurance* roles are ones for which the organisation requires additional forms of assurance. This need for heightened assurance may be based upon the functions associated with the role, the level of access to information / systems (including security classified information), the level of influence the role has on the organisation and/or the risk profile of the role.

78. According to VMIA documentation, as well as the suitability checks that apply to all general roles, additional financial background checks (including credit history and bankruptcy checks) are required ‘for applicable roles’. VMIA explained in its response to OVIC that ‘applicable roles’ are those which involve a financial component but this was not expressed in any of its policies or procedures.

79. CCYP’s policy and procedure documentation sets out specific screening techniques in recognition of risks posed by the potential to have contact with children. This involves the requirement to hold a WWCC as well as providing interview templates with mandatory child safety related values-based questions.

80. However, CCYP documentation sets out that these requirements relate to all personnel. There was no evidence that CCYP had identified specific high-assurance roles and commensurate additional pre-screening measures in its policies and procedures.

81. CCYP’s Recruitment and Selection Criteria states that a successful candidate must complete a declaration about their misconduct history and that if a candidate is applying for a role judged to be ‘higher risk’, their declaration may be verified with previous employers, even if they did not declare any misconduct. However, there is no detail provided on how to assess which roles are ‘higher risk’ or who should conduct this assessment.

82. Some of DPC’s personnel security policies and procedures appear to be informed by an assessment of the risk associated with certain roles. This is evident in some documents where they refer to pre-engagement requirements for general roles across the workforce, as well as additional requirements for high-assurance roles.

83. For example, the DPC Personnel Screening Policy establishes that in addition to requirements for general roles, a Security Clearance check will be required for a ‘Designated Security Assessed Position’(**DSAP**). A separate document notes that DSAPs include the Secretary, Deputy Secretaries, General Counsel, and various staff of the Community Security and Emergency Management Branch.

84. However, it is unclear how DPC determines which roles require security clearances and whether further roles require a security clearance beyond those listed in this DSAP document, given DPC does not have a register of positions requiring security clearance (see discussion in Audit Question 4).

85. VFMC has a Fit and Proper policy which applies to key executives, but the pre-engagement screening measures that are outlined in the policy do not differ significantly from those that apply to the general workforce. The exception is the requirement to provide probity-self declarations as well as a declaration of financial and other interests. However, all such declarations are made once a person has joined VFMC rather than during the pre-engagement phase.

86. VFMC stated that all functions are considered equal risk with respect to security vulnerabilities. VFMC’s position is that policies and procedures relating to pre-engagement screening apply in the same way to all roles and do not differentiate between general and high-assurance roles.

Findings and conclusions against Question 1

87. All organisations had a suite of documents containing requirements for pre-engagement screening. However, OVIC found that, in general, policies and procedures did not adequately capture all pre-engagement screening requirements in a detailed, coherent, and consistent way.

88. Overall, OVIC found that policies and procedures lacked clarity and detail around pre-engagement requirements and processes, with notable deficiencies including:

- A lack of a document hierarchy or linkages that clearly guide readers through the suite of relevant documents or reference materials
- Procedure documents that contain only high-level advice rather than 'how to' guidelines or instructions
- Gaps, duplication or inconsistency of content across documents
- Lack of clarity of roles and responsibilities for carrying out pre-engagement screening actions
- Lack of clarity around sequencing and timing of pre-engagement screening actions
- Incorrect or outdated legislative or policy references
- Outdated policy and procedure documents, or documents that have not been reviewed within reasonable policy cycles
- A lack of contact details for seeking further information from the policy owner.

89. OVIC therefore found that these deficiencies created a risk that staff (and particularly new staff) seeking to carry out pre-engagement screening would be confused over the correct sources and processes to use.

90. DPC's various documents were particularly difficult to navigate. DPC submitted to the audit six policy and procedure documents that had very similar titles. They were generally not comprehensive, and their content was inconsistent in parts. There was no discernible document hierarchy pointing users to other relevant policies and procedures. The documents were mostly undated, and did not identify a policy review cycle. These gaps and deficiencies mean that DPC's suite of documents is likely to be difficult for users to understand and apply in practice.

91. Some agency responses to OVIC regarding questions 2 – 4 illustrated that some practices exist and actions occur, despite not being clearly specified in documentation. However, where the requirements and processes for pre-engagement screening are not clearly reflected in organisational documentation, it creates a risk of instances where pre-employment screening is not carried out properly, consistently, or at all.

92. While not a mandatory criterion within this audit, OVIC believes that organisations could benefit from having a dedicated and comprehensive personnel security policy which addresses pre-engagement screening. This would sharpen the focus on personnel security risks and communicate in a clear, consistent way the requirements of all staff in addressing personnel security risks and requirements.

93. A standalone policy[20] need not be a lengthy document, but would contain (at least) the following features:

- A list or description of staff the policy applies to
- Roles and responsibilities for personnel security
- Eligibility and suitability requirements for general roles
- Roles or categories of roles identified as 'high-assurance' and the additional pre-engagement screening requirements for these roles
- Arrangements for contractors and other temporary or short-term staff
- Pre-engagement screening procedures explaining timing and sequencing of actions (with clear links to any associated procedure documents)
- Links to relevant legislation, policies, and guidance
- Policy review cycle
- Contact information of the policy owner
- Approval / Authorisation by the relevant organisational authority.

94. Organisations' pre-engagement policies and procedures should also be integrated into their human resource management documentation. This would help to ensure that both hiring managers and People and Culture/Human Resources personnel are informed about eligibility and suitability requirements and their respective responsibilities in the screening process.

95. OVIC also found that organisations' policies and procedures for pre-engagement screening were not adequately tailored to the differing risk profiles of roles across their workforces.

96. Each organisation had policies and procedures setting out eligibility and suitability requirements for their general workforce. However, some organisations did not identify any high-assurance roles and, importantly, did not document pre-engagement screening measures commensurate with the risk profile of these roles. In OVIC's view, it is highly unlikely that there are no such high-assurance roles in

[20] Any such policy should be based on the most up-to-date advice as outlined in the PSPF, VPDSS and AS 4811.

these organisations meaning that a one-size-fits-all approach to pre-engagement screening is not appropriate.

97. While there were some instances of documentation requiring additional screening for particular roles, in OVIC's view even these instances reflected only a partial exercise in assessing the workforce risk profile and identifying high-assurance roles.

98. Additionally, organisations' policies and procedures do not adequately address eligibility and suitability requirements for contractors and other short-term roles.

99. The lack of clarity here creates risks of contractors being subjected to inadequate pre-engagement screening or instances of pre-engagement screening processes not being followed in relation to contractors. This is a risk that has previously been identified by the Victorian Auditor-General[21] and OVIC has also considered instances of this risk materialising.[22]

100. All roles should be subject to sufficient and appropriate pre-engagement screening, regardless of the length of engagement. Should organisations deem that contractor and other short-term roles are not subject to the same pre-engagement screening as ongoing roles, they must nevertheless explicitly set out in policies and procedures the specific measures it applies to manage the personnel security risks associated with such positions.

101. OVIC recommends that pre-engagement screening is completed after the conclusion of the merit selection process, but before an offer of employment is made. It is therefore concerning that the policies and procedures of some organisations did not mandate such an approach.

102. Of particular concern was DPC's position that National Police Checks may be completed up to three months after personnel have commenced in the role. OVIC is concerned that DPC's current practices could foreseeably result in an otherwise unsuitable individual (that is, due to a relevant criminal history) having access to systems containing public sector information for a period of up to three months before their unsuitability is detected. This introduces significant personnel security risks for DPC which are not adequately mitigated by the signing of a statutory declaration from the candidate.[23]

[21] Victorian Auditor-General's Office, *Personnel Security: Due Diligence Over Public Service Employees*, May 2020, https://www.audit.vic.gov.au/sites/default/files/2020-05/20200521-Personnel-Security-report_0.pdf?. VAGO's audit found that across organisations it audited, only 39 per cent of a sample of 299 contractors had a police check conducted by either the supplier labour hire agency or the organisation's hiring manager. As such, it concluded that up to 3430 contractors worked in the VPS over a two-year period, without being checked for a criminal history.

[22] OVIC, *Misuse of Department of Health information by third party employees during pandemic response*, 2023, https://ovic.vic.gov.au/wp-content/uploads/2023/07/DOH-INV-20230628-Report-v1-1.pdf. This investigation revealed that confusion between the Department of Health and its provider about responsibility for conducting police checks meant that no police checks were conducted for a period of 8 months in relation to individuals who were engaged to assist in meeting the demands of the COVID-19 public directions hotline. This led to the engagement of an individual with a criminal history and who was on bail at the time. The individual used personal information from a departmental system to attend the home of a woman who was isolating, pretended to be an inspector from the department and used threats to try and coerce the woman into participating in sexual acts.

[23] For an example of such a risk materialising, see: *OVIC, Misuse of Department of Health information by third party employees during pandemic response* (25 July 2023) available at: https://ovic.vic.gov.au/regulatory-action/misuse-of-department-of-health-information-by-third-party-employees-during-pandemic-response/.

103. OVIC recognises that organisations cannot control the length of time taken to complete a National Police Check. However, it is OVIC's view that given most new appointments require a lead time of two or more weeks, it should be possible for organisations to obtain the results of a National Police Check before the candidate starts in the role, or soon after. To assist in achieving this, applications for National Police Checks should be submitted in a timely manner. Requirements in organisational policies should refer to timings for submission, rather than referring only to timing of completion of a police check.

104. Based on the above observations and findings, OVIC rated three of the organisations as 'partially' against question 1.

105. OVIC rated VFMC as 'substantially' largely on the basis that its suite of policies and procedures covering pre-engagement screening stood out as being the most clear, concise and easy to follow with fewer of the gaps and deficiencies seen in the other organisations' documents. Notably, its Recruitment and Selection Policy listed relevant eligibility and suitability requirements; assigned responsibility for conducting different checks; and specified the stage of the recruitment process when checks occur.

Recommendations regarding personnel security policies and procedures

Recommendation 1 to CCYP, DPC, VFMC, VMIA

106. Review existing personnel security policies and procedures with a view to:

- Producing a clear, comprehensive and cohesive personnel security policy and associated procedures covering pre-engagement screening for all personnel and positions.

- Clearly articulating the eligibility and suitability requirements that apply to contractors and other temporary or short-term staff.

- Integrating the most recent personnel security measures, including updated practices set out in the PSPF, VPDSS and guidance, and AS 4811.

- Clearly defining roles, responsibilities and accountabilities for pre-engagement screening.

- Creating clear linkages between personnel security policies and procedures and the organisation's broader security policies, human resources policies and its risk management framework.

- Specifying the timing of pre-engagement checks.

- Integrating clear personnel eligibility and suitability requirements into human resource management documentation.

- Implementing a policy review cycle for personnel security documentation.

Recommendation 2 to CCYP, DPC, VFMC, VMIA

107. Conduct an updated review of their workforce to:

- Determine the risk profile of the various roles across the organisation (including identification of general roles and high-assurance roles).

- Review personnel security policies and procedures to ensure they set out adequate pre-engagement requirements for both general and high-assurance roles.

Question 2 - Does the organisation verify the identity of its personnel?

Criteria tested for Question 2

Audit criteria

108. Question 2 sought to answer whether organisations verify the identity of their personnel. An identity check helps to establish confidence in a person's identity and provides organisations with a level of assurance about the prospective employee.

109. The consequences of incorrectly identifying a person may include fraud risks, security risks, privacy risks, and downstream risks (a person using an identity credential or record issued or created by one organisation to commit identity crime against other organisations).[24]

110. The criteria tested for Question 2 were that the organisation:

(i). has procedure(s) that clearly document how to undertake identity verification to LOA 3 under the NIPG using the DVS

(ii). has assurance that identity verification checks are undertaken to an appropriate standard, including instances where a third-party undertakes these checks on behalf of the organisation

(iii). has informed, qualified and skilled personnel / providers undertaking identity verification.

(iv). (if relevant) uses accredited / authorised third parties to provide / undertake identity verification on the organisation's behalf.

[24] NIPG, https://www.homeaffairs.gov.au/criminal-justice/files/national-identity-proofing-guidelines.pdf .

National Identity Proofing Guidelines and the Document Verification Service

111. PSPF Policy 12 sets out that entities must verify the identity of individuals as part of pre-engagement screening. The Policy:

- States that entities must verify a person's identification documents with the issuing authority by using the DVS for Australian issued primary identification documents.

- Recommends that the identity of all new personnel be verified to at least LOA 3 of the NIPG[25].

112. The DVS is a national real-time system that allows participating organisations to compare an individual's identifying information on particular government issued documents with the issuing government agency. The DVS is a secure system that operates 24/7 and matches key details contained on Australian-issued identifying credentials providing a 'yes' or 'no' answer within seconds.[26]

113. The NIPG provide a more robust, yet flexible risk-based approach to identity proofing than the traditional '100 point ID check'. LOA 3 aims to provide 'high' confidence in a claimed identity through obtaining evidence across 5 objectives to confirm[27]:

(a). The uniqueness of the identity in the intended context

(b). The claimed identity is legitimate

(c). The operation of the identity in the community over time

(d). The linkage between the identity and the person claiming the identity

(e). The identity is not known to be used fraudulently.

OVIC's assessment against Question 2

114. None of the organisations demonstrated that they fully meet the recommended standard for verifying all prospective personnel's identity. **Table 5** shows how OVIC assessed the organisations' performance against audit question two.

[25] NIPG, https://www.ag.gov.au/sites/default/files/2023-08/national-identity_proofing-guidelines.pdf

[26] NIPG, p.25.

[27] Tables 2 and 3 of the NIPG set out the description, aim, controls, method of processing and requirements of LOA 3 (high level of assurance).

Table 5 OVIC assessment against Question 2

Organisation	OVIC’s assessment
CCYP	Partially – the organisation meets some of the audit criteria
DPC	Partially – the organisation meets some of the audit criteria
VFMC	Partially – the organisation meets some of the audit criteria
VMIA	Partially – the organisation meets some of the audit criteria

Observations against Question 2

Identity verification procedures

115. None of the audited organisations had clear policies and procedures on how to undertake identity verification to the appropriate standard.

116. CCYP achieves this to some extent, with DFFH’s document on pre-employment screening, which mentions identity verification and that fact that it forms part of the National Police Check. In contrast, DPC submitted a standalone document, Evidence of Identity and Background Check Policy & Procedure, which does not meet the requirements of the NIPG and DVS, and which also conflicts with other advice that DPC conducts identity verification through a third-party provider (see below). VFMC’s and VMIA’s documentation did not mention identity verification.

117. All four organisations submitted to OVIC that, in practice, they conduct identity verification through the National Police Check process, conducted by respective third-party providers.

118. While these service providers are engaged primarily for the purpose of carrying out National Police Checks, upon reviewing relevant materials, OVIC was satisfied that verifying the identity of an applicant forms a necessary part of the National Police Check process, as discussed below.

119. Nonetheless, organisations were generally unaware of the process and requirements for identity verification involved as part of National Police Check process – which was insufficiently addressed in policies and procedures.

120. Additionally, DPC provided conflicting evidence regarding its identity verification process. DPC advised OVIC that it verifies identity through a mandatory National Police Check conducted by a third-party service provider. This contrasts with DPC's Evidence of Identity and Background Check Policy & Procedure submitted with its self-assessment, which requires that identity verification be undertaken by an authorised officer of DPC. It is therefore likely that the DPC policy and procedure document inaccurately describes current practice, noting that it appears to be nearly ten years old.

Assurance that identity verification checks are undertaken to appropriate standard

121. The four audited organisations did not initially provide assurance that identity verification carried out by their third-party service providers as part of a National Police Check fully meets the requirements for obtaining a LOA 3 under the NIPG, or that they use the DVS. Such requirements are not outlined in their service agreements with their respective providers.

122. As such, the audited organisations sought further information on their service providers' processes for identity verification during the audit. As a result, organisations were able to provide some level of assurance to OVIC.

123. Each of the service providers conducting National Police Checks on behalf of audited organisations are accredited with the National Police Checking Service which is operated by the ACIC.

124. In order to access this service, entities must be assessed and approved by ACIC to become accredited.[28] As part of this, ACIC assesses an entity's processes for verifying applicant identities. Where an entity has been assessed as suitable to become accredited, ACIC requires the organisation to enter into a legally binding contract[29] which sets out accredited bodies' requirements for verifying applicants' identity and include the sighting of:

- at least one of the documents listed as a 'Commencement of Identity Document'
- at least one of the documents listed as a 'Primary Use in Community Document'
- at least two of the documents listed as a 'Secondary Use in the Community Document'.

[28] Information on ACIC accreditation is on the ACIC website at https://www.acic.gov.au/services/national-police-checking-service/im-interested-becoming-accredited.

[29] A template of the 'Agreement for controlled access by duly Accredited Bodies to Nationally Coordinated Criminal History Checks' is available at: https://www.acic.gov.au/sites/default/files/2021-04/NPCS%20Agreement%20for%20controlled%20access.pdf. ACIC also states that it monitors organisations' compliance through a formal program comprising, data quality monitoring, investigations following referrals alleging non-compliance, periodic reviews of accredited bodies and/or legal entity customers, and ongoing suitability assessments.

125. Further, ACIC also monitors organisations' compliance through a formal program comprising, data quality monitoring, investigations following referrals alleging non-compliance, periodic reviews of accredited bodies and/or legal entity customers, and ongoing suitability assessments.

126. The above accreditation requirements provide a level of assurance that personnel conducting identity verification have the relevant skills and qualifications for doing so.

127. Three of the audited organisations provided advice from their third-party service providers that they use the DVS to verify documents. The remaining organisation, CCYP, did not provide sufficient assurance of this.

Skills and qualifications of personnel undertaking identity verification

128. DPC was the only audited organisation that made reference to in-house identity verification (noting the conflicting information on this described earlier).

129. DPC's policy states that an authorised person for verifying identity is an employee of DPC whose own identity has been verified. It is not evident whether any specific skills, knowledge or training are required to undertake this task. The policy and procedure document also does not provide clear guidance to authorised staff members on how to conduct the verification to a requisite standard, including how to detect potentially fraudulent documentation.

Findings and conclusions against Question 2

130. All four organisations rely on the conduct of National Police Checks by service providers for identity verification. Prior to the audit, they had limited understanding about their respective service providers' processes for verifying identity and did not have assurance that these checks met relevant standards.

131. Despite identity verification being a critical component of personnel security, none of the audited organisations had clear policies and procedures on how to undertake identity verification to the appropriate standard. It was apparent that the organisations were not familiar with key aspects of identity verification, such as the requirement to verify identity to LOA 3 of the NIPG, and use of the DVS.

132. The use of an external service provider for conducting identity checks reduces the internal resource burden on an organisation's staff and provides some comfort that skilled and qualified providers are conducting these checks. However, agencies should assure themselves that these third-party service providers meet the requirements of LOA 3 of the NIPG and use the DVS where possible. These requirements should be included in service agreements and monitored by the purchasing organisation.

133. In conclusion, all organisations were rated as only partially meeting the audit criteria, with none of them having clear policies and procedures on identity verification requirements and how they meet

them. While each agency arranges for the National Police Check via a third-party provider, none of the agencies submitted a service agreement or contract that clearly specified the process for conducting identity verification, nor the requirement to meet LOA 3 of the NIPG or the use of the DVS.

134. To assist in meeting the audit criteria in future, it is recommended that policies and procedures relating to pre-engagement screening explicitly articulate requirements and processes for verifying identity and that they encapsulate these in future service agreements or contracts with third-party service providers.

Recommendations regarding identity verification

Recommendation 3 to CCYP, DPC, VFMC, VMIA

135. Review existing identity pre-engagement screening policies and procedures with a view to:

- Updating content and aligning the organisation's practices with those set out in the NIPG, including identity verification to at least LOA 3 of the guidelines.

- Using the DVS for Australian issued primary identification documents.

- Providing clear instructions to authorised personnel (including third parties) on their role in undertaking identity verification.

Recommendation 4 to CCYP, DPC, VFMC, VMIA

136. When engaging with a third-party service provider to undertake identity verification on the organisation's behalf:

- Ensure that the service agreement or contract clearly specifies the requirements around meeting LOA 3 of the NIPG, including use of the DVS.

- Obtain ongoing assurance that the service provider meets the requirements of at least LOA 3 of the NIPG, including use of the DVS.

Question 3 - Does the organisation undertake pre-engagement screening of all personnel?

Criteria tested for Question 3

137. Question 3 sought to answer whether organisations carry out adequate pre-screening measures to assess whether prospective personnel are eligible and suitable to access public sector information.

138. This question focussed on the pre-engagement screening checks that organisations carry out for general roles. That is, the standard checks that are conducted across the organisation's workforce. Question 4 (below), in turn, considered additional pre-engagement screening measures that are carried out beyond such standard checks for high-assurance roles with a heightened risk profile.

139. The criteria tested for Question 3 were that the organisation:

(i). has procedures that clearly document how to undertake pre-engagement screening checks for all personnel

(ii). has informed, qualified and skilled personnel / providers undertaking pre-engagement screening checks for all personnel

(iii). (if relevant) uses accredited / authorised third parties to undertake pre-engagement screening checks for all personnel on the organisation's behalf

(iv). has assurance that pre-engagement screening checks for all personnel are completed to an appropriate standard, including instances where a third-party undertakes checks on the organisation's behalf.

Primary source material for Question 3

140. PSPF Policy 12 is the primary source for Question 3. This policy details the pre-engagement screening processes and standardised vetting practices to be undertaken when employing personnel. The outlined processes provide a high-quality and consistent approach to managing personnel eligibility and suitability risk across government.

141. PSPF Policy 12 sets out that:

- It is mandatory to assess a person's eligibility for employment by:
    - verifying a person's identity using the DVS
    - confirming a person's eligibility to work in Australia.
- It is mandatory to obtain assurance about a person's suitability to access government information and resources by carrying out pre-employment screening checks.

- Organisations are encouraged to obtain signed undertakings from prospective personnel (statutory declaration and agreement to safeguard government resources).

OVIC's assessment against Question 3

142. **Table 6** shows how OVIC assessed the organisations' performance against Question 3.

Table 6 OVIC assessment against Question 3

Organisation	OVIC's assessment
CCYP	Substantially – the organisation meets most of the audit criteria
DPC	Partially – the organisation meets some of the audit criteria
VFMC	Substantially – the organisation meets most of the audit criteria
VMIA	Substantially – the organisation meets most of the audit criteria

Observations against Question 3

143. All audited organisations stated that a satisfactory outcome of pre-engagement screening is a condition of employment with the organisation. The following sections show the organisations' approaches to pre-engagement screening.

Eligibility checks

144. The requirement to verify a person's identity is covered above in the analysis under question 2.

145. The eligibility to work in Australia check requires confirming that a person holds Australian citizenship, or if the person is not an Australian citizen, confirming that they have a valid visa with working rights.

146. All four organisations demonstrated that they conduct an eligibility to work in Australia check.

Suitability checks

147. PSPF Policy 12 recommends a range of minimum pre-employment screening checks for assessing a person's suitability. It recommends that entities undertake pre-engagement screening to AS 4811 requirements. It also recommends conducting entity-specific checks to mitigate particular security threats applicable to the entity that are not addressed by minimum pre-engagement screening checks.

148. **Table 7** shows which of the suitability checks are carried out by each organisation.

Table 7 Recommended pre-engagement checks

Recommended screening check	CCYP	DPC	VFMC	VMIA
Employment history – 5 years	✗	✗	✓	✓
Residential history – 5 years	✗	✗	✗	✗
Referee checks – 3 months	✓	✓	✓	✓
National Police Check	✓	✓	✓	✓
Credit history check	✗	✗	✓	✗
Qualification check	✓ – mandatory qualifications only	✓ – mandatory qualifications only	✓	✓

Conflict of interest declaration check	✗	✗	✗	✓
Entity-specific check	✓ – Working with Children Check – child safety values-based interview questions	✗	✓ – financial background checks	✗

149. As shown above, each of the audited organisations conduct most of the recommended pre-engagement screening checks, with some variations between them.

150. All organisations require that two reference checks are conducted, with VMIA specifying this can be reduced to one for internal applicants. In terms of specifying the nature of candidate referees, VMIA states that they must be at an equivalent or senior position commensurate to the candidate; VFMC requires at least one referee to be a former employer; DPC's policy says referees should be a current and former manager; and CCYP sets out that the two referees should be the candidate's current and/or former direct supervisor or manager within the last 5 years of employment.

151. Policies, procedures and templates for reference checks generally lacked detail in terms of using these tools to assess suitability issues[30]. However, CCYP's policy and referee check template specifically guide the user to answer questions about conduct and suitability as well as specifying questions about the candidate's appropriateness to engage with children and commitment to child safety. VFMC also provided a referee check template (from its recruitment partner that carries these out) which asks a referee to comment generally on honesty, integrity, commitment, and work ethic.

152. Employment history check varies considerably across organisations. The most thorough is VFMC, whose third-party service provider conducts a 10-year work history check through their screening process. VMIA also conducts the same check through its third-party provider who checks the last three employers on a candidate's resume.

153. CCYP and DPC do not appear to conduct specific checks in this regard, and rely on a review of a candidate's CV along with reference checks. CCYP also referred to relying on a candidate's statutory declaration declaring that all information provided in their application is complete, true and correct.

[30] PSPF 12 states that reference checks may address any substantiated complaints about the person's behaviour; information about any action, investigation or inquiry concerning the person's character, competence, or conduct; and any security related factors that might reflect on the person's integrity and reliability.

154. DPC and CCYP do not require prospective employees to make conflict of interest declarations before being engaged.

155. VMIA conducts a conflict-of-interest check after a candidate has been deemed successful, by requiring them to complete a comprehensive 'Declaration of Private Interests'. Rather than simply relying on a candidate understanding and properly identifying actual, potential or perceived conflicts, the document requires a candidate to specify a range of their or their family members' private interests (such as offices held and income sources) that could conflict with their performance of public duties.

156. None of the organisations directly conduct a residential history check. CCYP, DPC and VMIA noted that applicants are required to provide details of their residential addresses for the past 5 years when applying for a National Police Check.

157. Credit history checks establish whether the person has a history of financial defaults, is in a difficult financial situation, or if there are concerns about the person's finances. Only VFMC conducts such checks across its workforce.

158. The audited organisations had varying practices for conducting qualifications checks. CCYP and DPC advised that they only conduct checks for mandatory qualifications, while VFMC and VMIA indicated that they conduct checks for all qualifications.

159. For CCYP, if qualifications are mandatory for the role, original qualifications must be sighted by the Human Resources area to confirm validity, and then copies stored on the staff file. The Pre-employment Screening Procedure sets out the process if there are any doubts or concerns about the authenticity of the qualification.

160. DPC's Pre-employment Screening Policy states that for positions that require the incumbent to hold a qualification, the preferred candidate may be required to provide a copy of the qualification to the hiring manager during the recruitment process. Hiring managers may request and sight the qualification during or after the interview has been completed. If required, the hiring manager may request the recruitment team to conduct a qualification check by DPC's online provider. The policy recommends that hiring managers should not proceed to an offer of employment until the qualification has been sighted and the relevant documentation is received. Where the qualification check does not confirm that the proposed appointee holds the mandated qualification, the hiring manager must inform the candidate that they will not be made an offer of employment.

161. VFMC and VMIA documentation indicates that the qualification check is conducted as a standard background check through their contracts with third-party service providers.

162. An entity-specific check is a pre-employment screening measure that takes into account the specific nature of the organisation and particular risks associated with this. Three of the audited organisations conduct entity-specific pre-engagement screening checks.

163. CCYP's entity-specific checks include a requirement for all staff to hold a WWCC, specific child safety values-based interview questions (included in its interview template).

164. VMIA explained that it conducts anti-money laundering and counter terrorism financing checks for all roles. However, this is not accurately reflected in its Employee Lifecycle Policy which states that 'financial background checks (e.g. anti-money laundering, bankruptcy)' apply to 'applicable roles'.

165. VFMC explained that, while it is not regulated by the Australian Prudential Regulation Authority (**APRA**), it seeks to align its pre-employment screening practices with APRA standards.[31] It therefore conducts the following range of checks for all staff, mainly relating to financial background, to determine whether they are fit and proper:

- Anti-money laundering and counter terrorism financing
- ASIC Banned and Disqualified Persons
- Australian Bankruptcy and National Personal Insolvency
- Enforceable Undertakings
- APRA Disqualified Register
- Australian Basic Credit Check
- Australia Directorships
- Australian Driver Licence
- Global media
- Professional membership.

Signed undertakings

166. **Table 8** shows whether agencies obtain the following from prospective employees as part of pre-engagement screening in line with PSPF Policy 12:

- A statutory declaration stating all information provided is truthful and complete and documents are accurate and without amendments, issued by the issuing authority and relate to the clearance subject

[31] Prudential Standard CPS 520 Fit and Proper, July 2017, available at: https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-520-Fit-and-Proper-%28July-2017%29_0.pdf. The Standard sets out criteria for determining whether a person is fit and proper and includes an assessment of whether a person possesses requisite competence, character, diligence, honesty, integrity, and judgement of an individual; whether a person is disqualified under an applicable Prudential Act; and whether a person has conflicts of interests that would affect their ability to perform the duties of a position.

- A signed agreement to confirm their undertaking to safeguard government resources, including reference to compliance with relevant legislation and policies (such as secrecy or confidentiality obligations and related offences).

167. CCYP and VFMC require preferred candidates to complete a statutory declaration relating to misconduct (see below discussion), which also includes a declaration that all information provided in their application is complete, true and correct. DPC and VMIA also require preferred candidates to attest to the truthfulness of their applications, but these do not take the form of statutory declarations.

168. No organisation requires new personnel to sign a standalone agreement to confirm their undertaking to safeguard government resources. Organisations instead pointed to employment contracts which reference obligations around confidentiality of information and other policies and procedures.

Table 8 Signed undertakings from prospective personnel

Signed undertakings	CCYP	DPC	VFMC	VMIA
Statutory declaration	✓	✗	✓	✗
Signed agreement to safeguard resources	✗	✗	✗	✗

Misconduct screening

169. While not a specific requirement under PSPF Policy 12, all four audited organisations also require preferred candidates to complete misconduct[32] declarations – in line with requirements under the Victorian Public Sector Commission's (**VPSC**) Victorian Public Service Pre-employment Screening Policy.[33]

[32] As defined under section 4 of the *Public Administration Act 2004* (Vic).

[33] Available at VPSC website: https://vpsc.vic.gov.au/workforce-capability-leadership-and-management/recruitment-in-the-public-sector/pre-employment-and-misconduct-screening/about-misconduct-screening/

170. As noted by the VPSC, misconduct by VPS employees can put the safety of employees and the community at risk and erode public trust. Thorough pre-employment misconduct screening can reduce the chance of employees moving between employers without relevant misconduct being identified. It also enables a risk assessment of any misconduct identified in a candidate's work history.

171. VPSC's policy requires that a misconduct statutory declaration and consent form (or a misconduct declaration if a statutory declaration cannot be provided) be completed by all candidates as part of the pre-engagement process for all VPS positions in public service bodies.

172. The form asks candidates to declare if they have had their employment terminated due to misconduct; have been found to have engaged in misconduct; are the subject of an open misconduct investigation; or have ceased employment while being the subject of a misconduct investigation.

173. While all four organisations require the completion of misconduct screening checks in line with VPSC's policy, VMIA's timing of the check is different than other organisations – requiring the check upon commencement in the role instead of before commencement.

Use of third-party service providers for pre-engagement screening

174. All audited organisations use third parties to conduct some of their pre-engagement screening checks, although the extent to which third parties are used differs. For example, VFMC and VMIA contract third parties to conduct a suite of checks, including National Police Check, employment and qualifications checks, financial checks, and other verification checks (for example, entitlement to work, driver licence, professional memberships). In contrast CCYP uses a third party for conducting the National Police Check while DPC uses third parties to conduct the National Police Check, work rights/visa checks, and qualification checks, as well as for conducting security clearances.

Findings and conclusions against Question 3

175. The audited organisations each conduct most of the mandatory and recommended pre-engagement checks as set out in PSPF Policy 12. It was positive to see that three organisations reported undertaking entity-specific checks for general roles, which demonstrate some appreciation of the specific risks applicable to the respective organisations. Additionally, all four organisations also screen for misconduct despite not being required under PSPF Policy 12.

176. Some checks are not conducted by all organisations – notably, the residential history check; conflict of interest declarations; verification of all qualifications[34]; statutory declaration regarding applications

[34] As noted above, all organisations conduct verification of qualifications but two of the organisations only perform this for mandatory qualifications. An individual's misrepresentations about their qualifications (even if not mandatory for a role) may point to a lack of integrity and unsuitability for a role in the public sector. See for example: Qld CCC Prevention in focus, *Risks in recruitment — are you adequately vetting your staff?*, April 2018, available at: https://www.ccc.qld.gov.au/sites/default/files/Docs/Publications/CCC/Prevention-in-Focus-Risks-in-recruitment-2018.pdf

being truthful and complete; and signed agreements to confirm applicants' undertaking to safeguard government resources.

177. Note that the pre-engagement screening checks listed in PSPF Policy 12 are recommended checks to assist in meeting the overarching mandatory requirement of obtaining assurance of a person's suitability. This means all such checks may not necessarily be appropriate for all organisations. The range of checks that an organisation carries out should be tailored to its specific risk profile. However, organisations should at least consider all recommended checks and thoroughly assess whether they are required to appropriately manage personnel security risks.

178. Nevertheless, OVIC is of the view that some of the screening measures that are not currently carried out across the organisations should be carried out, and could be introduced with limited burden.

179. One such measure is a requirement for prospective employees to submit conflict of interest declarations. PSPF Policy 12 notes that matters such as financial particulars, secondary employment and associations can improperly influence the performance of official duties and the ability to safeguard government resources. As an example, the Independent Broad-based Anti-corruption Commission (IBAC) has specifically noted that inadequate screening such as by failing to require applicants to provide information about conflicts of interest can place a public sector agency at greater risk of corruption.[35]

180. OVIC acknowledges that organisations have components relating to personnels' undertaking to safeguard government resources. However, OVIC believes that better practice would involve new personnel signing an explicit statement, agreeing to comply with the government's policies, standards, protocols and guidelines that safeguard its resources from harm. This should include reference to any secrecy provisions and related offences, if applicable.

181. OVIC also observed differences in the completion of misconduct declarations among agencies. Better practice is for misconduct screening to take place during the pre-engagement phase, prior to the commencement of employment.

182. All organisations use third-party service providers to conduct at least some of their pre-engagement screening checks. It was notable during the audit, however, that the organisations needed to seek advice from their third-party service providers about the nature of checks they undertake and whether they meet relevant requirements (see Question 2 above).

183. The use of third-party providers can be an effective and efficient way of determining the eligibility and suitability of prospective personnel. However, to ensure the veracity of the checks, organisations

[35] IBAC, *Corruption and misconduct risks associated with employment practices in the Victorian public sector*, August 2018, available at: https://www.ibac.vic.gov.au/publications-and-resources/article/corruption-and-misconduct-risks-associated-with-employment-practices-in-the-victorian-public-sector. See also: IBAC, *Protecting the public sector from criminal networks,* September 2023, available at: https://www.ibac.vic.gov.au/protecting-public-sector-criminal-networks; IBAC, *Special report on corrections,* June 2021, available at: https://www.ibac.vic.gov.au/publications-and-resources/article/special-report-on-corrections.

should have clear governance arrangements, including documentation setting out the required standards and processes for conducting each check.

184. In conclusion, agencies achieved relatively highly on Question 3, mainly due to the range of pre-engagement screening checks undertaken, and the requirement that a satisfactory outcome from these checks is a condition of employment.

185. DPC was rated lower than the other organisations, as it conducts a narrower range of checks. In contrast, the entity-specific checks undertaken by CCYP and VFMC contributed to their higher ratings – with VFMC's range of checks being particularly thorough.

186. To assist in meeting the audit criteria in future, it is recommended that agencies consider broadening their range of pre-engagement screening checks and document associated policies and procedures, and ensure that where checks are conducted by third-party providers they are conducted to the appropriate standard.

Recommendations regarding pre-engagement screening

Recommendation 5 to CCYP, DPC, VFMC, VMIA

187. Review the suite of pre-employment checks they undertake against best practice material, with a view to including relevant checks that are not currently undertaken.

Recommendation 6 to CCYP, DPC, VFMC, VMIA

188. Liaise with their third-party service providers to understand and document the requirements of each pre-engagement screening check, with a view to ensuring that all checks meet the relevant standards outlined in the PSPF Policy 12, NIPG and AS 4811, or equivalent.

Question 4 - Does the organisation undertake additional pre-engagement screening of personnel that is commensurate with the risk profile of their roles?

Criteria tested for Question 4

189. Question 4 considered whether organisations carry out additional measures for high-assurance roles, beyond standard pre-engagement checks for general roles. This question reflects that not all roles carry the same information security risks and that a one-size-fits-all approach to pre-engagement

screening is usually not appropriate. Rather, organisations should identify high-assurance roles and implement additional pre-engagement screening commensurate with the risk profiles of those roles.

190. Additional pre-engagement screening measures further mitigate personnel security risks by providing an organisation with a higher degree of assurance about an individual's suitability to perform a particular function, occupy a certain role, and/or access high-value public sector information.

191. The criteria tested for this audit question were that the organisation has:

(i). procedure(s) that clearly document how to undertake additional pre-engagement screening checks for high-assurance roles

(ii). appropriately informed, qualified and skilled personnel undertaking these additional pre-engagement screening checks for high-assurance roles

(iii). (if relevant) uses accredited / authorised third parties to provide additional pre-engagement screening activities / services for high-assurance roles

(iv). assurance that additional pre-engagement screening checks are completed for high-assurance roles, including where a third-party undertakes these checks on behalf of the organisation

(v). (if relevant) has a register of positions requiring security clearance and the clearance level required.

Heightened risk profiles

192. Heightened risk profiles may be based on a range of factors, including the:

- Nature of the role, where the organisation has determined it requires greater assurance about the person's suitability (e.g. as a fraud mitigation or anti-corruption measure)

- Occupant having access to 'security classified' information or systems (i.e. information that has undergone an information security value assessment and has been rated with a BIL of 3[36] or above – resulting in a security classification of PROTECTED or above)

- Occupant having access to aggregations of information or assets (e.g. IT administrators, archival personnel overseeing hardcopy records)

- Occupant having privileged access to organisational assets (e.g. IT administrators, security personnel monitoring facilities, Executives, Internal audit)

- Occupants having a high degree of influence over the organisation (E.g. Executives).

[36] See above at n.13. See also OVIC Practitioner Guide, Protective Markings, available at: https://ovic.vic.gov.au/wp-content/uploads/2022/06/Practitioner-Guide-Protective-Markings-V2.0-1.pdf

Additional pre-engagement screening measures

193. Additional pre-engagement screening means checks that go beyond the measures for general roles, as set out earlier in Question 3. Organisations can use a range of screening techniques to gain heightened assurance regarding the suitability of a candidate.

194. The choice of additional screening check should be tailored to the risk profile of the particular role but may include, for example:

- Licencing check
- Disciplinary check
- Financial regulatory check
- Business interests check
- Psychometric or aptitude testing
- Drug and alcohol checks
- Enhanced verification of candidate declarations
- Security clearance (see below).

Security clearances

195. A method of conducting more stringent screening of an individual's suitability is to require prospective employees to undergo a security vetting process to attain a security clearance[37]. A security clearance is a status that may be granted by the Australian Government Security Vetting Agency (**AGSVA**) or an authorised vetting agency body.

196. The purpose of the security vetting process is to determine whether an individual is suitable to hold a security clearance—that is, whether they possess and demonstrate an appropriate level of integrity. In the security context, integrity is defined as a range of character traits that indicate the individual is able to protect government resources. These character traits are: honesty, trustworthiness, maturity, tolerance, resilience and loyalty.[38]

197. There are different levels of security clearances – Baseline, Negative Vetting (**NV**) 1, NV 2, Positive Vetting, and TOP SECRET – Privileged Access. The different levels of security clearances involve increasingly stringent and invasive screening. The level of clearance sought will depend on the level of

[37] Individuals cannot apply for a security clearance themselves; they must be sponsored by an authorised security clearance sponsor. State government agencies are authorised to sponsor a security clearance.

[38] Australian Government Security Vetting Agency, *Security Clearances – Overview*, available at: https://www.defence.gov.au/security/clearances/about/overview

risk associated with the role in question and the security classification of the resources the role will have access to.

198. PSPF Policy 12 sets out that an individual must be an Australian citizen and have a checkable background (unless an eligibility waiver is obtained) in order to be considered eligible for a security clearance. It also sets out the minimum personnel security checks conducted at different security clearance levels. These are also re-produced at **Annexure B**. As a summary, they will involve checks such as:

- Verification of identity
- Background assessment
- Police records check
- Professional and personal referee check
- Qualification verification
- Financial history assessment
- Digital footprint checks
- ASIO suitability assessment.

199. An individual's suitability to hold a security clearance is assessed based on all relevant, reliable and independently verified information obtained through the minimum personnel security checks, and any additional checks required. It is also assessed against the PSPF Personnel Security Adjudicative Guidelines,[39] with any doubt being resolved in the national interest.

200. PSPF Policy 12 also sets out that entities must identify and record positions that require a security clearance and the level of clearance required. The Department of Home Affairs recommends that entities keep a register identifying:

- positions that require a security clearance for ongoing access to government resources
- positions that require a security clearance as a higher-level assurance of personnel suitability
- when the requirement for a security clearance will be assessed (at least each time the position becomes vacant and before it is advertised).

[39] See PSPF Policy 12, Annexure A.

OVIC's assessment against Question 4

201. **Table 9** shows how OVIC assessed the organisations' performance against audit question four.

Table 9 OVIC assessment against Question 4

Organisation	OVIC's assessment
CCYP	Partially – the organisation meets some of the audit criteria
DPC	Substantially – the organisation meets most of the audit criteria
VFMC	Partially – the organisation meets some of the audit criteria
VMIA	Partially –the organisation meets some of the audit criteria

Observations against Question 4

202. DPC conducts additional screening for some roles it has identified as having a heightened risk profile, based on access to security classified information, by requiring security clearances for these roles. These roles are referred to as DSAPs by DPC. It advised that there are 10 DPC staff with Baseline clearances, 18 with NV 1 clearances and 2 with NV 2 clearances. This translates as five per cent of total DPC staff having security clearances.

203. DPC provided an excerpt from a policy document which outlines 10 positions that have been identified as DSAP positions requiring a security clearance. It includes the Secretary, Deputy Secretaries, General Counsel and various staff of the Community Security and Emergency Management Branch. This is not an exhaustive list, however, with the relevant document also noting that other staff across DPC may require a security clearance.

204. Similarly, while DPC provided other policy and procedure documents that address the issue of security clearances, it advised that it does not possess a register of all positions requiring a security clearance, as required under PSPF Policy 12.

205. Rather, its ‘Personnel Screening Procedure’ and ‘Personnel Screening Guidelines’ state that when a position is established, line managers must analyse the duties of the position and the highest level of classified information that will be accessed. Line managers must then seek advice from the DPC DSAP Coordinator on the need for, and the appropriate level of security clearance.

206. DPC noted that the security vetting process is carried out by a third-party service provider. The only documentation provided of the agreement between DPC and its service provider is correspondence dated 6 June 2007. The agreement contains outdated security classification references and clearance levels, as well as superseded Commonwealth Government policy references.

207. VMIA has recently introduced additional pre-engagement screening for all ‘heads of roles’ as well as those in the Business Performance (Finance Division). In addition to the anti-money laundering and counter-terrorism checks that apply to all general roles, these roles are now subject to a credit history check and a bankruptcy check – which are carried out by a third-party service provider.

208. VFMC requires key executives[40] to provide probity-self declarations in line with its Fit and Proper Policy. The declaration covers a range of issues, such as whether the person has been declared bankrupt, has been subject to disciplinary investigations, or has been director of a company which became insolvent. Such executives must also declare relevant financial and other personal interests. However, all such declarations are made once a person has joined VFMC rather than during the pre-engagement phase.

209. As such, whilst VFMC has determined that key executives are high-assurance roles, the pre-engagement screening process for these roles does not differ significantly from that which applies to general roles across the organisation (as outlined above in relation to Question 3). VFMC acknowledged this, stating that all roles undergo the same level of screening because it considers that all functions within VFMC are equal-risk with respect to security vulnerabilities.

210. A 2020 internal audit of VFMC’s implementation of the VPDSS (outsourced to a third-party service provider) noted that the personnel assessment process was a key challenge faced by VFMC. It found that there was no evidence of a risk-based approach to pre-employment screening and background checks where different levels of probity check are defined for different roles and risk profiles.

211. The internal audit report highlighted the risk that VFMC may not have the ability to confirm that candidates for higher risk roles have been sufficiently assessed. It recommended that VFMC consider implementing a process to conduct a deeper level of pre-employment screening for candidates applying to high-risk roles, potentially through a separate package of probity checks.

[40] Key executives under the Fit and Proper Policy are those deemed to be roles which are central to the ongoing management of VFMC and consist of the Chief Executive Officer, Chief Investment Officer, Chief Operating Officer, Chief Finance and Risk officer, Head of Client and Market Development and Head of People.

212. VFMC management responded to the internal audit, noting that all roles at VFMC are designated as high-risk and that pre-engagement background screening protocols are consistently applied across the business.

213. CCYP has identified that a WWCC is a required additional screening check relevant to its business context, and requires all employees to undergo this screening. CCYP also undertakes psychometric testing for a small number of identified positions within the regulatory advisory team. Their roles are considered high-assurance due to the sensitive nature of the information handled (protected under the Child Wellbeing and Safety Act) and their involvement in managing vicarious trauma across the team.

214. VMIA, VFMC and CCYP do not require any candidates to obtain a security clearance and do not have a register of all positions requiring a security clearance. Each provided explanations for this:

- VMIA asserted that it does not handle security classified information on the basis that while it handles some information assessed as PROTECTED (i.e. BIL 3) in line with OVIC guidance on assessing the security value of public sector information[41], this information would not be classified as PROTECTED, SECRET or TOP SECRET according to Commonwealth standards.

- VFMC asserted that it only handles information assessed as OFFICIAL:Sensitive (i.e. BIL 2) or below.[42]

- CCYP stated that it does not deem security clearances to be necessary and noted that introducing such a requirement to be carried out in isolation from DFFH (which provides CCYP with payroll and onboarding support) would pose significant financial and logistical challenges. It stated its belief that any requirement to conduct a security clearance should not be linked to the protective markings applied to its information holdings. CCYP also noted that it had never undertaken a formal review of its workforce regarding risk levels but would soon be undertaking such a project as well as considering the potential for security clearance requirements based on the results.

Findings and conclusions against Question 4

215. All organisations have taken steps to identify some high-assurance roles, with additional pre-engagement screening of varying degrees applying to these roles.

216. Overall, the findings in relation to Question 4 reflected those made in relation to Question 1 – that the audited organisations did not demonstrate a thorough, systematic approach towards understanding the risk profile of their workforce.

[41] See above, n.13.

[42] See discussion above at paragraph 27 and 28.

217. That is, OVIC concluded that none of the organisations had undertaken a root and branch analysis of the risk profile of the workforce by failing to identify all high-assurance roles and subsequently update policy and procedures with enhanced requirements for additional pre-engagement screening measures, commensurate with the risk profile of such roles.

218. DPC was rated as substantially meeting the criteria for audit question 4, given it conducts security clearances for certain high-assurance roles. It was not rated as fully meeting the relevant audit criteria because of its lack of a register of all positions that require security clearances and the process of ad hoc assessments by line managers. This did not demonstrate a thorough and consistent approach to determining roles that require security clearances. It is unclear exactly how DPC determines which roles require security clearances and whether this involves consideration of factors other than the value of information to which the role has access.

219. It is also unclear what assurance DPC has that additional pre-engagement screening checks are conducted to an appropriate standard, given the age of the agreement currently in place with a third-party provider, and the lack of currency of the content of that agreement.

220. VFMC was rated as partially meeting the audit criteria for Question 4, as it showed some appreciation of the fact that particular roles can attract higher risk – with key executives at VFMC being required to undertake extra declarations than the general workforce. These additional measures did not appear to be commensurate with roles of a higher risk profile and, in any case, VFMC noted that declarations are submitted after key executives had already been engaged.

221. As such, it appears that the risks previously highlighted in VFMC's internal audit may remain. While noting that all personnel at VFMC are subject to the most stringent pre-engagement screening measures compared with the other three organisations, OVIC considers it important that VFMC consider previous internal audit recommendations as they relate to pre-engagement screening – with a view to revising its policies and procedures to incorporate enhanced personnel security requirements where relevant.

222. VMIA showed a similar limited appreciation of the fact that particular roles can attract higher risk and recently introduced additional pre-engagement screening check for a small subset of roles. However, the fact that only roles with a financial element were specified pointed to these measures resulting from only a partial assessment of high-assurance roles. Additionally, it was noted that these additional measures did not differ greatly from the pre-engagement screening of the general workforce.

223. CCYP was rated as partially meeting the audit criteria on the basis of its WWCC, conducted for all employees, and psychometric testing conducted for a small number of employees. However, OVIC considers that additional pre-engagement screening would be warranted for a greater number of high-assurance positions. It is posited that CCYP's workforce would likely include additional high-assurance roles, especially noting that it reported that 34 per cent of its information assets are rated as PROTECTED.

224. Also contributing to the lower ratings of CCYP, VMIA and VFMC was the fact that they do not have registers of positions that require security clearances.

225. This does not necessarily mean that organisations should use security clearances. Rather, they should properly assess whether security clearances or equivalent processes should be implemented based on a thorough and structured assessment of the risk profile of roles within the organisation. It did not appear that CCYP, VMIA or VFMC had considered requiring security clearances for particular roles and opted against this based on a thorough risk assessment.

226. Of some concern, the three agencies who do not conduct security clearances each provided arguments as to why they are not relevant to their organisation. These centred around arguments about the security classification of information which in some cases exposed organisations' lack of knowledge or understanding of the practices and principles of classifying information.

227. Furthermore, these arguments did not take into account that while access to higher value information is a key risk factor, some roles can attract increased risk even where they do not involve access to information assets rated as PROTECTED or above.

Recommendations regarding additional screening commensurate with risk

Recommendation 7 to DPC

228. Update documentation regarding security clearances to reflect the current expectations of, and service provided by, the third-party service provider, together with processes for ensuring the service provider carries out security clearances to the appropriate standard.

Recommendation 8 to CCYP, DPC, VFMC, VMIA

229. After conducting the workforce review referred to in Recommendation 2:

- consider strengthening pre-engagement screening measures for high-assurance roles; and
- establish and maintain a register of positions that require security clearances, including when the need for a security clearance will be assessed.

Recommendation 9 to CCYP, DPC, VFMC and VMIA

230. Ensure that for any position identified as requiring a security clearance, the security clearance process is undertaken by an authorised vetting agency, with appropriate processes in place to ensure the vetting agency carries out security clearances to the appropriate standard.

Recommendation 10 to CCYP, DPC, VFMC and VMIA

231. Improve organisational understanding of the security value of the information holdings and risk profiles associated with the various roles and functions across the workforce, as a critical input into an informed workforce review.

Office of the Victorian
Information Commissioner

Annexure A – Audit criteria

Question	Control objectives	Criteria tested	Primary source material referenced[43]
1. Do organisations' personnel security policies and procedures-address the pre-engagement (eligibility and suitability) phase?	Element 10.010 of the VPDSS states that the organisation's personnel security policies and procedures address the personnel life cycle phases: a. pre-engagement (eligibility and suitability)	The organisation has: 1. personnel security policies and procedures reflective of the risk profile of its workforce ***(Yes or No)*** The risk profile of its workforce informed by a review of: • the roles across its workforce • the associated functions of each role • the security value of information / systems each role has access to • the level of influence of each role • current control environment of the organisation	The primary source material referenced under Standard 10 of the VPDSS, relevant to this question and associated criteria are: • PSPF Policy 3 Security planning and risk management • PSPF Policy 12 Eligibility and suitability of personnel

[43] OVIC has referenced the most recent version of the primary source material for this audit.

Question	Control objectives	Criteria tested	Primary source material referenced[43]
	b. engagement (ongoing and re-engagement) c. separating (permanently or temporarily). This audit considered the first phase only, pre-engagement (eligibility and suitability).	2. personnel security policies and procedures that contain requirements that address pre-engagement screening to an appropriate standard *(Yes or No)* 3. personnel security policies and procedures that clearly articulate *eligibility* requirements for personnel to an appropriate standard *(Yes or No)* 4. personnel security policies and procedures that clearly articulate *suitability* requirements for personnel to an appropriate standard *(Yes or No)* 5. personnel security policies and procedures that address all forms of personnel (e.g., ongoing, fixed-term or casual employees, including full-time or part-time employees and trainees, contractors and/or labour hire staff) *(Yes or No)* 6. personnel security policies and procedures that require pre-engagement screening checks of all personnel be undertaken prior to commencement / onboarding *(Yes or No)* 7. personnel security policies and procedures that contain adequate requirements / directions for: a. **general roles** across the workforce *(Yes or No),* and b. **high-assurance roles** that the organisation requires additional forms of assurance for *(Yes or No)*	- Australian Standard 4811: 2022 Workforce Screening
2. Does each organisation verify the identity of its personnel?	Element 10.020 of the VPDSS states that the organisation verifies the identity of personnel,	The organisation:	The primary source material referenced under Standard 10 of the VPDSS, relevant to this question and associated criteria are:

Question	Control objectives	Criteria tested	Primary source material referenced[43]
	revalidates, and manages any changes as required. This audit considered the first phase only, ie. the organisation verifies identity.	1. has procedure(s) that clearly document how to undertake identity verification to an appropriate standard (i.e. LOA 3 under the NIPG using the DVS) ***(Yes or No)*** 2. has assurance that identity verification checks are undertaken to an appropriate standard (including instances where a third party undertakes these checks on behalf of the organisation) ***(Yes or No)*** 3. has informed, qualified and skilled personnel / providers undertaking identity verification ***(Yes or No)*** 4. *(if relevant)* uses accredited / authorised third parties to provide/ undertake identity verification on the organisation's behalf ***(Yes or No)***	• PSPF Policy 12 Eligibility and suitability of personnel • Australian Standard 4811: 2022 Workforce Screening • National Identity Proofing Guidelines
3. Does each organisation undertake pre-engagement screening of all personnel?	Element 10.030 of the VPDSS states that the organisation undertakes pre-engagement screening commensurate with its security and probity obligations and risk profile.	The organisation: 1. has procedure(s) that clearly document how to undertake pre-engagement screening checks for all personnel, to an appropriate standard ***(Yes or No)*** Consideration given to the following checks: i. Table 1 Mandatory pre-employment screening checks ii. Table 2 Recommended pre-employment screening checks iii. Table 3 Better practice checks (encouraged) 2. has informed, qualified and skilled personnel / providers undertaking pre-engagement screening checks for all personnel ***(Yes or No)***	The primary source material referenced under Standard 10 of the VPDSS, relevant to this question and associated criteria are: • PSPF Policy 12 Eligibility and suitability of personnel

Question	Control objectives	Criteria tested	Primary source material referenced[43]
		3. *(if relevant)* uses accredited / authorised third parties to undertake pre-engagement screening checks for all personnel on the organisation's behalf ***(Yes or No)*** 4. has assurance that pre-engagement screening checks for all personnel are completed to an appropriate standard (including instances where a third party undertakes checks on the organisation's behalf) ***(Yes or No)***	
4. Does each organisation undertake <u>additional</u> pre-engagement screening of personnel that is commensurate with the risk profile of their roles?	Element 10.070 of the VPDSS states that the organisation undertakes additional personnel screening measures commensurate with the risk to support roles requiring high-assurance and/or handling security classified information.	The organisation: 1. has procedure(s) that clearly document how to undertake additional pre-engagement screening checks for ***high-assurance roles***[44], to an appropriate standard ***(Yes or No)*** Consideration given to the following additional checks already undertaken for all personnel: - Table 4 minimum personnel security vetting checks and requirements for security clearances, noting that not all checks are required for all security clearance levels - Table 5 example additional vetting checks for security clearance applicants	The primary source material referenced under Standard 10 of the VPDSS, relevant to this question and associated criteria are: - PSPF Policy 12 Eligibility and suitability of personnel

[44] ***High-assurance*** roles are ones that the organisation requires additional forms of assurance for. This need for heightened assurance may be based on the functions associated with the role, the level of access to information / systems (including security classified information), the level of influence the role has on the organisation and/or the risk profile of the role.

Question	Control objectives	Criteria tested	Primary source material referenced[43]
		- Personnel Security Adjudicative Guidelines and common risk factor areas 2. has appropriately informed, qualified and skilled personnel undertaking these additional pre-engagement screening checks for *high-assurance* roles ***(Yes or No)*** 3. *(if relevant)* uses accredited / authorised third parties to provide additional pre-engagement screening activities / services for *high-assurance* roles ***(Yes or No)*** 4. has assurance that additional pre-engagement screening checks are completed for *high-assurance* roles, to an appropriate standard (including where a third party undertakes these checks on behalf of the organisation) ***(Yes or No)*** 5. *(if relevant)* has a register of positions requiring security clearances and the clearance level required ***(Yes or No)***	

Annexure B – Minimum personnel screening checks and requirements for a security clearance

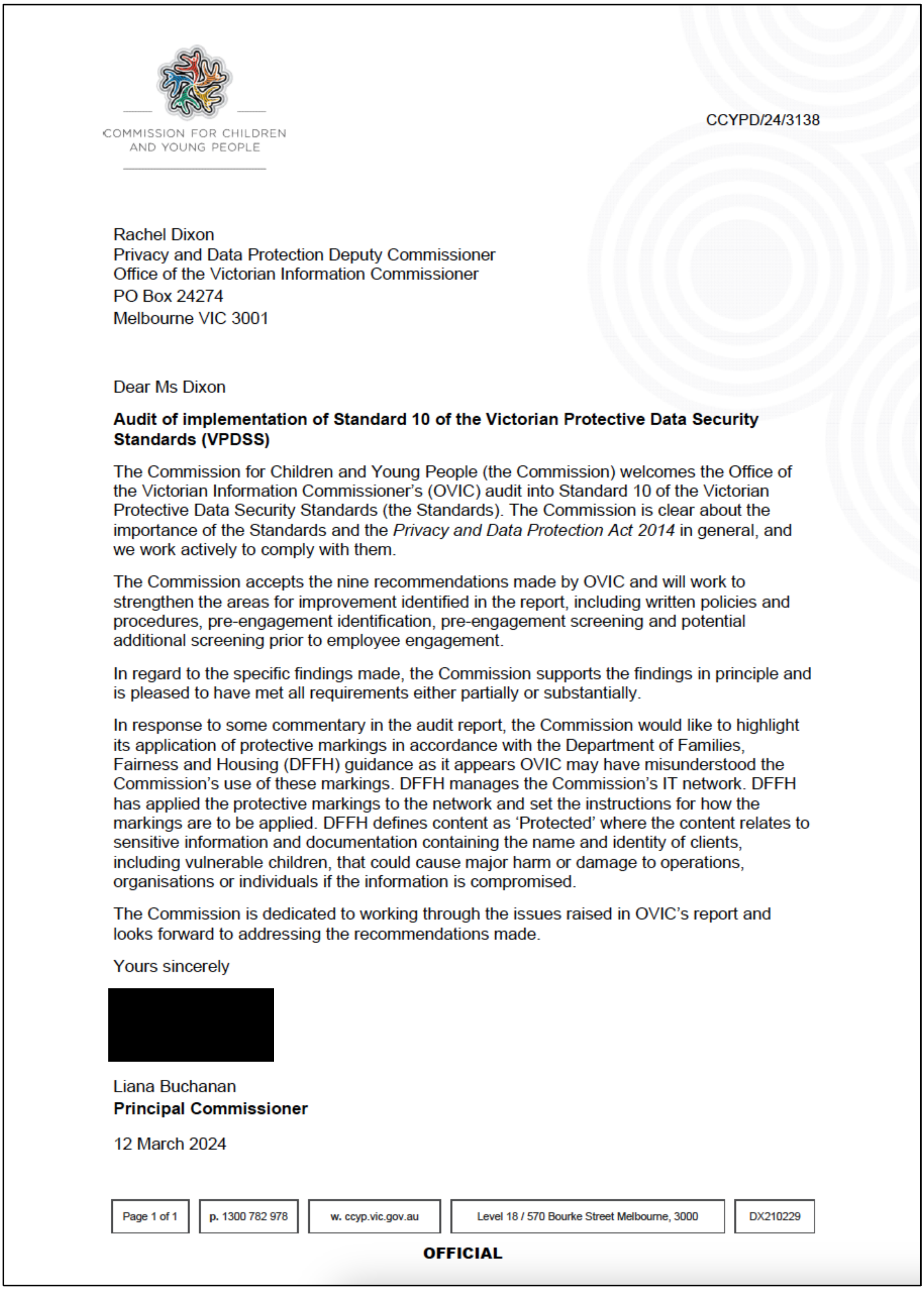
Check	Baseline Vetting	Negative Vetting 1	Negative Vetting 2	Positive Vetting	TOP SECRET – privileged access
Identity check	Required for all security clearance levels. Entities must verify the person's identification documents with the issuing authority by using the Document Verification Service for Australian issued primary identification documents.				
Confirmation of Australian citizenship and status of any other citizenships	Required for all security clearance levels.				
Background assessment	Required for the checkable period of 5 years	Required for the checkable period of 10 years	Required for the checkable period of 10 years	Required for the checkable period that is greater of 10 years or from the age of 16	Required for the checkable period that is from the age of 16, or 10 years if under 26 years of age
Acknowledgment of relevant legislation	Required for all security clearance levels.				

(secrecy of information)					
Referee checks	Required for all security clearance levels.				
Digital footprint check	Required for all security clearance levels.				
National Police Check/criminal history check	Required, no exclusion	Required, full exclusion	Required, full exclusion	Required, full exclusion	Required
Financial history assessment	Required	Required	Required	Required	n/a
Financial statement	Not required	Required	Required	Required with supporting documents	n/a
Financial probity assessment	Not required	Not required	Not required	Required	n/a
Comprehensive financial assessment	n/a	n/a	n/a	n/a	Required
ASIO security clearance suitability assessment	Not required	Required	Required	Required	Required
Security interview	Not required	Not required	Required	Required	Required

Psychological assessment	Not required	Not required	Not required	Required	Required
Overseas travel check	n/a	n/a	n/a	n/a	Required
Statutory declaration (only when vetting is conducted by a state or territory agency	Required	Required	Required	n/a	n/a

Source: PSPF Policy 12, https://www.protectivesecurity.gov.au/system/files/2023-11/pspf-policy-12-eligibility-and-suitability-of-personnel.pdf, Accessed 22 November 2023.

Annexure C – Organisation responses to audit report



COMMISSION FOR CHILDREN AND YOUNG PEOPLE

CCYPD/24/3138

Rachel Dixon
Privacy and Data Protection Deputy Commissioner
Office of the Victorian Information Commissioner
PO Box 24274
Melbourne VIC 3001

Dear Ms Dixon

Audit of implementation of Standard 10 of the Victorian Protective Data Security Standards (VPDSS)

The Commission for Children and Young People (the Commission) welcomes the Office of the Victorian Information Commissioner's (OVIC) audit into Standard 10 of the Victorian Protective Data Security Standards (the Standards). The Commission is clear about the importance of the Standards and the *Privacy and Data Protection Act 2014* in general, and we work actively to comply with them.

The Commission accepts the nine recommendations made by OVIC and will work to strengthen the areas for improvement identified in the report, including written policies and procedures, pre-engagement identification, pre-engagement screening and potential additional screening prior to employee engagement.

In regard to the specific findings made, the Commission supports the findings in principle and is pleased to have met all requirements either partially or substantially.

In response to some commentary in the audit report, the Commission would like to highlight its application of protective markings in accordance with the Department of Families, Fairness and Housing (DFFH) guidance as it appears OVIC may have misunderstood the Commission's use of these markings. DFFH manages the Commission's IT network. DFFH has applied the protective markings to the network and set the instructions for how the markings are to be applied. DFFH defines content as 'Protected' where the content relates to sensitive information and documentation containing the name and identity of clients, including vulnerable children, that could cause major harm or damage to operations, organisations or individuals if the information is compromised.

The Commission is dedicated to working through the issues raised in OVIC's report and looks forward to addressing the recommendations made.

Yours sincerely

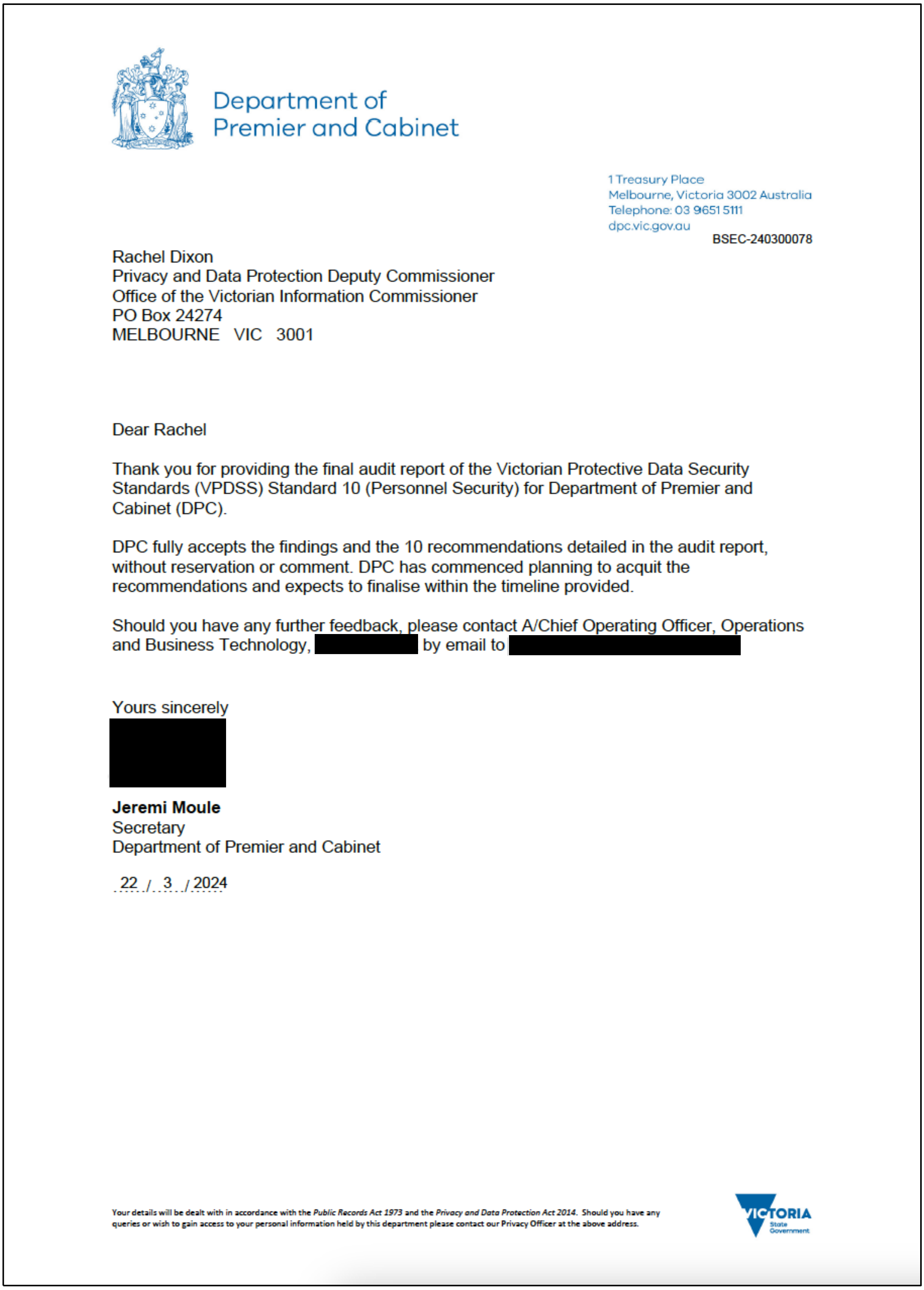
[redacted]

Liana Buchanan
Principal Commissioner

12 March 2024

Page 1 of 1 | p. 1300 782 978 | w. ccyp.vic.gov.au | Level 18 / 570 Bourke Street Melbourne, 3000 | DX210229

OFFICIAL



Department of
Premier and Cabinet

1 Treasury Place
Melbourne, Victoria 3002 Australia
Telephone: 03 9651 5111
dpc.vic.gov.au

BSEC-240300078

Rachel Dixon
Privacy and Data Protection Deputy Commissioner
Office of the Victorian Information Commissioner
PO Box 24274
MELBOURNE VIC 3001

Dear Rachel

Thank you for providing the final audit report of the Victorian Protective Data Security Standards (VPDSS) Standard 10 (Personnel Security) for Department of Premier and Cabinet (DPC).

DPC fully accepts the findings and the 10 recommendations detailed in the audit report, without reservation or comment. DPC has commenced planning to acquit the recommendations and expects to finalise within the timeline provided.

Should you have any further feedback, please contact A/Chief Operating Officer, Operations and Business Technology, [redacted] by email to [redacted]

Yours sincerely

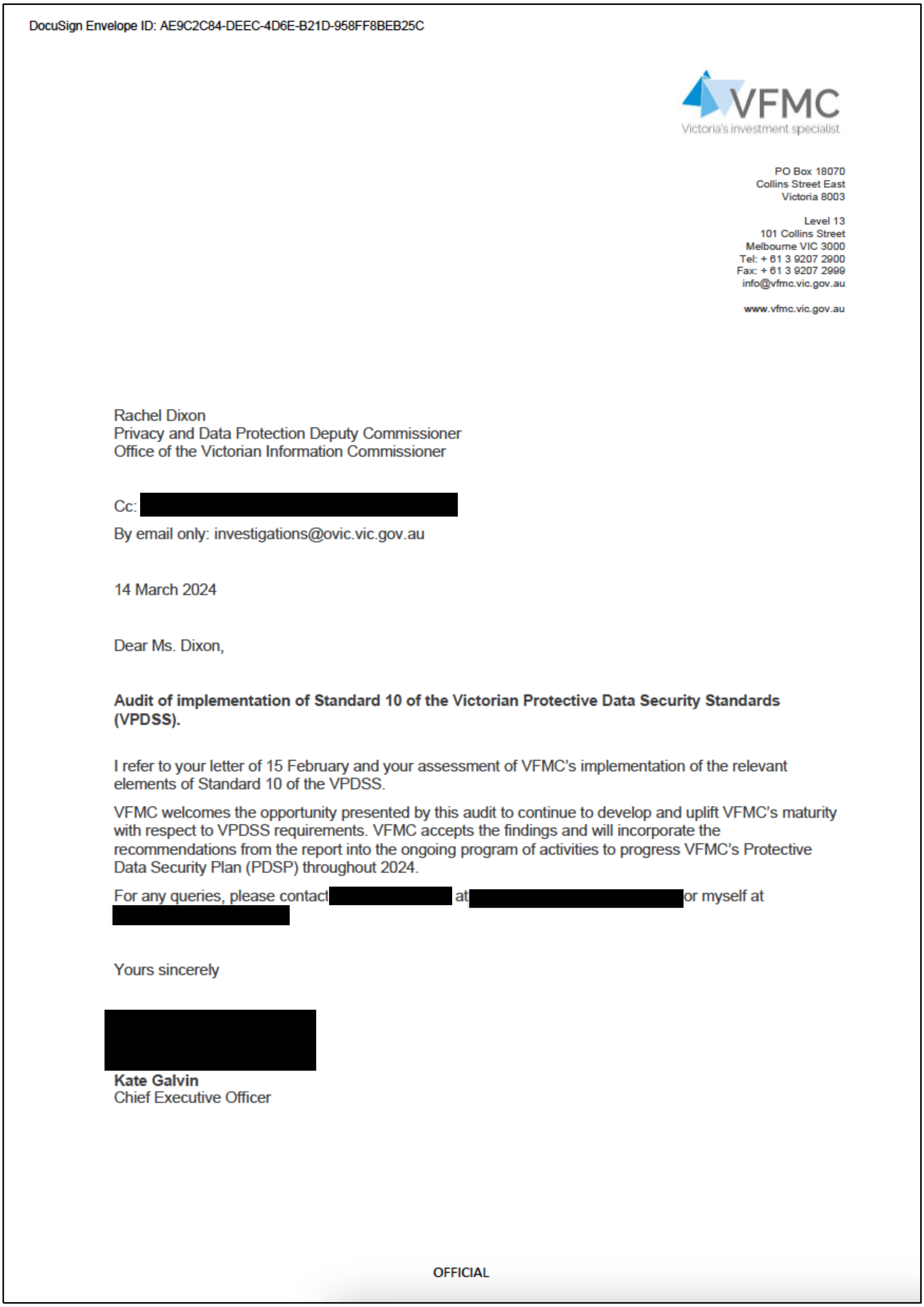
[redacted]

Jeremi Moule
Secretary
Department of Premier and Cabinet

22 / 3 / 2024

Your details will be dealt with in accordance with the *Public Records Act 1973* and the *Privacy and Data Protection Act 2014*. Should you have any queries or wish to gain access to your personal information held by this department please contact our Privacy Officer at the above address.

VICTORIA
State Government



DocuSign Envelope ID: AE9C2C84-DEEC-4D6E-B21D-958FF8BEB25C

VFMC
Victoria's investment specialist

PO Box 18070
Collins Street East
Victoria 8003

Level 13
101 Collins Street
Melbourne VIC 3000
Tel: + 61 3 9207 2900
Fax: + 61 3 9207 2999
info@vfmc.vic.gov.au

www.vfmc.vic.gov.au

Rachel Dixon
Privacy and Data Protection Deputy Commissioner
Office of the Victorian Information Commissioner

Cc: [redacted]

By email only: investigations@ovic.vic.gov.au

14 March 2024

Dear Ms. Dixon,

Audit of implementation of Standard 10 of the Victorian Protective Data Security Standards (VPDSS).

I refer to your letter of 15 February and your assessment of VFMC's implementation of the relevant elements of Standard 10 of the VPDSS.

VFMC welcomes the opportunity presented by this audit to continue to develop and uplift VFMC's maturity with respect to VPDSS requirements. VFMC accepts the findings and will incorporate the recommendations from the report into the ongoing program of activities to progress VFMC's Protective Data Security Plan (PDSP) throughout 2024.

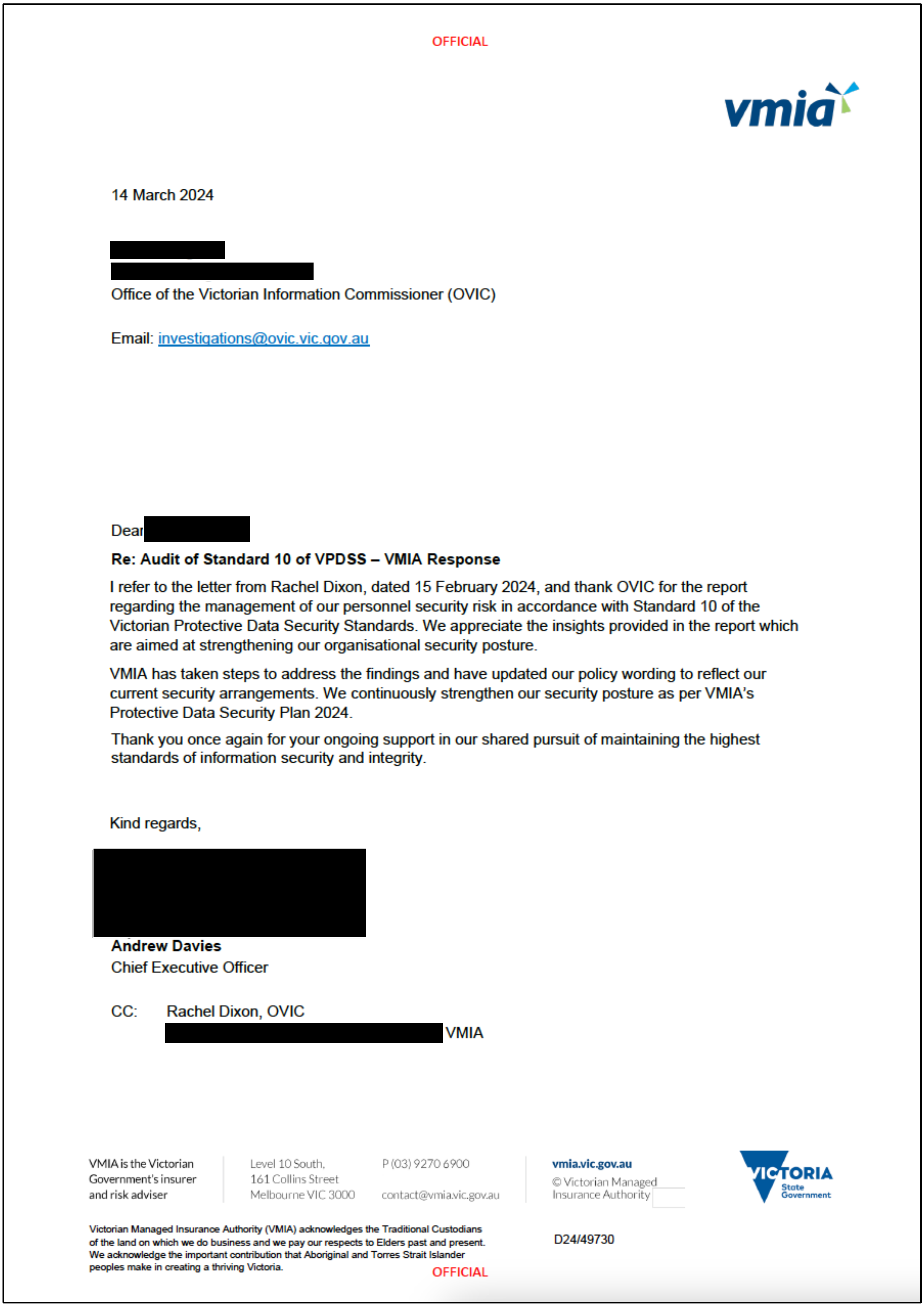
For any queries, please contact [redacted] at [redacted] or myself at [redacted]

Yours sincerely

[redacted]

Kate Galvin
Chief Executive Officer

OFFICIAL



OFFICIAL

vmia

14 March 2024

[redacted]
Office of the Victorian Information Commissioner (OVIC)

Email: investigations@ovic.vic.gov.au

Dear [redacted]

Re: Audit of Standard 10 of VPDSS – VMIA Response

I refer to the letter from Rachel Dixon, dated 15 February 2024, and thank OVIC for the report regarding the management of our personnel security risk in accordance with Standard 10 of the Victorian Protective Data Security Standards. We appreciate the insights provided in the report which are aimed at strengthening our organisational security posture.

VMIA has taken steps to address the findings and have updated our policy wording to reflect our current security arrangements. We continuously strengthen our security posture as per VMIA's Protective Data Security Plan 2024.

Thank you once again for your ongoing support in our shared pursuit of maintaining the highest standards of information security and integrity.

Kind regards,

[redacted]

Andrew Davies
Chief Executive Officer

CC: Rachel Dixon, OVIC
[redacted] VMIA

VMIA is the Victorian
Government's insurer
and risk adviser

Level 10 South,
161 Collins Street
Melbourne VIC 3000

P (03) 9270 6900
contact@vmia.vic.gov.au

vmia.vic.gov.au
© Victorian Managed
Insurance Authority

VICTORIA State Government

Victorian Managed Insurance Authority (VMIA) acknowledges the Traditional Custodians of the land on which we do business and we pay our respects to Elders past and present. We acknowledge the important contribution that Aboriginal and Torres Strait Islander peoples make in creating a thriving Victoria.

D24/49730

OFFICIAL

OVIC

www.ovic.vic.gov.au