Office of the Victorian Information Commissioner

Standard 8 of the Victorian Protective Data Security Standards

Audit of information security in third-party arrangements under section 8D(2)(b) of the *Privacy and Data Protection Act 2014* (Vic)

Table of contents

Foreword

The Victorian Protective Data Security Standards establish 12 high level mandatory requirements to assist Victorian public sector (**VPS**) organisations protect public sector information.

Standard 8 relates to third-party arrangements. It requires VPS organisations to ensure that any third-parties they engage to collect, hold, manage, use, disclose or transfer public sector information in a secure way.

The standard recognises that there are information security risks when an organisation engages third-parties. Its object is to ensure that the public sector information held by the organisation remains protected when this occurs – by requiring the assessment and mitigation of risk before, during and after the engagement.

In this audit, OVIC sought to establish whether the four organisations subject to the audit have appropriate practices and procedures in place to ensure third-parties they share public sector information with are dealing with it securely.

While none of the organisations were considered 'effective' across all four audit criteria, there was a wide range of practices and procedures at varying levels of sophistication. We aim to highlight some of the good practices and key learnings in this report.

The audit results suggest that there are many opportunities for strengthening management of information security risks across the public sector, right across the life of a third-party engagement.

This includes assessing the security risks of entering third-party arrangements; identifying and responding to changes to risk through the life of an engagement; taking active assurance measures to ensure third-parties are meeting their security obligations rather than relying only on contractual clauses; and protecting information at the conclusion of a third-party engagement.

I thank the four audited organisations for their involvement in and constructive approach to the audit. They invested significant time and other resources to consider and assess their practices and procedures for securing public sector information. The audit process has helped them to reflect on their practices and will provide sound guidance to other public sector organisations.

Sven Bluemmel
Victorian Information Commissioner

20 July 2022

Executive Summary

1. The Victorian Protective Data Security Framework and accompanying Victorian Protective Data Security Standards (**VPDSS**) were released in 2016. Adherence to the Standards is mandatory for all organisations within the scope of Part 4 of the *Privacy and Data Protection Act 2014* (**PDP Act**).

2. On 18 October 2021 the Privacy and Data Protection Deputy Commissioner commenced an audit with respect to Standard 8 of the VPDSS of four Victorian public sector (**VPS**) organisations - Department of Environment, Land, Water and Planning (**DELWP**); Department of Jobs, Precincts and Regions (**DJPR**); Transport Accident Commission (**TAC**); and Victorian WorkCover Authority (**WorkSafe**) (**the Organisations**).

3. The purpose of the audit was to confirm that the four Organisations subject to the audit have practices and procedures in place to ensure third-parties they share public sector information with are securing it. To do this, the audit assessed the organisations' practices against Standard 8, with reference to specific audit criteria, to express an opinion about the effectiveness of the Organisations in ensuring that third-parties they work with handle public sector information securely.

4. The audit involved OVIC meeting with staff from the four Organisations to discuss their adherence to Standard 8, reviewing supporting documentation and reviewing selected third-party arrangements from each Organisation.

5. To reach an audit conclusion OVIC assessed the Organisations against four criteria:

    - How the Organisation assesses the security risks of entering an engagement with a third-party;
    - How the Organisation identifies and responds to changes to risk through the life of an engagement;
    - How the Organisation ensures that third-parties are meeting their security obligations.; and
    - How the Organisation protects information at the conclusion of a third-party engagement.

How the organisation assesses the security risks of entering an engagement with a third-party

6. All four Organisations had practices and procedures to assess the security risks of entering an engagement with a third-party. All Organisations were able to demonstrate that risks (often with respect to spend amounts) are identified and assessed prior to finalising a third-party arrangement.

7. The Organisations that were assessed as 'effective' by OVIC ensured that information security risks were identified and assessed, in addition to other identified risks such as spend amount. These VPS organisations utilised assessment tools which assisted in identifying the information security risks, and controls that should be put in place prior to finalising a third-party agreement, and they ensured that the process for doing so was clearly documented in policy and procedure documentation. The Organisations assessed as 'partially effective' demonstrated that information security assessments were being conducted but did not have clearly documented policy and procedure documentation, and therefore OVIC could not be satisfied that assessments were happening consistently across all third-party arrangements.

How the organisation identifies and responds to changes to risk through the life of an engagement

8. All four Organisations took some steps to identify and respond to risks during the life of a third-party arrangement (with some Organisations demonstrating more sophisticated steps than others). However, OVIC is of the view that this is an area that all four Organisations require improvement in.

9. To adhere to Standard 8, organisations should implement a framework for reviewing third-party arrangements in response to events and changing levels of risk that occur during the life of the arrangement. The Organisations that were assessed higher than others were able to provide OVIC with policy and procedure documentation with respect to incident response management, contract management processes and change management processes. They were also able to demonstrate that all information security risks were considered in identifying and responding to changes of risk, and not just cyber security risks.

How the organisation ensures that third-parties are meeting their security obligations

10. All four Organisations demonstrated to OVIC that third-parties were made aware of their security obligations, however the Organisations varied in their level of assurance activities with respect to this issue.

11. Some Organisations utilised Contract Managers and contract management plans to assist in ensuring third-parties meet their security obligations, while others utilised contractual terms within the third-party agreement. However, all Organisations required improved documentation for their policies and procedures.

12. Relying on appropriate contractual clauses can provide partial information security mechanisms. However, doing so without appropriate assurance mechanisms can be problematic. OVIC is of the view that having appropriate policy and procedure documentation that is followed by Organisation staff would assist in ensuring there is an appropriate assurance mechanism in place.

How the organisation protects information at the conclusion of a third-party engagement.

13. Two of the four Organisations were able to demonstrate to OVIC that they effectively protected public sector information at the conclusion of a third-party engagement. They were able to demonstrate good policy and procedures, as well as guidance material such as checklists, to ensure public sector information was protected.

14. The remaining two Organisations require improvement in this area, as it is an integral part of ensuring public sector information is protected. Those Organisations demonstrated a heavy reliance on the third-party returning or destroying the public sector information without the input or oversight from the Organisation.

OVIC's Assessment of each Organisation

Agency	1. Risk assessment before engagement	2. Identifying and responding to change to risk	3. Assurance and monitoring	4. Concluding the engagement
TAC	Effective	Partially Effective	Partially Effective	Effective
DELWP	Effective	Partially Effective	Partially Effective	Partially Effective
WorkSafe	Partially Effective	Partially Effective	Partially Effective	Partially Effective
DJPR	Partially Effective	Partially Effective	Not Effective	Effective

Background

15. The Victorian Protective Data Security Framework and accompanying Victorian Protective Data Security Standards were released in 2016. Adherence to the Standards is mandatory for all organisations within the scope of Part 4 of the PDP Act. This includes most VPS organisations but does not include councils, universities, public hospitals, and health services. The organisations within the scope of Part 4 of the PDP Act are referred to as 'VPS organisations' in this report.

16. Standard 8 states:

> *An organisation ensures that third-parties securely collect, hold, manage, use, disclose or transfer public sector information.*

17. 'Third-parties' refers to any organisation that deals with public sector information for, or on behalf of, the VPS organisation, for example, contracted service providers.

18. The objective of Standard 8 is to ensure that public sector information is protected when a VPS organisation interacts with a third-party.

Our Audit

Purpose and objective of the audit

19. The purpose of the audit was to confirm that the four VPS organisations subject to the audit have practices and procedures in place to ensure third-parties they share public sector information with are securing it.

20. The objective was to assess VPS organisations' practices against Standard 8, with reference to specific audit criteria, to express an opinion about the effectiveness of those Organisations in ensuring that third-parties handle public sector information securely.

What we audited

21. To reach an audit conclusion, we assessed the Organisations against four criteria:

    1. How the organisation assesses the security risks of entering an engagement with a third-party;
    2. How the organisation identifies and responds to changes to risk through the life of an engagement;
    3. How the organisation ensures that third-parties are meeting their security obligations; and
    4. How the organisation protects information at the conclusion of a third-party engagement.

Criterion one

22. As part of OVIC's assessment of criterion one, OVIC focussed on elements E8.010[1] and E8.030[2] and considered the following:

    - The Framework for assessing security risks of proposed third-party arrangements and addressing residual risks prior to finalising the arrangement. This included reviewing policy documents, guides, checklists, and any other governance documents relevant to this criterion;
    - Whether the Organisation has a Register of third-party arrangements and whether that register contained information relating to the risk assessment of the third-party; and
    - The Organisations' Enterprise risk management framework.

Criterion two

23. As part of OVIC's assessment of criterion two, OVIC focussed on elements E8.010[3] and E8.060[4] and considered the following:

    - The contractual term requiring third-parties to report information security incidents;
    - The Framework for reviewing third-party arrangements;
        i. In response to information security incidents;
        ii. In response to change events;
        iii. Periodically; and
    - The change management process for third-party arrangements.

[1] E.8010 The organisation's information security policies, procedures and controls cover the entire lifecycle of third-party arrangements (e.g., contracts, MOUs and information sharing agreements).
[2] E.8030 The organisation undertakes an information security risk assessment of the third-party's service offering and addresses any residual risks prior to finalising the arrangement.
[3] See 2
[4] E8.060 The organisation monitors, reviews, validates, and updates the information security requirements of third-party arrangements and activities.

Criterion three

24. As part of OVIC's assessment of criterion three, OVIC focussed on elements E8.010[5], E8.020[6], and E8.040[7] and considered the following:

    - Whether the Organisation has a register of third-party arrangements;
    - Whether the Organisation has a framework to determine frequency and density of third-party monitoring activities;
    - Whether the Organisation has monitoring activities designed to check that third-parties are complying with their contractual security obligations; and
    - Whether the Organisation has an allocation of information security responsibilities for third-party arrangements to identified Organisation staff.

Criterion four

25. As part of OVIC's assessment of criterion four, OVIC focussed on elements E8.010[8] and E8.090[9] and considered the following:

    - Whether the Organisation has a procedure for the recovery of public sector information from third-parties at the conclusion on an engagement; and
    - Whether the Organisation has a procedure for terminating access to systems at the conclusion of an engagement.

How we conducted the audit

26. The audit method involved:

    - Reviewing Organisations' policy and procedure documents relating to ongoing engagement with third-parties;
    - Reviewing the Organisations' template Memoranda of Understanding, information sharing agreements and contracts used for third-party engagement;
    - Reviewing Organisations' register of third-party arrangements;
    - Reviewing a sample of three third-party arrangements per Organisation; and
    - Speaking with those responsible for engagement with third-parties and information sharing arrangements to hear how third-parties are procured and managed.

[5] See 2
[6] E8.020 The organisation includes requirements from all security areas in third-party arrangements (e.g., contracts, MOUs and information sharing agreements) in accordance with the security value of the public sector information.
[7] E8.040 The organisation identifies and assigns information security roles and responsibilities in third-party arrangements (e.g., contracts, MOUs and information sharing agreements).
[8] See 1
[9] E8.090 The organisation applies appropriate security controls upon completion or termination of a third-party arrangement (e.g., contracts, MOUs and information sharing agreements).

27. At the conclusion of the evidence gathering stage of the audit OVIC wrote to each Organisation, explaining in detail our preliminary view with respect to their assessment against each of the four criteria. OVIC offered the Organisations an opportunity to respond to the preliminary assessment and provide any further information or evidence. Each of the four Organisations responded to the preliminary assessment.

How we assessed the Organisations

28. Audited Organisations were assessed against the four aspects of Standard 8 as being either 'effective', 'partially effective' and 'not effective'.

29. 'Effective' means that, based on evidence provided to OVIC, the audited VPS Organisation has effectively addressed the audit criteria.

30. 'Partially effective' means that, based on evidence provided to OVIC, the audited VPS Organisation has addressed the audit criteria, subject to the qualifications described in this report.

31. 'Not effective' means that, based on evidence provided to OVIC, the audited VPS Organisation has not effectively addressed the audit criteria.

VPS Organisations audited

32. The audited VPS Organisations were:

    - Department of Environment, Land, Water and Planning (**DELWP**);
    - Department of Jobs, Precincts and Regions (**DJPR**);
    - Transport Accident Commission (**TAC**); and
    - Victorian WorkCover Authority (**WorkSafe**).

The Organisations' engagement with OVIC

33. All audited Organisations provided OVIC with access to documents and personnel necessary for OVIC to complete the audit.

Power to conduct the audit

34. The audit was carried out under s 8D(2)(b) of the PDP Act. The PDP Act gives the Data Protection Deputy Commissioner the power to audit VPS organisations 'to ascertain compliance with data security standards.'

Focus of the audit report

35. This report will focus on the key learnings and practices found by OVIC. The report will highlight each Organisations' assessment against the four criteria however the focus of the discussion within the report is on the practices and procedures OVIC considers important for the wider VPS community to understand and learn from.

What we found: adherence to Standard 8 of the VPDSS

Criterion one: Do VPS Organisations effectively assess the security risks of entering an engagement with a third-party?

36. Each of the four Organisations demonstrated to OVIC that there was a process for assessing risk prior to entering a third-party arrangement however, with varying degrees of effectiveness. OVIC assessed the Organisations' performance against criterion one as follows:

Organisation	**OVIC's Assessment**
TAC	Effective
DELWP	Effective
WorkSafe	Partially Effective
DJPR	Partially Effective

Framework for assessing security risks of proposed third-party arrangements and addressing residual risks prior to finalising the arrangement

37. Both TAC and DELWP demonstrated that they performed risk assessments on third-parties. Each Organisation approached the risk assessments in different ways.

38. Prior to commencing a procurement TAC categorises the procurement into one of three complexity categories: 'simple,' 'moderate' or strategic'. Each of the categories have features to assist TAC staff in identifying the most appropriate complexity group. Once a procurement has been categorised, it then has a designated procurement process based on its complexity.

39. This procurement process includes the requirement to consult with speciality advisors within TAC such as the information security team as well as the privacy team. To assist it with the risk assessment process TAC has formulated questionnaires to be used throughout the stages of procurement. The questionnaires request information from the prospective vendors on a range of topics relative to information security. These include questions about:

    - Business Impact Levels (**BILs**);
    - Vendor access to TAC data;
    - Data transmission to the vendor;
    - Cross border services and whether TAC data will be stored outside of Australia;
    - Cloud Services;
    - Access to TAC facilities (physical access);
    - Whether the third-party uses sub-contractors; and
    - Whether the vendor requires access to TAC devices.

40. The information gathered via the questionnaires is assessed by the Information Security Unit and/or Privacy unit within TAC, and advice is provided to the procurement and legal teams about the risk assessment, rating of the prospective vendor, and the controls that should be put in place prior to engaging the vendor.

41. DELWP, on the other hand, performs most of its risk assessments prior to going to tender. DELWP uses a report called the 'Information Security Classification Grading and Risk Report.' The objective of the report is to assess, grade, and document the data classification and risks for the proposed third-party engagement prior to commencing the procurement process.

42. The report addresses the objective of the new information asset/system or application that DELWP is proposing to procure. It then performs an assessment of the information and information systems that are proposed to be used as part of the procurement. This involves identifying all the information, classifying it, applying a security grading, performing a business impact assessment on the information, and using all that information to perform a risk assessment. To complete the report DELWP procurement team must consult with the information security, privacy units, and any other speciality unit within DELWP that is relevant to the proposed procurement.

43. The report is used as guidance for DELWP Executive group to make a risk-based decision to endorse the project and proposed third-party arrangement. For the Executive to make such a decision, the report must be supported by a detailed privacy impact assessment, system security plan, business continuity and disaster recovery plan.

44. The report is also used to identify the information security controls that DELWP will require to be included in the Request for Quote (**RFQ**). All the relevant information security controls are defined and detailed in the RFQ and form part of the requirements of the tender.

45. This process is different to TAC's, in which the information security controls are identified towards the end of the tender process, based on the vendors' response to tender.

46. It is OVIC's view that both approaches to risk assessments are effective. However, it is important to note that the DELWP process of identifying controls based on risk assessment performed prior to the RFQ being released and on a defined scope of work may not identify all information security risks and controls if the scope changes throughout the procurement process. It is OVIC's recommendation that if the DELWP process is used, a final risk assessment or checklist should be created to ensure that all risks and controls are identified prior to finalising the third-party arrangement.

47. Both TAC and DELWP had comprehensive policy and guidance material to assist staff with the information risk assessments during a procurement.

48. WorkSafe was also able to demonstrate that some risk assessments were performed on third-parties. Like TAC, WorkSafe has a Procurement Framework which defines and details three categories of procurement: low, medium, and high. However, unlike TAC these categories are based on their spend value, and factors and considerations with respect to risk or information security are not detailed.

49. OVIC was able to determine via interviews with WorkSafe personnel and review of sample third-party engagements that WorkSafe does perform risk assessments, both at the commencement of a procurement and prior to finalising an arrangement. WorkSafe does this by completing a 'Strategic Procurement Plan.' The plan assists WorkSafe staff to identify and manage risks during the procurement phase.

50. Like TAC, WorkSafe uses questionnaires to assist it in determining the information security risks of each vendor, and to determine what controls are required to be in place prior to finalising a third-party arrangement. Unlike TAC and DELWP, WorkSafe did not have sufficiently comprehensive policy and procedure documentation for OVIC to assess it as 'effective.' While the personnel interviewed by OVIC demonstrated a good understanding of the processes needed to assure security, without a policy and procedure document that describes and outlines such processes, OVIC has concerns that new personnel may not have the same understanding of the processes. This could mean that the process of assessing risks in third-party arrangements will be inconsistent.

51. Like WorkSafe, DJPR also lacked comprehensive and clear policy and procedure documentation.

52. DJPR provided OVIC with a comprehensive information security checklist document that would assist DJPR in performing effective risk assessments of third-party arrangements.

Register of third-party arrangements and whether that register contained information relating to the risk assessment of the third-party

53. All four Organisations record third-party arrangements on a register or database. However, the effectiveness of each varied.

54. TAC has a centralised contract register. This register includes all third-party engagements TAC has, including grants, and engagements other than procurements. It is a written record of all engagements managed by the procurement team.

55. The types of information that is kept on the register is:

    - Copies of all contract documentation;
    - Assurance certificates;
    - Approvals;
    - Unique record number;
    - Responsible Contract Manager; and
    - Value.

56. Currently the risk rating for each engagement is not easily identified. Each file in the register has a link to the corporate filing system where the risk assessments and contract management plans can be located. The register is a monitored database and has a full time FTE contract support officer who is responsible for maintaining and managing the register. Their role is to make sure all the information in the register is accurate and up to date.

57. WorkSafe uploads all third-party arrangements into a program called the Oracle database.

58. Oracle is a centralised system where WorkSafe employees can upload and view details of the third-party arrangements. The type of information contained within the Oracle database includes:

    - the value;
    - key contract dates and information;
    - copies of the contract documents;
    - key roles and responsibilities;
    - the operational Contract Manager; and
    - the procurement sponsor.

59. The Oracle database triggers expiration notifications of the term of the contract and interconnects with the procedure pay system to mitigate the risk of non-compliance. Currently the system does not contain information on the risk rating of the third-party arrangement, however a report could be generated to identify all high-risk procurements (based on spend amount only).

60. DELWP uses a similar program called Cypress iContract. The register is monitored by DELWP staff members to ensure it remains up to date. The register does not contain information about the risk rating of the third-party engagement. Information about the risk is contained in the information that is attached to the file within the register.

61. DJPR also uses the Oracle database however, it is monitored by the Accounts Payable team within DJPR, and the register contains vendor name, vendor contact details and ABN. The accounts payable team is responsible for maintaining and managing the data in Oracle.

62. Due to the limited information contained within the register OVIC was unable to determine the current third-party arrangements, to understand the risk rating or obtain any further information with respect to information security of DJPR's third-party arrangements.

The Organisations' enterprise risk management framework

63. All four Organisations had an enterprise risk management framework that included at least one information security risk relevant to third-party arrangements. OVIC was satisfied with the quality and standard of all four Organisations' enterprise risk management frameworks.

Criterion two: Do VPS Organisations effectively identify and respond to changes to risk through the life of an engagement?

64. All four Organisations demonstrated some level of identifying and responding to risks during the life of a third-party arrangement (with some Organisations demonstrating higher levels than others). However OVIC is of the view that this is an area that all four Organisations require improvement in. Contract management is a significant aspect of ensuring public sector information is protected.

65. OVIC assessed the Organisations' performance against criteria two as follows:

Organisation	**OVIC's Assessment**
TAC	'Partially Effective'
WorkSafe	'Partially Effective'
DELWP	'Partially Effective'
DJPR	'Partially Effective'

The contractual term requiring third-parties to report information security incidents.

66. Both TAC and WorkSafe have strong contractual clauses requiring a third-party to report information security incidents.

67. TAC and WorkSafe have clauses in their contracts that require the third-party to notify TAC of any security incidents and/or events. Both Organisations require their third-parties to provide monthly reports for general security incidents or events. However, if a serious incident occurs, the third-party is required to notify TAC/WorkSafe immediately.

68. OVIC was unable to determine DJPR had effective contractual controls requiring third-parties to report incidents.

69. DELWP did not provide OVIC with pro forma contracts, and the sample third-party arrangements reviewed by OVIC did not include any contract material. This is because DELWP often engages third-parties through 'head Agreements' that are owned and controlled by the Department of Premier and Cabinet (**DPC**), which means that the contractual terms requiring the third-party to report information security breaches are contained in the agreement between DPC and the third-party.

70. DJPR and DELWP provided OVIC with a template 'Master Supply Agreement', which contained several pro forma terms relating to the protection of personal information and actual, threatened, or suspected information security breaches by third-parties.

Framework for reviewing third-party arrangements in response to information security incident, change events and periodically

71. DELWP has comprehensive cyber-incident response policy and procedure documents that assist DELWP employees to effectively respond to cyber events. However, as DELWP's focus was on cyber incidents it was unable to demonstrate to OVIC that the incident response framework extended to information security incidents more generally.

72. DJPR was able to demonstrate that its policy and processes with respect to incident management and response were comprehensive and effective. DJPR provided OVIC with several detailed and thorough plans, registers, workflows, and playbooks to assist it in effectively responding to information security incidents.

73. Like DJPR, TAC was also able to demonstrate to OVIC that its policy and processes with respect to incident management and response were comprehensive and effective. TAC's incident policy and processes provide for the triaging of security incidents to assist in identifying who in the organisation is best suited to respond. It also defines a security incident as when confidentiality, integrity and/or availability has been compromised and resulted in financial, data or asset loss, or the impact is an adverse effect on operational service delivery or reputational damage. Importantly, TAC was the only Organisation to demonstrate that a third-party arrangement is reviewed as part of a post information security incident activity. TAC assesses the controls of the third-party and ensures that any further controls that are required because of the incident are put in place prior to the third-party arrangement continuing.

74. WorkSafe provided OVIC with a comprehensive incident management/response document. It contained guidance on:

    - Ensuring third-parties are aware of their obligation to report security incidents;
    - Formalising appropriate roles and responsibilities to handle incidents;
    - Performing post-incident analysis and evaluation of current controls; and
    - Ensuring that a written incident response or recovery plan is put in place following a third-party incident notification.

75. However, this comprehensive document was provided to OVIC in draft form, and OVIC was unable to determine if the processes contained within it were in place. Furthermore, WorkSafe did not provide OVIC with an information security incident policy.

76. With respect to contract management and responding to change events and third-parties periodically, all four Organisations were able to demonstrate that some form of contract management was taking place. However, most of this contract management was performed as part of the performance management process and focussed on the management of KPI's rather than information security.

77. WorkSafe demonstrated to OVIC that it monitors its third-parties in accordance with the information security risk rating. WorkSafe has implemented a contract management process that identifies the need to monitor higher risk third-parties more frequently than those who are lower risk.

78. WorkSafe manages its third-parties through Contract management plans that are assigned to a Contract Manager. It is this Contract Manager's responsibility to ensure the plan is adhered to. This is usually done by monthly meetings with the third-party to go through the plan. To ensure that its Contract Managers are progressing in accordance with the plans, WorkSafe also conducts weekly operational meetings to ensure that the Contract Managers are on top of their responsibilities.

79. Like WorkSafe, DELWP also uses Contract Managers to conduct regular performance reviews on third-parties. However, unlike WorkSafe, DELWP was unable to demonstrate to OVIC that the performance reviews extended beyond the management of KPI's to consider information security.

80. TAC is in the process of moving to a contract management process that mirrors WorkSafe's. TAC will be transitioning to a contract management system that manages third-parties based on information security risk. TAC informed OVIC that it recognised the need for greater assurance and risk management for its higher risk 'strategic contracts', and as such will be adopting a tiering model to assist in identifying those third-parties that require more frequent monitoring.

81. At the time of the audit, however, TAC had not implemented its new contract management strategy and was performing reviews around contract renewal times, and when a third-party has notified it of any changes.

82. TAC also has an internal audit function that regularly reviews TAC third-party arrangements. The internal audit plan is set at the beginning of each year and selects various third-party arrangements to review. If any factors are identified as part of the internal audit, they are referred to the procurement and legal team for further review, advice, and recommendations on management. However, OVIC was also unable to determine how many of these internal assessments are performed by TAC per year, and whether it covers a large enough sample of the total number of third-parties TAC engages.

83. With respect to the reviewing of third-party arrangements, DJPR provided OVIC with its Contract Management Framework. The purpose of the document is to provide a clear and standardised approach to contract management. It outlines how to manage and administer contracts for goods and services, and defines governance and reporting requirements, roles and responsibilities, and contract management phases. It also provides information on contract variation, and the approval process for contract variation.

84. DJPR also provided OVIC with its Contract Management Plan, which was a comprehensive document used to assist the Contract Managers in the regular review of a third-party arrangement.

85. However, the documents provided by DJPR made no reference to information security risks and focussed on the management of KPI's, monetary performance and general risks to the delivery of the product or service.

Change management processes for third-parties

86. DELWP provided OVIC with a copy of a "Schedule of Changes" document that records changes in the terms of a third-party arrangement. This document is monitored regularly and is a comprehensive document that covers the following key areas:

    - The project type;
    - The risk rating (low, medium or high);
    - The impact (low, medium or high);
    - The planned start and end dates;
    - A description of the project;
    - Who it is assigned to;
    - The assignment group; and
    - The close date.

87. DELWP also provided OVIC with a document, 'IT Change Management Process', which identifies the requirements for managing change. However, the sample third-party arrangements OVIC reviewed did not demonstrate that DELWP was performing its change management process consistently.

88. WorkSafe did not provide OVIC with any policy or procedure document with respect to change management. However, OVIC was able to determine that the contractual clauses WorkSafe uses in high-risk third-party arrangements require a third-party to provide WorkSafe with a succession plan in the event the third-party wishes to terminate its agreement early or does not wish to renew the agreement.

89. WorkSafe provided a copy of a sample succession plan from one of its third-parties. The document contained detailed action plans for the following areas:

    - Governance;
    - Monitoring and Reporting;
    - Resource planning;
    - Change management Framework;
    - Engagement and Communications;
    - Risk Management Plan;
    - Customer Transfer; and
    - Record and File Transfer.

90. WorkSafe reviews all succession plans and provides formal written approval of the succession plan. The succession plan cannot be implemented by the third-party without approval from WorkSafe. Once the succession plan is approved, it becomes binding on the third-party and WorkSafe both before and after the expiration of the arrangement.

91. Overall, WorkSafe has very comprehensive contractual terms with respect to identifying and responding to risks throughout the life of an engagement and relies heavily on those terms to guide it. It is OVIC's view that this could be problematic. Heavy reliance on contractual terms without policy and procedure documents to support these could result in important assurance mechanisms being overlooked.

92. At the time of the audit, TAC was unable to demonstrate that it had a change management process in place, however TAC informed OVIC that a change management process will be built into the contract management strategy discussed above.

93. With respect to DJPR's change management processes, OVIC found no evidence of a change management process for third-parties in the information obtained from DJPR throughout the audit.

Criterion three: Do VPS Organisations effectively ensure that third-parties are meeting their security obligations?

94. All four Organisations demonstrated to OVIC that third-parties were made aware of their security obligations, however the Organisations varied in their level of assurance activities with respect to this issue.

95. OVIC assessed the Organisations' performance against criterion three as follows:

Organisation	OVIC's Assessment
TAC	Partially Effective
WorkSafe	Partially Effective
DELWP	Partially Effective
DJPR	Not Effective

96. With respect to the question of whether the Organisation has a register of third-party arrangements, please refer to criterion one on paragraph 53 above.

Framework to determine frequency and density of third-party monitoring activities

97. At present TAC does not have any formal or documented processes for monitoring its third-parties' compliance with their security obligations.

98. TAC informed OVIC that it is in the process of moving to a risk-based assurance process that will align the frequency and density of third-party monitoring activities to the risk rating of the third-party.

99. DELWP provided OVIC with a Contract Management Plan, which is a comprehensive document that ensures the Contract Manager is aware of the risk associated with the third-party arrangement and provides a suitable plan for managing those risks.

100. DELWP also provided OVIC with policy and procedure documentation that outlines the process for contract management and when and how the Contract Management Plan is to be used.

101. WorkSafe relies heavily on contractual clauses to assist in ensuring third-parties are meeting their security obligations. While OVIC generally considers contractual clauses to be insufficient on their own to provide adequate assurance, OVIC was able to determine based on the responses to the audit and the example documentation provided by WorkSafe, that these are effective assurance mechanisms in this instance.

102. Notwithstanding this, OVIC was unable to identify policy and guidance material that reflected the processes demonstrated by WorkSafe.

103. Relying on contractual clauses without policy and procedure documentation to assist in ensuring third-parties are meeting their security obligations can be problematic as it could result in important assurance mechanisms being overlooked.

104. DJPR has a Contract Management Framework document which outlines the frequency of compliance and monitoring activities with respect to third-party arrangements. However, there is no reference to what type of monitoring and assurance activities DJPR undertakes.

Monitoring activities designed to check that third-parties are complying with their contractual security obligations

105. TAC has Managers who are responsible for monitoring and managing third-parties. They do this in accordance with a contract management plan, which is created during the procurement phase based on the initial risk assessment of the third-party. TAC informed OVIC that there is an expectation that Contract Managers are collecting, monitoring, and reviewing information against the third-party's KPIs in accordance with the time frames and terms of the arrangement. However, currently there is no oversight on how, or if, the Contract Managers are doing this.

106. TAC has commenced external audits of its third-parties and has completed one so far. This audit requires the third-party to complete a specific questionnaire like those used by TAC during its procurement process to assist the information security unit within TAC to ensure the third-party is meeting its security obligations. In addition to ensuring the completion of the questionnaire, TAC also performs remote auditing activities such as end-to-end penetration testing, red-teaming exercises, vulnerability scanning and stress testing.

107. DELWP Contract Managers have regular meetings with its third-parties, however OVIC was unable to determine if compliance with contractual security obligations formed part of the meetings. The information obtained from DELWP suggested that the focus of the regular meetings was to ensure the third-party was meeting its KPIs.

108. OVIC determined that for some of DELWP's third-party arrangements it requests annual attestations with respect to information security obligations however, the general principle within DELWP is that unless an issue or an incident is identified, DELWP will rely on the information obtained from the third-party during the procurement process, which in some cases could be years old.

109. OVIC was able to determine that DELWP was performing some monitoring and compliance activities, however the approach was not consistent across all third-party arrangements.

110. Based on the information obtained from DJPR throughout the audit OVIC was unable to ascertain if any information security monitoring activities are included in the contract management process.

Allocation of information security responsibilities for third-party arrangements to identified Organisation staff

111. At the time of the audit TAC did not have an allocation of information security responsibilities for third-party arrangements to identified Organisation staff. However, TAC provided OVIC with a draft RACI[10] matrix that identified key activities for contract management and how, and who they will be assigned to under a 'simple,' 'moderate' and 'strategic' procurement.

112. DELWP, WorkSafe and DJPR did not have an allocation of information security responsibilities for third-party arrangements to identified Organisation staff.

113. Organisations should identify and allocate information security responsibilities for third-party arrangements to identified Organisation staff, as it assists in the overall monitoring and assurance mechanisms and supports accountability.

[10] RACI is an acronym for Responsible, Accountable, Consulted, Informed and is a common term of art in information security.

Criterion four: Do VPS Organisations effectively protect information at the conclusion of a third-party engagement?

114. One of the four Organisations was able to demonstrate to OVIC that it effectively protected public sector information at the conclusion of a third-party engagement. This is an area that the remaining three Organisations require improvement on as it is an integral part of ensuring public sector information is protected.

115. OVIC assessed the Organisations' performance against criterion four as follows:

Organisation	OVIC's Assessment
TAC	Effective
WorkSafe	Partially Effective
DELWP	Partially Effective
DJPR	Effective

Procedure for the recovery of public sector information from third-parties and for terminating access to systems at the conclusion of a third-party engagement

116. TAC has contractual terms regarding the return of and destruction of TAC data. TAC has implemented a 'Quick Reference Guide: Closing a Contract.' This document outlines the process a Contract Manager should go through when closing a contract. It includes a comprehensive checklist document that covers a range of actions that will help protect information which include:

- Ensuring all building passes have been returned;
- Ensuring all TAC devices have been returned;
- Ensuring all TAC provided data and information is destroyed or returned; and
- Ensuring that system access has been cancelled.

117. The newly implemented process ensures that there is an oversight mechanism with respect to the Contract Manager at the conclusion of a third-party engagement, by requiring the checklist to be completed by the Contract Manager and then sent to the contract register for checking and adding to the third-party register.

118. As with criteria 2 and 3, WorkSafe relies heavily on contractual clauses to assist in protecting information at the conclusion of a third-party engagement. OVIC determined that WorkSafe's reliance on the contractual controls is currently working.

119. However, OVIC was unable to identify or locate policy and guidance material that reflected the processes outlined to it by WorkSafe. Relying on contractual clauses without policy and procedure documentation to assist in protecting public sector information at the conclusion of a third-party engagement can be problematic, as it could result in important assurance mechanisms being overlooked.

120. DJPR uses a 'Transition Out Checklist' which requires its Contract Managers to complete prior to closing out a third-party arrangement. Contained within the checklist are specific requirements to ensure access to IT systems has been withdrawn, security passes have been returned, and all DJPR information or material has been destroyed or returned.

121. In addition, DJPR place reliance on its Information Systems Access Management Policy which details the process for managing user ID's and the disablement or removal of old or redundant users. It also contains a process for deprovisioning access to systems.

122. DELWP provided OVIC with a draft 'Decommissioning Process' document which outlines the process for when a third-party arrangement ends. It is comprehensive document that covers off all areas of information security.

Recommendations

123. As a result of this audit OVIC made the following recommendations to each Organisation.

TAC

Recommendation 1

124. That TAC implements a process for ensuring its monitoring and assurance activities are performed in accordance with the level of risk.

Recommendation 2

125. That TAC implements its 'partnered' approach of managing engagements and implement an assurance mechanism that factors in the risk rating of the third-party arrangement.

WorkSafe

Recommendation 3

126. That WorkSafe implements clear policy and guidance material with respect to:

- assessing security risks of entering an engagement with a third-party;
- identifying and responding to risk through the life of a third-party engagement;
- ensuring third-parties meet their security obligations; and
- protecting information at the conclusion of a third-party engagement.

DELWP

Recommendation 4

127. That DELWP implements policy and procedure documents that address all types of information security incidents.

Recommendation 5

128. That DELWP implements its proposed draft process for protecting information at the conclusion of a third-party arrangement and document it in the form of a policy or procedure.

DJPR

129. In comparison to the other three Organisations, DJPR initially provided limited information to OVIC. DJPR had only one representative at the interview, whereas the other agencies ensured that members for all relevant areas were present. In addition to this, the documents and other material provided by DJPR was significantly less than the other Organisations.

130. However, upon receipt of the preliminary assessment DJPR provided a comprehensive supplementary response, which included many additional documents and a comprehensive explanation of how DJPR seeks to adhere to Standard 8.

131. However, the failure to provide material initially may suggest there is a lower level of understanding about their procedures across DJPR, and it is for this reason that OVIC makes the following recommendation.

Recommendation 6

132. That DJPR engages an appropriately qualified consultant to review its practices and procedures for managing security risks when sharing information with third-parties and provide recommendations for improvement. OVIC recommends that the following be considered in the review:

    - How DJPR assesses security risks of entering an engagement with a third-party and documenting that process in policy and procedure documentation;
    - The process for third-parties to notify DJPR of information security incidents;
    - The contract management process and how information security is included in those processes; and
    - The change management process for third-parties.

    This process should be overseen by DJPR's Audit and Risk Committee, and DJPR should provide a copy of the consultant's report and its proposed response to OVIC.

Agency responses

TAC

Thank you for providing the TAC with a pre-publication copy of the Standard 8 Audit Report which we note and accept as presented.

We would like to thank the OVIC Investigations team for an informative and highly valuable assessment of our adherence to Standard 8. As mentioned during the review, third-party risk management continues to be a challenge and the TAC has been focused on understanding and addressing risks in this area in recent times. We also have investment and operational plans in place to continue improving our control environment and this report helps us to keep these initiatives appropriately focused. The TAC will incorporate the two recommendations provided by OVIC as part of this work.

Worksafe

We appreciate OVIC's collaborative approach in undertaking this audit and acknowledge OVIC's affirmation of the effectiveness of our information security practices and controls.

We note the observations and recommendation in the pre-publication audit report and welcome the opportunity to implement measures to further enhance WorkSafe's information security practices.

We have a strong focus on information security and are well-progressed in the implementation of your recommendation.

DELWP

*The Department of Environment, Land, Water and Planning (**DELWP**) welcomes the report and thanks the Office of the Victorian Information Commissioner for the opportunity to assess its performance in ensuring that third-parties securely collect, hold, manage, use, disclose or transfer public sector information, and identify areas for improvement.*

The department notes the findings that:

- *its process of identifying controls based on risk assessments performed prior to an RFQ being released may not identify all information security risks and controls if the scope changes throughout the procurement process*
- *it should extend its incident response framework beyond cyber incidents to information security incidents more generally*

It accepts the two recommendations and provides an action plan to implement them [attachment provided].

DJPR

DJPR welcomes the opportunity to work with OVIC as we continue to strengthen our management of information security risks in line with our obligations under the Privacy and Data Protection Act 2014.

To that end, I can advise that your report and recommendations will be tabled at DJPR's next Audit and Risk Committee. The committee will then receive regular reports as we close out all activities in line with the recommendations set out in the audit.

Again, thank you for working with us on compliance with VPDSS standards.