OVIC
Office of the Victorian
Information Commissioner

Standard 2 of the Victorian Protective Data Security Standards

Audit under section 8D(2)(b) of the *Privacy and Data Protection Act 2014* (Vic)

Table of contents

Foreword

The Victorian Protective Data Security Standards assist Victorian public sector (**VPS**) organisations to mitigate information security risks by using risk management principles.

Standard 2 articulates the foundation of a risk-based approach to information security: identifying, recording, and valuing information assets. An agency cannot protect information it does not know it holds – let alone put appropriate protections in place that reflect the security value of that information.

Agencies provide Protective Data Security Plans (**PDSP**) to my office at least every two years. These tell the story of each agency's information security journey and outline their plan for minimising security risks to public sector information.

In this audit report, OVIC assessed agencies' plans against their practices, and used the observations and findings of the audit to test the organisations' assessments. It follows that an element status of 'implemented' will be closely examined and needs to not only reflect the key controls of the element, but also the process to implement those controls, and that the controls can operate and are operating effectively in their environment.

The audit is not designed to test right and wrong. It is designed for organisations to critically assess the status of the elements in their PDSP and recalibrate if necessary or as required through recommendations.

I thank the agencies for their open and honest engagement with my office. It is to their credit that they have positively engaged with OVIC to review their processes and practices. The audit report will not only be helpful to these agencies, but to all Victorian government agencies working with the Standards.

Government agencies must think of themselves not as owners, but as custodians of information. As custodians, we have a responsibility to ensure that information is identified, recorded, and valued appropriately.

Sven Bluemmel
Information Commissioner

Executive summary

OVIC conducted the audit to assess four organisations' adherence to Standard 2 of the Victorian Protective Data Security Standards (**VPDSS** or **Standards**), and to identify areas of potential improvement. The four organisations involved in the audit were the Department of Treasury and Finance, Barwon Region Water Corporation, the Victorian Institute of Forensic Medicine and CenITex.

The Standards establish 12 high level criteria for the consistent application of risk-based practices to manage the security of Victorian government information. Organisations subject to Part 4 of the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**) are required to adhere to the Standards.

OVIC's audit focused on 'Standard 2 – Information Security Value', which states: 'An organisation identifies and assesses the security value of public sector information.'

The audit assessed each organisation against the elements of Standard 2, as contained in OVIC's *VPDSS Implementation Guidance*,[1] and examined whether the organisations had achieved the level of assessment reported in their 2020 attestations to OVIC.

The audit found that all four audited agencies had practices, procedures, and systems in place to assess the security value of information they hold. Three of the four organisations had a formalised information asset register to record the security value of their information holdings. OVIC saw evidence that each organisation used their conclusions about the security value of their information to develop controls to protect that information.

There were differences between how organisations assessed themselves against some elements and OVIC's assessment. This appeared to be caused by misunderstandings about the requirements of certain elements. OVIC encourages agencies to seek further guidance if material requires clarification. This audit report will provide agencies with a clearer understanding of OVIC's expectations for Standard 2.

Some of the findings of the audit were that:

- none of the audited organisation had an Information Management Framework that incorporated all security areas. While all the organisations had policies and procedures that dealt with security, none had a consolidated framework for managing security risks across all security areas (governance, information, personnel, ICT, and physical security);
- three audited organisations have developed an Information Asset Register (**IAR**). One audited organisation is developing its IAR;
- two audited organisations had developed contextualised Business Impact Level (**BIL**) tables to assist staff to assess the security value of information; and
- two audited organisations apply protective markings.

[1] OVIC, 'Victorian Protective Data Security Standards – Implementation Guidance V2.1'. Available online at https://ovic.vic.gov.au/wp-content/uploads/2021/02/20210216-VPDSS-V2.0-Implementation-Guidance-V2.1.pdf.

Background

Protective data security in the Victorian public sector

The Victorian Protective Data Security Framework

1. The Victorian Protective Data Security Framework (**VPDSF** or **Framework**) is established under Part 4 of the PDP Act. The VPDSS accompany the Framework and were first issued in July 2016. In October 2019, the Standards were reviewed and updated along with the Framework. The Framework and Standards together provide direction to Victorian public sector agencies or bodies on their data security obligations. Adherence to the Standards is mandatory for all organisations within the scope of Parts 4 and 5 of the PDP Act.

2. The Framework[2] provides a model to monitor and measure the extent to which Victorian public sector (**VPS**) organisations implement the Standards and adhere to the requirements of the PDP Act. It employs a risk-based approach, seeking to enhance information security capability and maturity of VPS organisations, using an organisation's existing risk management principles and guidelines. The Framework and the Standards rely on protective data security principles to maintain the confidentiality, integrity, and availability of public sector information.

The Victorian Protective Data Security Standards

3. The Standards establish 12 high level requirements to protect public sector information. They deal with all security areas including governance, information, personnel, Information Communications Technology (**ICT**) and physical security.

4. In 2019, the Victorian Information Commissioner issued Version 2.0 of the Victorian Protective Data Security Standards. To assist organisations' adoption and implementation of the Standards, OVIC also released VPDSS Implementation Guidance,[3] a document which contains a list of elements, or security measures for each Standard, supporting good information security practices in an organisation.

5. OVIC expects organisations to assess the applicability of each VPDSS element to its risk treatment options. In this way, elements can assist an organisation to develop multiple levels of relevant, and interacting, mechanisms, or specific controls, to protect its information based on its internal and external context, the security value of information held, and other associated risks.

6. Standard 2 of the VPDSS ('Information Security Value') requires organisations to identify and assess the security value of public sector information. The VPDSS Implementation Guide contains nine elements that support Standard 2. Organisations' adoption of these elements, and implementation of supportive controls, helps mitigate risks to public sector information.

7. While organisations must demonstrate to OVIC that they are adhering to the Standards, they have autonomy in the selection and subsequent implementation of controls. The elements in the VPDSS Implementation Guidance support the intent of the Standard and demonstrate best practice.

[2] https://ovic.vic.gov.au/data-protection/framework-vpdsf/.

[3] https://ovic.vic.gov.au/data-protection/victorian-protective-data-security-standards-implementation-guidance/.

8. The VPDSS Implementation Guide lists the primary source each element is drawn from. Although OVIC encourages agencies to refer to the primary source when implementing each of the elements, agencies may also use an alternative source that has at least functional equivalence to the primary source.

Protective Data Security Plans submitted to OVIC in 2020

9. Under section 89 of the PDP Act, organisations are required to develop a Protective Data Security Plan (**PDSP**) and submit a copy to OVIC at least every two years, or upon significant change.[4]

10. Organisations were required to submit a completed PDSP by 31 August 2020 that covers security activities across 2018 – 2020 and any future planned activities. OVIC received 301 PDSPs, including multi-organisational and single organisational forms.[5]

11. Part A of the 2020 PDSP template included a requirement for organisations to complete an 'Organisational Profile Assessment' (**OPA**) which includes an indicative breakdown of the protective markings of information assets within the organisation.

12. Part B of the 2020 PDSP template requires organisations to nominate an implementation status for each element under the 12 Standards. The selections that organisations can use to communicate the status of implementation are shown in Table 1.

Table 1. Implementation status for elements

Status	Description
Not Applicable	The requirement is not applicable to the organisation
Not Commenced	[The organisation] has not yet defined or planned the work needed to meet the requirement. Alternatively, [the organisation has] started work but there are significant risks it cannot complete it.
Planned	[The organisation] has a program of work in place that includes work to meet the requirement; and the program is appropriately planned and resourced.
Partial	[The organisation] has delivered some of the aspects needed to meet the requirement. Remaining work is underway and progressing as planned.
Implemented	[The organisation] currently meet[s] the requirement of the element.

[4] For more information on what may constitutes a significant change refer to Information Sheet: Significant Change Notification Process available at https://ovic.vic.gov.au/data-protection/significant-change-and-protective-data-security-obligations/.

[5] There are more than 301 agencies in scope for the VPDSS, but organisations can submit a multi-organisation PDSP on behalf of one or more entities. This figure also excludes Class B Cemetery Trust PDSP submissions.

13. Once organisations have completed the ‘element assessment’ for each Standard, the PDSP form then prompts organisations to review and consider the combined or overall effectiveness of the controls implemented, and determine the organisation’s current, target and aspirational maturity level for each standard. The maturity levels are shown in Table 2.

Table 2. Maturity levels

Maturity level	Description
Informal	Processes are usually ad-hoc and undocumented. Some base practices may be performed within the organisation, however there is a lack of consistent planning and tracking. Most improvement activity occurs in reaction to incidents rather than proactively. Where practice is good it reflects the expertise and effort of individuals rather than institutional knowledge. There may be some confidence security-related activities are performed adequately, however this performance is variable and the loss of key staff may significantly impact capability and practice.
Basic	The importance of security is recognised, and key responsibilities are explicitly assigned to positions. At least a base set of protective security measures are planned and tracked. Activities are more repeatable and results more consistent compared to the ‘informal’ level, at least within individual business units. Policies are probably well documented, but processes and procedures may not be. Security risks and requirements are occasionally reviewed. Corrective action is usually taken when significant problems are found.
Core	Policies, processes, and standards are well defined and are actively and consistently followed across the organisation. Governance and management structures are in place. Risk assessment and management activities are regularly scheduled and completed. Historic performance information is periodically assessed and used to determine where improvements should be made.
Managed	Day-to-day activity adapts dynamically and automatically in response to situational changes. Quantitative performance measures are defined, baselined, and applied to ensure security performance is analysed objectively and can be accurately predicted in advance. In addition to meeting VPDSS requirements, the organisation also implements many optional ‘better practice’ requirements in response to its risk assessment.
Optimised	Security is a strategic issue for the organisation. Long-term planning is in place and integrated with business planning to predict and prepare for protective security challenges. Effective continuous process improvement is operating, supported by real-time, metrics-based, performance data. Mechanisms are also in place to encourage, develop and test innovations.

14. OVIC considered that each organisations' implementation status for the elements of Standard 2, the maturity assessment for Standard 2, and the breakdown of protective markings of information assets, was relevant to this audit.

15. OVIC's analysis of the submitted PDSPs found that across all the standards, Standard 2 had the lowest reported level of implementation across the whole of the Victorian government.[6] Consequently, OVIC chose four organisations that reported high implementation and maturity (core or higher) to assess the organisations alignment with Standard 2 and whether the organisations were making reasonable assessments.

16. In this audit, OVIC considered both the process, and extent, of the security capability of each organisation in relation to Standard 2.

Standard 2

17. Standard 2 – Information Security Value expects that*:*

> *An organisation identifies and assesses the security value of public sector information.*

18. The objective of Standard 2 is to:

> *Ensure an organisation uses consistent identification and assessment criteria for public sector information across its lifecycle to maintain its confidentiality, integrity, and availability*.

19. The identification and subsequent assessment of the 'security value' of an information asset are fundamental steps in establishing an effective information security program. An organisation cannot protect information it does not know it holds, nor can it understand information security risks if it does not have an appreciation of an information asset's value. The organisation needs to understand this value before investing time, effort, and resources in the application of particular security measures (or 'controls').

20. Under the VPDSS, 'security value' is expressed using BILs. An information security value assessment calls on organisations to consider equally the importance of maintaining the confidentiality, integrity, and availability of public sector information. BILs describe impacts which would be expected to cause harm or damage to government operations, organisations, or individuals, if there were a compromise of the confidentiality, integrity and/or availability of public sector information. The use of a standardised set of criteria (BILs) to assess the security value of public sector information helps promote a consistent approach to secure handling practices across an organisation, and secure information sharing across the VPS.

21. To help organisations understand the relationship of security value to the management of information security risks, OVIC has developed the Five Step Action Plan. The Five Step Action Plan sets out practical activities designed to assist in managing information security risks. Standard 2 corresponds with actions set out under Step 1 and Step 2 of OVIC's Five Step Action Plan, as shown in Figure 1.[7]

[6] This finding is based on the number of 'partial' and 'implemented' responses to the elements supporting Standard 2 compared to other standards.

[7] Guidance on the Five Step Action Plan is available on OVIC's website https://ovic.vic.gov.au/resource/the-five-step-action-plan/.

Figure 1. Five Step Action Plan

Five Step Action Plan				
01	02	03	04	05
Identify your information assets	Determine the **'value'** of this information	Identify any **risks** to this information	**Apply** security measures to protect the information	**Manage** risks across the information lifecycle

22. The nine elements supporting Standard 2 are shown in Table 3.

Table 3. Elements of Standard 2

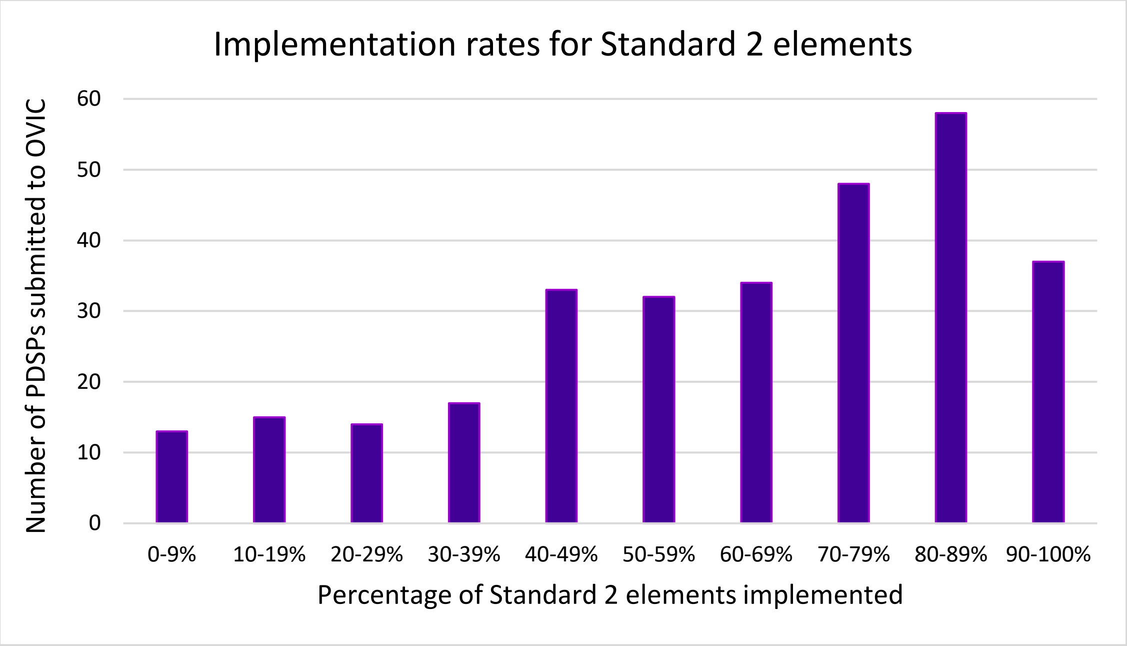
V2.0 #	Element
E2.010	The organisation's Information Management Framework incorporates all security areas.
E2.020	The organisation identifies, documents, and maintains its information assets in an information asset register (**IAR**) in consultation with its stakeholders.
E2.030	The organisation uses a contextualised VPDSF business impact level (**BIL**) table to assess the security value of public sector information.
E2.040	The organisation identifies and documents the security attributes (confidentiality, integrity, and availability business impact levels) of its information assets in its information asset register.
E2.050	The organisation applies appropriate protective markings to information throughout its lifecycle.
E2.060	The organisation manages the aggregated (combined) security value of public sector information.
E2.070	The organisation continually reviews the security value of public sector information across the information lifecycle.
E2.080	The organisation manages externally generated information in accordance with the originator's instructions.
E2.090	The organisation manages the secure disposal (archiving/destruction) of public sector information in accordance with its security value.

Application of Standard 2 across the Victorian public sector

23. OVIC looked at the implementation rate and maturity levels for Standard 2 as reported in the 301 PDSPs received from VPS organisations in 2020.

24. Figure 2 shows the percentage range of implementation scores allocated to VPS organisations, using the data contained in the 301 PDSPs OVIC received.[8] For example, 58 organisations received an implementation score that ranged from 80-89%.

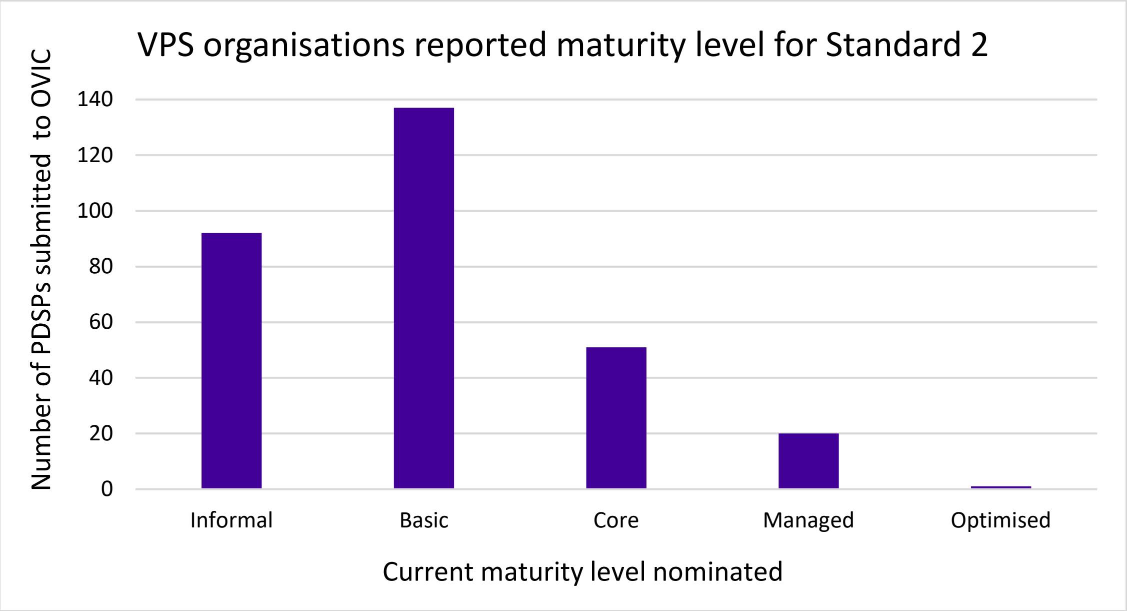
Figure 2. Implementation rates for Standard 2 elements



25. Figure 3 shows the 2020 maturity levels nominated by VPS organisations for Standard 2 in the 2020 PDSP submissions. The 2020 PDSP template requested organisations nominate a maturity level for 2020 (current), 2022 (target) and 2024 (aspirational).

[8] OVIC calculated the implementation rate by assigning a score to each implementation status (Implemented = 3, Partial = 2, Planned =1 and Not Commenced = 0). 'Not Applicable' elements were not counted. The percentage represents an organisation's 'implementation rate', which is calculated by adding up the total score and dividing the total score by the total potential score. The total potential score may be lower than 27 if organisations identified elements as 'Not Applicable'.

Figure 3. Reported maturity levels for Standard 2



Selection method for organisations to be audited

26. The Privacy and Data Protection Deputy Commissioner selected the organisations to be audited after considering the PDSPs submitted by Victorian public sector organisations in 2020. A list of organisations who submitted a PDSP in the 2020 reporting period was generated and filtered to reflect organisations that reported a *high* level of performance against Standard 2 (by considering the number of elements reported as Implemented or Partially Implemented, and a current reported maturity assessment of 'Core' or higher).

27. The four organisations involved in the audit were selected from this subset to form a sample of different sectors, sizes, structures, information held and organisational objectives. The following organisations were selected for inclusion in the audit:

Barwon Region Water Corporation

28. Barwon Region Water Corporation (**Barwon Water**) is Victoria's largest regional urban water corporation and operates as a statutory corporation under the *Victorian Water Act 1989*. Barwon Water provides water and sewerage services to about 320,000 residences and manages water supplies for the Greater Geelong region of Victoria. Barwon Water has the equivalent of approximately 300 full-time employees.[9]

CenITex

29. CenITex (**Cenitex**) provides ICT services and technology to the Victorian public sector. Cenitex groups its services into five categories:

    a. Identity;

    b. Security;

[9] Barwon Water's 2019-2020 annual report is available at https://www.barwonwater.vic.gov.au/__data/assets/pdf_file/0029/187409/Annual-Report-2019-2020.pdf.

c. Network;

d. User workspace; and

e. Cloud services.[10]

30. Cenitex is a State body under the *State-Owned Enterprises Act 1992*. Cenitex has the equivalent of approximately 500 full-time employees.[11]

The Victorian Institute of Forensic Medicine

31. The Victorian Institute of Forensic Medicine (**VIFM**) is Australia's largest multi-disciplinary centre for forensic medical and scientific services. VIFM has the equivalent of approximately 200 full-time employees.[12]

The Department of Treasury and Finance

32. The Department of Treasury and Finance (**DTF**) provides economic, financial and resource management advice to help the Victorian Government deliver its policies. As of June 2020, DTF had the equivalent of approximately 750 full-time employees.[13]

[10] https://www.cenitex.vic.gov.au/services.

[11] Cenitex's 2019-2020 annual report is available at https://www.cenitex.vic.gov.au/sites/default/files/2020-11/Cenitex%20Annual%20Report%202019-20.pdf.

[12] VIFM's 2019-2020 annual report is available at https://www.vifm.org/wp-content/uploads/VIFM-Annual-Report-2019-2020.pdf.

[13] DTF's 2019-2020 annual report is available at https://www.dtf.vic.gov.au/about-us/what-we-do.

OVIC’s audit of Standard 2 of the VPDSS

Objective of the audit

33. The objective of this audit was to assess the audited organisations’ application of Standard 2. This was assessed by examining the extent to which the organisations had implemented the elements of Standard 2, drawn from OVIC’s *VPDSS Implementation Guidance*.

How the audit was conducted

34. In December 2020, the Privacy and Data Protection Deputy Commissioner wrote to the heads of the four selected organisations to commence the audit and request information. The Deputy Commissioner asked the organisations to show how they identify and assess the security value of information they hold, with reference to the elements.

35. The audited organisations provided a response to OVIC’s request for information.

36. OVIC assessed the documentation provided to OVIC by the agencies, including the audited organisations IARs and policy and procedure documents.

37. Following OVIC’s review of the documentation provided by the organisations, OVIC staff conducted interviews with representatives identified by the audited organisations (typically information security or information management staff).

Limitations of the audit

38. OVIC reviewed documentation provided by the audited organisations and conducted interviews with personnel responsible for each organisation’s information security practices. OVIC did not examine how other staff at the organisations were implementing the security policies and procedures.

Audit findings

1. Do organisations have an Information Management Framework incorporating all security areas (VPDSS E2.010)?

Table 4. Assessment against VPDSS E2.020

Organisation	**Status Reported on 2020 PDSP**	**OVIC Assessment**
Barwon Region Water Corporation	Implemented	Agree, with qualifications Barwon Water's framework did not address personnel security.
CenITex	Partial	Agree
Victorian Institute of Forensic Medicine	Implemented	Disagree VIFM did not have a formalised information management framework.
Department of Treasury and Finance	Implemented	Agree, with qualifications DTF's framework did not cover all security areas.

E2.010 Explained

39. VPDSS E2.010 under Standard 2 states '*the organisation's Information Management Framework incorporates all security areas*.'

40. The objective of an information management framework (**IMF**) is to provide a high-level overview of the information management landscape of the organisation, articulating the shared direction and approach that the organisation intends to take, to securely govern its information assets (records, information, and data) throughout their lifecycle.

41. VPDSS E2.010 requires organisations to address all information security areas in its IMF.

42. The primary source for E2.010 is the whole of Victorian Government Information Management Framework (**WoVG IMF**).[14] The WoVG IMF provides a high-level view, and shared direction, for VPS agencies, and is intended to help agencies explore all components of an IMF, including linkages to supporting primary source references.

E2.010 Implementation

43. OVIC considers that organisations have implemented this element where they have developed an IMF that:

[14] https://www.vic.gov.au/information-management-whole-victorian-government.

a. articulates a shared direction and approach for securely governing the organisations' information assets throughout their lifecycle;

b. describes the information management landscape of the organisation;

c. describes internal governance arrangements;

d. incorporates information security, personnel security, ICT security and physical security;

e. is calibrated to address the unique information security risks of the organisation; and,

f. communicates the organisation's approach to information management (and, in turn, information security).

E2.010 Observations (Documentation Review and Interviews)

44. OVIC reviewed the documentation provided by the audited organisations to consider whether it met the requirements of E2.010. Each agency presented evidence that showed a consideration of the management of information, both in policy, practice, and supporting guidance. However, the audit was unable to identify alignment with the core components of the WoVG IMF.

45. Barwon Water provided an artefact that went some way to addressing the requirements of the E2.010 (outlined in paragraph 44 above). This document took the form of an Information Security Framework, which included some sections referencing information management.

46. Barwon Water's IMF did not explicitly address personnel security. Information security staff at Barwon Water explained that personnel security is handled by their Human Resources area. OVIC observed from the audit interviews that it is common for personnel security to be addressed by a separate area of an organisation and not necessarily included within an information security team's area of responsibility. However, by not including personnel security in overall information governance arrangements, organisations are at risk of failing to adequately identify and mitigate personnel security risks to their information.

47. DTF provided an information security management framework, and information security policy as the governance framework for information at DTF. DTF has advised it intends to develop an IMF.

48. Cenitex and VIFM both provided information security and information management policies and procedures in response to this element. However, OVIC did not observe any document that cohesively describes, at a high-level, the information management landscape of the organisation. This included any legislative, regulatory, and administrative drivers, to articulate a shared direction and approach for the organisation to securely govern information assets (records, information, and data) throughout their lifecycle.

49. Cenitex provided a records management policy and draft guidelines around handling security classified information. While both documents contain statements about some aspects of information management, they were not framework documents.

50. In interviews, organisations noted they followed the WoVG IMF. The WoVG IMF is the primary resource that provides 'a structural view of the government's existing and desired

information management environment,'[15] but it does not replace the need for a detailed, contextualised framework for the organisation. Organisations can look to the WoVG IMF for guidance, but an organisation-specific IMF must be developed that articulates the specific strategic information management direction for the respective organisation while considering the objectives outlined in paragraph 43 above.

51. Overall, OVIC observed that the materials provided by all the audited organisations did not provide adequate reference to the application of controls based on the security value of the information. Standard 2 calls for all Victorian Government agencies to develop and maintain an IMF. In respect of this audit, each of the four agencies showed gaps in their approach to, and self-assessment of, the expectations and intent of the element.

E2.010 Findings

52. Each organisation was able to refer to other documents which showed – to varying degrees – how they managed information within their agency, including communicating some requirements for handling information to staff.

53. Barwon Water had an Information Security Framework document.

54. While it had the most mature framework of any of the four agencies, OVIC found that Barwon Water's documentation did not:

    a. Reference scalable security controls, proportionate to the security value of the information; and

    b. Incorporate all security areas. As noted in Paragraph 46, Barwon Water's framework did not address personnel security.[16]

55. DTF also provided an Information Security Management Framework, and information security policy. It also provided an information and records management policy. Although it did not have a document called an 'Information Management Framework', OVIC considered that these other policies and procedures partially met the requirements of the element. However, they did not address all security areas explicitly.

56. Each agency should consider the following points to help support and strengthen the development and maintenance of their information management framework, policies, and processes.

    a. The currency of the content (i.e., checking for superseded material, or outdated references within and between documents / resources);

    b. There is proper version control;

    c. The material is appropriately authorised;

    d. There is clear accountability and responsibility, by clearly defining and assigning roles and responsibilities;

[15] https://www.vic.gov.au/information-management-whole-victorian-government

[16] Standard 10 – Personnel Security: 'An organisation establishes, implements and maintains personnel security controls addressing all persons continuing eligibility and suitability to access public sector information.'

e. There are clear linkages both within, and between, the documentation;

f. Key terms are defined upfront, and used consistently throughout all material (for example, 'Security classified', 'Protective marking', and 'Security value');

g. The scope and application of the material is clear;

h. The extent and coverage of the material addresses the maintenance of the confidentiality, integrity, and availability of all forms of public sector information (inc. hard copy, soft copy and verbal disclosures);

i. Any gaps, anomalies and discrepancies are identified and rectified; and

j. Any new policies or procedures need to be developed by considering the organisation's risks and legislative obligations.

E2.010 Recommendations

Recommendation 1 – Barwon Water, Cenitex, VIFM, and DTF to develop an Information Management Framework

57. OVIC recommends that Barwon Water, Cenitex, VIFM, and DTF complete an Information Management Framework (or other policy and procedural documents that serve the same purpose) that incorporates and addresses all security areas.

2. Do organisations identify, document, and maintain Information Asset Registers in consultation with their stakeholders (VPDSS E2.020)?

Table 5. Assessment against VPDSS E2.020

Organisation	**Status Reported on 2020 PDSP**	**OVIC Assessment**
Barwon Region Water Corporation	Implemented	Agree, with qualifications Barwon Water did not consider consulting external stakeholders in developing its IAR.
CenITex	Partial	Agree
Victorian Institute of Forensic Medicine	Partial	Agree
Department of Treasury and Finance	Implemented	Agree, with qualifications DTF did not consider consulting external stakeholders in developing its IAR.

E2.020 Explained

58. VPDSS E2.020 under Standard 2 states '*The organisation identifies, documents and maintains its information assets in an information asset register (**IAR**) in consultation with its stakeholders.'*

59. The objective of this element is to ensure appropriate governance is being given to the protection of public sector information, through central oversight and management of the organisations information holdings.

60. The primary source for E2.020 is OVIC's *Practitioner Guide: Identifying and Managing Information Assets*.[17]

E2.020 Implementation

61. OVIC considers that organisations have implemented this element where they have:

    a. Identified the organisation's information assets;[18]

[17] https://ovic.vic.gov.au/data-protection/practitioner-guide-identifying-and-managing-information-assets/

[18] An information asset is described as a body of information, defined and practically managed so it can be understood, shared, protected, and used to its full potential. Information assets support business processes and are stored across a variety of media and formats (i.e., both papers as well as electronic material).

b. Documented its information assets in an IAR;

c. Actively maintained the IAR; and,

d. Consulted with the organisation's stakeholders throughout this process.[19]

62. To maintain an IAR, organisations should consult with their stakeholders – both internal and, where applicable, external – to validate and verify the currency of the content within the register. At a minimum, organisations should populate any new assets, or re-validate or retire existing entries in accordance with the *VPDSF Requirements* tab of the *Sample IAR template*.[20]

63. If an organisation is using an alternative tool or system to register their information assets, they are encouraged to cross reference the fields on the *Sample IAR template*, as well as consider updating or enhancing existing registers/systems, ensuring all relevant security attributes are captured for each information asset.

64. IARs should be reviewed frequently (at least once a year).[21] Reviews should consider all information assets and include a review of both the content within the IAR as well as the currency of the IAR fields.[22] For IAR reviews to be most effective, they should include a comprehensive review of the security value of the information assets documented in the IAR, as this can change over the lifecycle of the information. Due care must be given to verifying BIL ratings for confidentiality assessments and corresponding protective markings.

E2.020 Observations (Documentation Review and Interviews)

E2.020 Identifying Information Assets

65. DTF, Cenitex and Barwon Water had each developed an IAR.

E2.020 Documenting Assets in an IAR

66. The appropriate number of assets in an organisation's IAR will depend on multiple factors, such as the size of the organisation and the information it holds.

67. Barwon Water, DTF and Cenitex reported having completed the initial work of documenting their information assets in an IAR. These organisations reported structuring their information assets into groups that broadly reflect the business areas across the organisation (for example, Human Resources information assets, Corporate/Financial/Technology information assets).

68. In the audit interviews, Barwon Water's information security staff reported that they had achieved an ideal balance in the level of specificity of the information assets documented in

Information assets have a recognisable and manageable value, risk, content, and lifecycle. An information asset can be a specific report, a collection of reports, a database, information contained in a database, information about a specific function, subject or process. https://ovic.vic.gov.au/data-protection/practitioner-guide-assessing-the-security-value-of-public-sector-information-v2-0/?highlight=practitioner%20guide.

[19] Stakeholders can include internal and external personnel or entities.

[20] *Sample IAR template* can be found here https://ovic.vic.gov.au/data-protection/sample-information-asset-register-template-v2-0/

[21] Section 12 of the *OVIC Practitioner Guide: Identifying and Managing Information Assets,* available at https://ovic.vic.gov.au/resource/practitioner-guide-identifying-and-managing-information-assets-v2-0/.

[22] As above.

the IAR, meaning that the assets identified are not too broad or too narrow. For Barwon Water this makes the IAR easier to use and more effective.

69. In the documentation review, OVIC observed DTF had invested upfront effort in establishing a detailed IAR, with over 400 information assets centrally registered. The register records departmental information assets, as well as capturing several subsidiary entities' information assets.

70. As of February 2021, VIFM was developing its IAR, with a list of its information assets recorded in the register. The VIFM team was working to identify the security value of those registered assets using the Business Impact Levels (**BILs**). These activities and ongoing work effort, align with the selection of a '*Partial'* implementation status as reported on VIFM's 2020 PDSP.

E2.020 Use of an IAR

71. OVIC observed that organisations were not using the security value assessment consistently to inform the controls needed to protect the information. This was demonstrated through the audit of organisation's policies and procedures, which often failed to focus or emphasise the security value assessment as a foundational activity in the development of their broader organisational approach to information security.

E2.020 Maintenance of an IAR

72. OVIC reviewed DTF, Barwon Water and Cenitex's procedures for maintaining their IARs. Each of the audited organisations' maintenance procedures set out timeframes for the review of its IAR. In summary:

    a. DTF procedure said that its IAR is reviewed biennially, or when a significant change occurs (such as a 'Machinery of Government' change);

    b. Barwon Water's procedure said that the organisation will review its information assets on a regular basis. The procedure also stated that new information assets will be created and documented in the IAR as required; and,

    c. Cenitex's documentation said that an information review must be conducted, in consultation with internal stakeholders, at least once a year to identify, validate and update information assets created and used at Cenitex to conduct business that have a BIL of 2 or more.

E2.020 In consultation with stakeholders

73. Each of the four audited organisations reported that they developed, or are in the process of developing, their IARs in consultation with their internal stakeholders. The four audited organisations described to OVIC a process for stakeholder consultation that involved staff responsible for maintaining the central/master IAR, meeting with the information asset owners/directors across various business areas. During the meetings, the agencies described a process of verbally briefing internal stakeholders on the purpose of the IAR, the process of identifying information assets, and the way to assess the security value of those assets.

74. None of the audited organisations referenced consultation with external stakeholders.

E2.020 Findings

75. Barwon Water, DTF, and Cenitex demonstrated that they identify and document their information assets in an IAR in consultation with internal stakeholders.

76. Cenitex had not, at the time the IAR was provided, adequately maintained it in line with internal policy or the *OVIC Practitioner Guide: Identifying and Maintaining Information Assets*, and their *partial* rating aligns with this finding.

77. No agency consulted with external stakeholders.

78. As VIFM was developing its IAR at the time of the audit it has partially implemented this element, as indicated in its 2020 PDSP.

E2.020 Recommendations

Recommendation 2 – Barwon Water, Cenitex, VIFM and DTF review, validate and update the IAR at least annually

79. OVIC recommends that Barwon Water, Cenitex, DTF and VIFM should review, validate, and update as necessary, their IARs at least once a year.

Recommendation 3 – Barwon Water, Cenitex, VIFM and DTF consult External Stakeholders

80. OVIC recommends that Barwon Water, Cenitex, VIFM, and DTF should consult with relevant or affected stakeholders, including external stakeholders where applicable, (for example, custodians, information sharing partners, third parties, contracted service providers) when identifying and documenting information assets and maintaining the organisation's the IAR.

Recommendation 4 – Barwon Water, Cenitex, VIFM and DTF integrate the IAR into business processes

81. OVIC recommends that Barwon Water, Cenitex, VIFM, and DTF should examine how the organisation uses the IAR, through integrating security value assessments into standard business processes, using the IAR to inform risk assessments and the subsequent selection of security controls, to further protect their information assets and information systems.

3. Do organisations use a contextualised Business Impact Level table (VPDSS E2.030)?

Table 6. Assessment against VPDSS E2.030

Organisation	**Status Reported on 2020 PDSP**	**OVIC Assessment**
Barwon Region Water Corporation	Implemented	Agree
CenITex	Implemented	Agree
Victorian Institute of Forensic Medicine	Partial	Agree
Department of Treasury and Finance	Implemented	Disagree DTF does not have a BIL table contextualised to its circumstances.

E2.030 Explained

82. VPDSS E2.030 under Standard 2 states that '*The organisation uses a contextualised VPDSF business impact level (**BIL**) table to assess the security value of public sector information*.'

83. E2.030 refers to core security concepts that have distinctive meanings behind them. To help understand the intent of this element, each concept has been briefly set out below:

    a. *Business Impact Level* (**BIL**) - Scaled impacts (with an associated rating/level) which describe the harm or damage to government operations, organisations, or individuals, if there were a compromise to the confidentiality, integrity and/or availability of public sector information.

    b. *Contextualised BIL table* - A version of the VPDSF BIL table, where impact statements (consequences) have been tailored by an organisation to reflect operational impacts on that organisation.

    c. *Security value assessment* - A method to assess public sector information to determine the overall security value. The assessment process involves the originator[23] of the information:

        i. considering the content (and context) of the information;

        ii. assessing potential impacts (using the BILs) of a compromise of the confidentiality, integrity and/or availability of the information; and

[23] 'The person, or organisation, responsible for preparing/creating public sector information or for actioning information generated outside the public sector (i.e., private industry). This person, or organisation, is also responsible for deciding whether, and at what level, to value/protectively mark that public sector information.' This definition is included in the VPDSS Glossary V2.0 - https://ovic.vic.gov.au/data-protection/victorian-protective-data-security-standards-glossary/.

iii. applying proportionate security measures to protect the information.

d. *Security Value* – The outcome of a security value assessment, expressed in a quantitative form (BIL of 1, BIL of 2, or BIL of 3, etc.), for the confidentiality, integrity, and/or availability of public sector information.

84. As operational impacts may vary greatly from organisation to organisation, the objective of a contextualised BIL table is to assist different personnel within an organisation in assessing the security value of information (for example, documents, emails) accurately, consistently, and efficiently.

85. Contextualising an organisation's BIL table means to modify the statements around potential impact levels to align with the organisation's specific operating requirements and environment. In other words, the contextualised statements should be based on potential operational impacts that are reasonable and proportionate to the organisation's risk posture.

86. Organisations only need to develop contextualised impact statements for the impact categories that are relevant to them. Where sample impacts are presented in the VPDSF BIL table (for example, an organisation's operating budget), organisations should reflect on their own operating context and interchange that standardised impact descriptions with a reference that suitably describes the actual impact and implication to their business. Not all impact statements presented in the VPDSF BIL table will require this contextualisation, but some will. Some impact statements may be the same across multiple Business Impact Levels (for example, personal harm). In which case, organisations should consider scaling the severity of the impact in question.

87. The primary source for E2.030 is OVIC's *Practitioner Guide: Assessing the security value of public sector information*.[24] Appendix B points organisations to the VPDSF BIL table. The most recent release of this table (V2.1) was published in November 2019.

E2.030 Implementation

88. OVIC considers that organisations have implemented this element where they have:

a. A contextualised BIL table in line with the organisation's specific operating requirements; and

b. Are using this BIL table to assess the security value of public sector information.

E2.030 Observations (Documentation Review and Interviews)

E2.030 Contextualised BIL tables

89. Barwon Water and Cenitex provided a copy of their contextualised BIL tables to OVIC.

90. Barwon Water's contextualised BIL table contained statements that set clear parameters around each BIL level and clearly described what the BIL level means within Barwon Water's organisational context. The statements also retained the same meaning and high-level indicators identified in the VPDSF BIL table.

[24] The *OVIC Practitioner Guide: Assessing the security value of public sector information* can be found at https://ovic.vic.gov.au/data-protection/practitioner-guide-assessing-the-security-value-of-public-sector-information-v2-0/

91. Cenitex's contextualised BIL table contains high-level statements across the BIL levels.

92. VIFM said it will be developing a contextualised BIL table as one of their next steps following identification of their information assets, to support their information security value assessments.

93. DTF did not have a contextualised BIL table. In OVIC's interview with DTF, DTF explained that when discussions are had with staff about information security value, context is provided about DTF's legal obligations and reputation to help information asset owners assign BIL values. By doing so DTF guides the users through contextualising the BIL table verbally.

E2.030 How contextualised BIL tables are used to perform BIL assessments

94. Barwon Water and Cenitex use their BIL table by presenting it to information asset owners to assist them to select an appropriate BIL for the assets they are responsible for. A range of BIL levels are reviewed and explained to support the information asset owner to select the appropriate BIL level.

95. Contextualised BIL tables assist organisations to perform consistent BIL assessments across the different business areas of an organisation. OVIC observed from the audit interviews that Barwon Water and Cenitex staff consider that use of their BIL tables supports consistent assessments. However, OVIC observed that neither organisation has a process where information security staff review or moderate outcomes of the BIL assessments carried out by information asset owners to ensure that assessments are consistent across the organisation (for example, where the person or team responsible for their organisation's IAR reviews assessments to make sure that an area of the organisation has not over, or under, represented the security value of its information assets).

E2.030 Findings

96. Barwon Water and Cenitex have developed, and during the interviews advised that they use, a contextualised BIL table to assess the security value of public sector information.

97. VIFM and DTF did not have a contextualised BIL table at the time of the audit. DTF advised that they used the OVIC BIL assessment app to assist staff to assess the security value of public sector information.[25] The BIL app is intended to assist with the process of assessing information assets and it is by no means developed for the 'context' of the user. Organisations are still expected to have organisational-specific indicators for the types and severity of impacts that align with the VPDSF BIL table.

E2.030 Recommendations

Recommendation 5 – VIFM and DTF develop and use a contextualised BIL table

98. OVIC recommends VIFM and DTF develop a contextualised BIL table.

[25] Response by DTF to the draft report – correspondence received by OVIC on 23 July 2021.

4. Do organisations identify and document the security attributes of an information asset (VPDSS E2.040)?

Table 7. Assessment against VPDSS E2.040

Organisation	Status Reported on 2020 PDSP	OVIC Assessment
Barwon Region Water Corporation	Implemented	Agree
CenITex	Implemented	Agree
Victorian Institute of Forensic Medicine	Partial	Agree
Department of Treasury and Finance	Implemented	Agree

E2.040 Explained

99. VPDSS E2.040 under Standard 2 states that *'The organisation identifies and documents the security attributes (confidentiality, integrity and availability business impact levels) of its information assets in its information asset register.'*

100. The objective of E2.040 is for organisations to understand the security value of their information holdings (as recorded in their IARs), to manage information security risks in a proportionate manner.

101. The primary source for E2.040 is OVIC's *Practitioner Guide: Assessing the security value of public sector information*.

E2.040 Implementation

102. OVIC considers that organisations have implemented this element where they have:

    a. Identified the security attributes of its information assets; and

    b. Documented a BIL rating for each of the security attributes (Confidentiality, Integrity, and Availability) of an information asset in the organisation's IAR.

103. To achieve this, an organisation needs to consider the potential impacts if there was a compromise of the Confidentiality, Integrity, and Availability**,** of public sector information.

104. The *VPDSF Requirements tab* of the *Sample IAR template*[26] includes fields to document the security value (BIL rating) associated with each of the security attributes of an information asset. These security values are expressed in the form of BIL ratings. For example, an information asset may be assessed as having a BIL of 2 for Confidentiality, a BIL of 2 for Integrity, and a BIL of 3 for Availability.

[26] *Sample IAR template* can be found here https://ovic.vic.gov.au/data-protection/sample-information-asset-register-template-v2-0/

105. The outcome of the Confidentiality assessment directly corresponds with a protective marking(s).

106. The outcome of the Integrity and Availability assessments helps to identify whether additional security measures are required (beyond those established by the protective marking) to further protect the information.

107. Once all three security attributes (C, I, A) BIL ratings have been identified, the organisation is able to determine the overall 'security value' of the information. The overall security value is based on the highest of the three BIL ratings, for the C, I, and/or A assessments.

108. Under E2.040, organisations are expected to use their contextualised VPDSF BIL table to conduct these security value (BIL) assessments.

E2.040 Observations (Documentation Review and Interviews)

109. DTF, Barwon Water and Cenitex all had documented BIL ratings for the Confidentiality, Integrity, and Availability attributes of their information assets in their IARs. Although as previously identified, DTF did not have a contextualised BIL table to use to support the accurate identification of security attributes for its information assets.

110. VIFM had not yet documented BIL ratings for the Confidentiality, Integrity, and Availability attributes of the information assets in its IAR but was carrying out that exercise at the time of the audit interviews in March 2021.

111. As raised earlier in this report in paragraph 83, OVIC observed in DTF's IAR that the BIL ratings for some of the Confidentiality assessments did not correspond with the appropriate protective marking for information assets.

E2.040 Findings

112. Cenitex, DTF and Barwon Water demonstrated that they have identified and documented the security attributes of information assets.

113. VIFM confirmed that it intends to identify and document the security attributes of information assets as it develops its IAR. The IAR VIFM provided included some documented Confidentiality BIL ratings, with Integrity and Availability BIL ratings yet to be documented in VIFM's IAR at the time of this audit.

E2.040 Recommendations

Recommendation 6 – VIFM and DTF use contextualised BIL table to identify security attributes

114. OVIC recommends that VIFM and DTF should use a contextualised BIL table to assess the information assets documented in the organisation's IAR.

Recommendation 7 – DTF review the organisation's IAR for inconsistent BIL ratings and protective markings

115. DTF should review the organisation's IAR for any inconsistencies in the BIL ratings for confidentiality assessments and the documented protective marking assigned to information assets. Where necessary, DTF should reassess the security attributes (and protective marking assigned) to information assets.

5. Do organisations apply appropriate protective markings to information throughout the information lifecycle (VPDSS E2.050)?

Table 8. Assessment against VPDSS E2.050

Organisation	**Status Reported on 2020 PDSP**	**OVIC Assessment**
Barwon Region Water Corporation	Implemented	Disagree Barwon Water does not currently apply protective markings to its documents.
CenITex	Partial	Agree
Victorian Institute of Forensic Medicine	Partial	Agree
Department of Treasury and Finance	Implemented	Agree, with qualifications OVIC observed inconsistent use of protective marking terminology.

E2.050 Explained

116. VPDSS E2.050 under Standard 2 states '*The organisation applies appropriate protective markings to information throughout its lifecycle.*'

117. The objective of E2.050 is for organisations to use protective markings to communicate the confidentiality requirements of public sector information in a standardised manner. Where there are changing confidentiality requirements for the information across its lifecycle, protective markings should be reviewed and updated to ensure proportionate security measures can be applied.

118. Protective markings are security labels assigned to information. They inform the minimum level of protection needed to maintain the confidentiality requirements of the information throughout its lifecycle (for example, from the point that information is initially captured, collected, or recorded, through to when it is no longer needed and can be archived or destroyed).

119. The primary source of E2.050 is OVIC's *Practitioner Guide: Protective Markings*[27] and the *PSPF INFOSEC-8 Sensitive and Classified Information.*

[27] The *OVIC Practitioner Guide: Protective Markings* can be found at https://ovic.vic.gov.au/data-protection/practitioner-guide-protective-markings/

E2.050 Implementation

120. OVIC considers that organisations have implemented this element where they can demonstrate they:

    a. Apply appropriate protective markings; and

    b. Manage these markings across the information lifecycle, by periodically reviewing protective markings for currency and updating it if required.

E2.050 Observations (Documentation Review and Interviews)

121. OVIC reviewed the documentation provided by the audited organisations for E2.050, drawing out some high-level observations. These included:

    a. Different organisations appear to be at varying stages of their implementation of protective markings across all areas of business; and

    b. Some organisations reported delays in this implementation, due to difficulties in sourcing technical solutions to apply this element.

122. Whilst technical solutions can assist staff apply a protective marking to a document, email, or record, they cannot ensure the appropriate marking is applied. In addition, technical solutions do not ensure that the appropriate protective marking is applied throughout the information lifecycle**.** Staff must receive appropriate training and support to assist them to both assess and apply the appropriate protective marking to information.

123. Cenitex and DTF reported to have transitioned to the new protective markings scheme and require staff to apply protective markings to information. Both organisations provided documented guidance for staff on how to apply an appropriate protective marking to internally generated information, such as documents and emails.

124. DTF advised that it uses technical controls to assist staff, by prompting them to apply protective markings to emails before they are sent. DTF's document storage system also requires users to select a protective marking for all records.

125. DTF has produced training and awareness material to assist its users in understanding and applying protective markings, issuing a guideline that contains descriptions of the markings and Information Management Markers (**IMMs**). With changes to the protective marking schema in late 2019, some superseded references were identified that should be updated to fully benefit user training and awareness.[28]

126. Cenitex provided a draft document outlining security classification and handling requirements for its information. It detailed each protective marking with the corresponding BIL level (for example, BIL of 2 corresponds to a protective marking of OFFICIAL: Sensitive) to provide guidance to users.

127. Barwon Water and VIFM personnel are not currently applying protective markings to information (such as documents and emails), but both organisations outlined their plans to require staff to apply appropriate protective markings to the information they generate in future.

[28] For more information about the VPDSF protective marking scheme introduced in 2019 visit https://ovic.vic.gov.au/resource/practitioner-guide-protective-markings-v2-0/.

128. Barwon Water provided details of a project to select appropriate tools to assist in the roll out of the protective markings scheme to the wider organisation.

129. VIFM has tools available to apply protective markings to information but first needs to train its personnel in how to apply the appropriate protective marking. In the interim, while VIFM is planning to introduce a requirement on its staff to apply protective markings, it explained that it currently has information handling checklists relevant to different business areas. VIFM also has other processes of labelling documents to indicate the sensitivity of information and restrictions around the information's use. However, information may not be handled consistently, based on information security value, across the organisation, or with third parties.

130. Barwon Water considered that it had implemented this element because it assigns protective markings at a high-level to the information assets contained in its IAR. Whilst E2.040 requires this of organisations (i.e., document security attributes, including corresponding protective markings, in the IAR), it is also a requirement to apply protective markings to public sector information across its lifecycle.

131. Information assets may contain multiple items of information (such as emails, electronic and physical documents). The protective marking that is applied to an information asset should reflect the outcome of a confidentiality BIL assessment carried out by considering the impact if all the information in the asset was disclosed. The pieces of information that make up the information asset should be assessed individually and marked with an appropriate protective marking to communicate to others the confidentiality requirements of that information.

132. Barwon Water explained to OVIC in the audit interviews that they ensure staff handle (non-protectively marked) information according to the information's confidentiality requirements as set out in the Barwon Water's IAR. Barwon Water staff explained in the audit interviews that they require information asset owners to communicate to other staff the handling requirements of information. When handling requirements have not been communicated, the recipient is expected to contact the information asset owner to find out the information handling requirements.

133. Barwon Water do not have information handling guides but did have a procedure for sharing information outside of Barwon Water. The procedure requires users to view the protective marking of the information recorded in the IAR and contact the Information Custodian. However, if the organisation does not have a reference for what handling requirements should accompany certain information, then a protective marking will not have meaning to staff.

E2.050 Findings

134. Barwon Water documents a protective marking to its information assets in the IAR but does not apply protective markings to individual pieces of information (such as documents, emails) that are generated and handled internally (such as by staff members).

135. VIFM does not yet apply protective markings in line with the Victorian protective marking scheme to information that is generated and handled internally. VIFM described other labelling requirements placed on VIFM through alternative policies, agreements, and legislation that are used to communicate the nature of the information and handling requirements in specific circumstances.

136. DTF and Cenitex staff apply protective markings to information assets. Both organisations provided documented guidance that explain to staff how to select an appropriate protective marking.

E2.050 Recommendations

Recommendation 8 – Barwon Water and VIFM develop and implement the ability to protectively mark information

137. OVIC recommends that Barwon Water and VIFM continue to develop and implement the capacity to apply appropriate protective markings to information received, handled, stored, or disseminated by the agency.

Recommendation 9 – Barwon Water to develop and implement information handling checklists

138. OVIC recommends that Barwon Water develop and implement information handling checklists for personnel to refer to when handling protectively marked information. The checklists should include instructions that:

a. Address the secure management of information assessed as OFFICIAL, OFFICIAL: Sensitive, PROTECTED and SECRET (where relevant).

b. Cover all security areas (information, personnel, ICT, and physical security controls); and

c. Cover the full information lifecycle (cradle to grave).

6. Do organisations manage the aggregated security value of information (VPDSS E2.060)?

Table 9. Assessment against VPDSS E2.060

Organisation	**Status Reported on 2020 PDSP**	**OVIC Assessment**
Barwon Region Water Corporation	Implemented	Agree, with qualifications Evidence of management of aggregated security value in IAR, but other security policies and procedures did not refer to this concept.
CenITex	Partial	Agree
Victorian Institute of Forensic Medicine	Planned	Agree
Department of Treasury and Finance	Implemented	Agree

E2.060 Explained

139. VPDSS E2.060 under Standard 2 states ‘*The organisation manages the aggregated (combined) security value of public sector information.*’

140. The objective of E2.060 is for organisations to ensure the combined security value of public sector information is appropriately managed and maintained.

141. Where multiple pieces of public sector information are stored together, the overall security value of this combined material needs to be considered. Risks associated with these combined pieces of information may be higher than any single instance or individual record. This is because the collated information reveals new and more sensitive information or intelligence than would be apparent from the main source records and would cause greater damage than individual documents. When viewed separately, the components of the information compilation retain their individual classifications.

142. Additional security measures may be needed to protect these combined (aggregated) information assets. This is particularly important when selecting types of equipment, systems, facilities, or services needed to protect this information, as extra security controls may be required.

143. The primary source for E2.060 is OVIC's *Practitioner Guide: Assessing the security value of public sector information*.[29]

E2.060 Implementation

144. OVIC considers that organisations have implemented this element where they:

a. Are using the contextualised BIL table to assess the security value of public sector information; and

b. Manage the combined (aggregate) security value of public sector information.

E2.060 Observations (Documentation Review and Interviews)

145. All the audited organisations reported structuring their information assets in their IARs into groups that broadly reflect the business areas across the organisation (for example, Human Resources information assets, Corporate/Financial/Technology information assets). As such, the information assets in their IAR's represented a high-level information asset, generally made up of multiple pieces of information/records combined under one broad asset title. Given the broad nature of the information asset entries in their IARs, the audited organisations were observed to be assessing and recording the aggregated security value of these assets.

146. Documentation provided by DTF and Cenitex referenced the concept of aggregated value, and broadly outlined how and why the concept was important to that agencies' information holdings, and corresponding security value

147. DTF's guidance includes statements about what aggregate value means and referred to the potential of heightened risks relating to the collection of information. The guidance material also contained high level commentary that additional security controls may be needed to protect the combined information assets, with consideration to be given to equipment, systems, facilities, or services for the protection of the aggregated information.

148. Cenitex's draft document outlining security classification and handling requirements contained an excerpt of OVIC guidance that explains the meaning of aggregated security value.

149. Neither VIFM nor Barwon Water's documentation contained reference to the management of the combined (aggregate) security value of public sector information.

150. No agency provided in-depth guidance or policies that showed or explained different ways in which staff should manage information in accordance with the information's aggregated security value.

E2.060 Findings

151. OVIC found that the organisations that have developed their IARs (Cenitex, DTF and Barwon Water) show that they have assigned and documented the aggregated security value of its information assets in their IARs.

[29] The *OVIC Practitioner Guide: Assessing the security value of public sector information* can be found at https://ovic.vic.gov.au/data-protection/practitioner-guide-assessing-the-security-value-of-public-sector-information-v2-0/

152. Outside of the aggregated value attributed within the IAR, the documentation provided by VIFM and Barwon Water had no reference to the combined, or aggregate, security value of information, or how this was to be managed within the organisation.

153. No agency had in-depth documentation or process relating to the management of aggregated information.

E2.060 Recommendations

154. To properly manage the aggregated security value of public sector information, OVIC recommends that:

Recommendation 10 – Barwon Water and VIFM to embed aggregated security value management into existing or new policies or procedures.

155. Both Barwon Water and VIFM should strengthen their existing documentation by referencing how the agency considers and manages the combined (aggregate) security value of public sector information.

Recommendation 11 –Barwon Water, Cenitex and VIFM strengthen the management and understanding of aggregated information assets.

156. OVIC recommends that Barwon Water, Cenitex and VIFM develop policy and procedures to support staff to:

   a. Understand and handle aggregated information assets, and the corresponding combined security value; and

   b. Implement security measures to actively manage the information, according to its aggregated security value.

7. Do organisations continually review the security value of information across the information lifecycle (VPDSS E2.070)?

Table 10. Assessment against VPDSS E2.070

Organisation	**Status Reported on 2020 PDSP**	**OVIC Assessment**
Barwon Region Water Corporation	Implemented	Disagree Did not observe evidence that Barwon Water is reviewing security value across the information lifecycle.
CenITex	Partial	Agree
Victorian Institute of Forensic Medicine	Planned	Agree
Department of Treasury and Finance	Implemented	Disagree Did not observe evidence that DTF is reviewing security value across the information lifecycle.

E2.070 Explained

157. Element E2.070 of Standard 2 is '*The organisation continually reviews the security value of public sector information across the information lifecycle.*'

158. The objective of this element is to ensure organisations understand the potential for security value to change over time, and to ensure the appropriate protections are applied to the information at different points across its lifecycle.

159. Information lifecycle describes the sequence of changes from creation until disposal. It includes, but is not limited to:

a. The initial drafting process;

b. Capture, collection, recording, or acquisition;

c. Use, handling, and management of information under changing contexts;

d. Updates to, or adjustments of content; and

e. Disposal (either archive or destructions) when it is no longer being actively used.

160. The security measures that need to accompany the material throughout its lifecycle will be influenced by its security value.

161. For example, at the drafting stage of a document there may be limited content in a document. As the document moves through various iterations the sensitivity of the content may change, as additional content is added or removed. The context in which the document was being created, and its intended use, may also have changed. Each of these factors needs to be considered when assessing what the current security value of the document is. There may be increased confidentiality concerns with the material, or the integrity and availability of the material become more or less important.

162. As illustrated in this example, organisations need to remain mindful of, and continually review the security value of public sector information across its lifecycle. There will be scenarios where more stringent controls may be needed to protect information, and other times when these controls can be paired back.

163. The primary source for E2.070 is the *OVIC Practitioner Guide: Assessing the security value of public sector information* and supplementary VPDSF BIL Table.[30]

E2.070 Implementation

164. OVIC considers that organisations have implemented this element where their personnel actively review the security value of public sector information across its lifecycle (from cradle to grave) and adjusts security measures to manage these changing requirements.

E2.070 Observations (Documentation Review and Interviews)

165. The audited organisations did not provide any documents that outlined the need for continual review of the security value of information across the information lifecycle, or any procedural documentation to assist staff to do so.

166. OVIC observed that there was a strong association of the term 'information lifecycle' with records and information management. Whilst retention and disposal schemes are an important business consideration, and assist in the management of public sector information, under the VPDSS information lifecycle refers to how the form and content of a document can change over time (throughout the lifecycle). Any change may increase or decrease the sensitivity of the material.

E2.070 Findings

167. All audited organisations provided examples of some situations where the security value of information was assessed at a stage during the information lifecycle.

168. OVIC did not see evidence that that the audited organisations are continually reviewing the security value of information across the information lifecycle. This finding also ties in with organisations not effectively protectively marking information through its lifecycle.

[30] The *OVIC Practitioner Guide: Assessing the security value of public sector information* can be found at https://ovic.vic.gov.au/data-protection/practitioner-guide-assessing-the-security-value-of-public-sector-information-v2-0/

E2.070 Recommendations

Recommendation 12 – Barwon Water, Cenitex, VIFM and DTF develop comprehensive documentation (policies and processes), or strengthen existing policy or process, to support and promote the continual review of public sector information across the information lifecycle.

194. OVIC recommends that all audited agencies should consider:

   a. Educating staff on the meaning of this element, and how it applies in their day-to-day work; and

   b. Developing and implementing guidance material for staff outlining how to manage changes to the security value across the lifecycle of information.

8. Do organisations manage externally generated information in accordance with instructions (VPDSS E2.080)?

Table 11. Assessment against VPDSS E2.080

Organisation	Status Reported on 2020 PDSP	OVIC Assessment
Barwon Region Water Corporation	Not applicable	Disagree Barwon Water does receive externally generated information.
CenITex	Implemented	Agree, with qualifications Policy and procedure were developed but still marked as drafts.
Victorian Institute of Forensic Medicine	Partial	Agree
Department of Treasury and Finance	Implemented	Agree, with qualifications Did not have sufficient policy and procedural documents to support staff awareness and handling of externally generated information.

E2.080 Explained

169. VPDSS E2.080 under Standard 2 states '*The organisation manages externally generated information in accordance with the originator's instructions.*'

170. VPS organisations will receive information from other organisations, including within the VPS, in a wide range of circumstances that may include one-off situations or as standard practice.

171. The originators of information should communicate instructions for handling information to VPS organisations through applying protective markings to the information and/or by providing prescriptive handling requirements.

172. The primary source for E2.080 is OVIC's *Practitioner Guide: Protective Markings*.[31]

E2.080 Implementation

173. OVIC considers that organisations have implemented this element where VPS personnel readily understand how to recognise and interpret protective markings, including by understanding what security measures correspond with protective markings, or handling instructions.

174. Where material (such as a document) does not have a protective marking, personnel should be comfortable in seeking clarification or instructions from the originator when handling or managing the information while in the organisation's custody.

E2.060 Observations (Documentation Review and Interviews)

175. OVIC did not receive any policies or procedures that stated that externally generated information should be handled in accordance with relevant contractual obligations, Memoranda of Understanding (**MoUs**), Information Sharing Agreements, or the information's protective marking.

176. Cenitex did not provide a document that sets out how to manage externally generated information in accordance with the information's protective marking or other instructions from the originator. Cenitex did, however, supply a draft document outlining some security classification and handling requirements, including instructions regarding the management of protectively marked information from another government agency.

177. In interviews with the audit team, DTF detailed a range of scenarios in which it receives externally generated information. DTF explained that the business groups that handle that information are aware of the handling requirements, and some groups have safes, lockable rooms, and other control measures relevant to the protective marking.

178. VIFM reported that it generates more information than what it receives from external organisations. In audit interviews VIFM described stakeholder meetings that take place to ensure that certain information is managed according to the originator's standards. This is an important process, as it allows an organisation to discuss any markings that are applied to the document and the most appropriate way to handle the information.

179. Barwon Water reported that it receives a small amount of information from external parties such as customers and vendors, but did not receive information that was protectively marked, such as having a security classification. As such, they have not developed processes or guidance explaining how to handle externally generated information in accordance with originators instructions.

180. During interviews with the audit team, nominated personnel from each of the four audited organisations commonly said that when their staff receive externally generated information that has protective markings attached, they handle that material in accordance with that protective marking. However, OVIC observed across all organisations a deficiency in core security controls expected for material protectively marked at a certain level (for example, receiving classified information marked at PROTECTED).

[31] https://ovic.vic.gov.au/data-protection/practitioner-guide-assessing-the-security-value-of-public-sector-information-v2-0/

181. Within this element, OVIC expected to see the development and implementation of clear and concise information handling checklists that guide and support staff in understanding and applying the minimum controls required for different protective markings, across the different security areas. For example, checklists can promote, and guide, staff to utilise appropriate destruction methods such as (in line with the protective marking) secure destruction bins.

182. During the conduct of the interviews, DTF advised that the agency relies on staff expertise to handle externally generated information. The handling of information is supported by an information handling guide that covers off 'use', 'store' and 'dispose' expectations across the security valued information handled by the organisation.

E2.080 Findings

183. During the audit interviews VIFM described existing processes that it had in place to ensure externally generated information is handled in accordance with the originator's instructions.

184. DTF and Cenitex rely on staff awareness (that is often role specific) to ensure that externally generated information is handled in accordance with the originator's instructions. This may not be an effective approach and limits the capability of large, diverse organisations to effectively handle information.

185. Barwon Water did not demonstrate that it has processes in place to ensure that externally generated information is handled in accordance with the originator's instructions.

E2.080 Recommendations

Recommendation 13 – Barwon Water, Cenitex, VIFM and DTF create, or continue to develop, supporting process and guidelines for how personnel can manage the security value of externally generated information.

186. OVIC recommends that all audited agencies develop processes and guidelines for managing the security value of externally generated information through:

    a. Documenting the requirement to manage externally generated information, in accordance with instructions in relevant policies and procedures;

    b. Developing and implement information handling guides for personnel; and

    c. Articulating controls, where necessary, within agreements with third parties and defining these upfront prior to receiving information from third parties.

9. Do organisations manage the secure disposal of information in accordance with its security value (VPDSS E2.090)?

Table 12. Assessment against VPDSS E2.090

Organisation	**Status Reported on 2020 PDSP**	**OVIC Assessment**
Barwon Region Water Corporation	Implemented	Agree
CenITex	Partial	Agree
Victorian Institute of Forensic Medicine	Implemented	Agree
Department of Treasury and Finance	Planned	Agree

E2.090 Explained

187. Element E2.090 of Standard 2 is '*The organisation manages the secure disposal (archiving/destruction) of public sector information in accordance with its security value.*'

188. The objective of E2.090 is to ensure that organisations dispose of public sector information, in accordance with the security value of the material, either through secure archive or by using secure destruction techniques.

189. The primary source for E2.090 is *PSPF INFOSEC-8 Sensitive and Classified Information*.

E2.090 Implementation

190. OVIC considers that organisations have implemented this element where they can establish that:

a. The techniques or methods used by the organisation to archive and/or destroy public sector information is done:

i. in accordance with the security value of the information;

ii. if soft copy, considers specific requirements regarding media types[32]; and

b. The organisation's policies and procedures adequately govern the disposal (archives and/or destroys) of all security valued information that the organisation manages (for example, an organisation may manage information that ranges from BIL 1 – 3).

E2.090 Observations (Documentation Review and Interviews)

191. OVIC focussed on how agencies explain, and provide evidence supporting, the secure disposal (archiving/destruction) of public sector information in accordance with its security value. Based on information gathered during the audit, including PDSP responses, organisational profile assessments, the review of available IARs, and interview responses, OVIC was able to identify the type of information handled by the organisations, and the

[32] Refer to the Information Security Manual for destruction techniques for different ICT media types.

highest level of protectively marked information within the agency, including security classified information. The relevant findings and observations are set out below.

192. Some organisations, such as VIFM and Barwon Water, explained that they employ strict security controls to destroy information.

193. During the document review, both Cenitex and DTF provided evidence of guidance around the secure disposal of information according to the information's BIL, or protective marking, level.

194. Cenitex's security classification and handling standards procedure states:

> *Sensitive and classified information can be compromised because of inappropriate destruction. Cenitex staff must use approved procedures to dispose of sensitive and classified information.*

195. DTF provided a guide to protecting information both within the office, and while working remotely. This document outlined 'use', 'store' and 'dispose' expectations and guidance, as well as additional 'better practice' considerations for working remotely. DTF also provided a specific example of how it disposes of hard copy information marked as OFFICIAL: Sensitive, by utilising locked security waste bins managed under contract through a sensitive waste contractor, who securely disposes of the hardcopy waste.

E2.090 Findings

196. VIFM and Barwon Water did not provide supporting evidence to support statements they manage the secure disposal of all types of information in accordance with the security value of information. However, while VIFM and Barwon Water reported that their processes for disposal were sufficiently secure, the nature of this audit meant OVIC was not able to verify in practice whether the way they manage disposal was appropriate.

197. Cenitex showed, through its draft procedure documentation, that its approach is to dispose of 'sensitive and classified' information using different procedures to those used for information assessed to be of a lower security value.

198. DTF provided a simple and concise guideline to articulate the link between the protective marking, up to and including security classifications, and the appropriate disposal of information.

Agency responses

Barwon Water

Thank you for your letter dated 3 November 2021, providing Barwon Water the opportunity to provide comment on the audit report of practices to assess the security value of public sector information.

We have appreciated the collaborative approach in undertaking this evaluation and the opportunity to align on interpretations of the VPDSS elements.

We note the findings of the audit report and welcome the opportunity to identify and implement measures that will further enhance the security of information. Barwon Water has an ongoing focus on information security and will ensure the findings of this audit are addressed as part of our comprehensive risk-based information security action plans.

Cenitex

[Cenitex notes that in OVIC's] examination of the alignment between the assessment reported in Cenitex's 2020 attestation to OVIC, your office agreed with our assessment for all nine elements in Standard 2 with only one qualification. That qualification for element 2.080 notes that policy and procedural material that Cenitex considers implemented was still marked as 'draft'.

I have requested a review and as appropriate adjustment to our Protective Data Security Plan (PDSP) and implementation program based on your office's recommendations, findings, and observations. The explanation that is included in your report for each element has been helpful to Cenitex's implementation planning.

Cenitex remains committed to the implementation of the VPDSS across its business processes and culture, and to collaborating with customer organisations and external entities to increase the level of protection of public sector information.

Victorian Institute of Forensic Medicine

The VIFM has appreciated the opportunity presented by the audit to better understand the actions required by the Victorian Protective Data Security Standards (the Standards) and to improve our information management and security.

Since the inception of the VIFM some 30 years ago, our operational workflows have been structured around to need to recognise and preserve the sensitivity and confidentiality of the information we gather and the expert reports that we produce for the Victorian justice system as part of our statutory functions.

The VIFM accepts OVIC's audit findings and will incorporate the recommendations from the final report into ongoing activities to progress the VIFM's Protective Data Security Plan. The VIFM has already recognised the need to focus on information management and has recently recruited a dedicated Information Manager to assist the VIFM to meet its information management requirements.

As a small organisation with a complex legislative and regulatory compliance framework, we are constantly faced with the challenges of implementing new and changing compliance programs within our existing. Given these challenges, the VIFM notes in particular that one of the audit's findings is that none of the audited organisations had a consolidated Information Management Framework for managing security risks across all security areas. The VIFM considers that it would be of great assistance to public sector agencies, particularly those with limited resources, if there were a template or example document that agencies could refer to in order to implement this element of the Standards.

Department of Treasury and Finance

[…] [T]hank you for submitting a revised report that has incorporated our feedback. We believe the updated report is fair and reasonable and that we can use this guidance to target maturity improvements for our VPDSS program.

DTF notes this revised report and has no further change requests to submit.