Office of the Victorian Information Commissioner

VICTORIAN PUBLIC SECTOR INSIGHTS

INFORMATION SECURITY MONITORING AND ASSURANCE

2025

Document Details

Victorian Public Sector Insights – Information Security Monitoring and Assurance – 2025		
Protective Marking		OFFICIAL
Approved for unlimited public release		Yes – Authorised for release
Release Date		August 2025
Review Date		N/A
Document Version		1.0
Authority		Office of the Victorian Information Commissioner (**OVIC**)
Author		Information Security Unit - OVIC
Version Control		
Version	Date	Key Changes
1.0	August 2025	Original version

Contents

Introduction

This report presents insights based on information security assurance activities undertaken between 2022 - 2024 of organisations reporting to OVIC.[1]

As an integrity body, OVIC seeks to highlight the information security achievements of organisations, whilst reflecting on information security areas or themes that require further investment and focus. OVIC encourages organisations to consider the insights and intelligence offered in this report and if needed, review their information security risks and recalibrate future work programs.

How to read this report

Chapter 1 – PDSP Insights draws on data from Protective Data Security Plan (PDSP) submissions received in 2022 and 2024.

In 2022, OVIC received 367 PDSPs from organisations, while in 2024, OVIC received 360 PDSPs. Any comparative data between the 2 PDSP cycles are drawn from submissions of 316 organisations. A quantitative and qualitative analysis was also undertaken by the Information Security Unit of this PDSP data.

Chapter 2 – Information Security Incident Insights summarises and contrasts information security incident notifications received by OVIC under the Scheme,[2] from 1 July 2022 to 31 December 2024, paired with incident data reported via 2024 PDSPs.

Chapter 3 – Audits, Investigations, Examinations and Reviews provides an overview of audits, investigations, examinations and reviews conducted by OVIC and other regulatory bodies spanning 2019 to 2024. These monitoring and assurance activities highlight information security insights and suggest associated actions to inform and improve information security practices of organisations.

Chapter 4 – Business Engagement and Outreach Program provides an overview of the proactive outreach activities undertaken by OVIC designed to assist organisations in meeting their obligations under the PDP Act, as well as presenting the volume of enquiries received from 2020 to 2024.

Chapter 5 – Futures provides a brief overview of anticipated product reforms, proposed legislative changes, reporting models and the desire for clarified roles and responsibilities in the information security space.

The Annexure provides background to our analysis, approach, data sources and comparisons, as well as a summary of OVIC's information security monitoring and assurance functions, supplementary insights and resources.

[1] See *Appendix - Report sources, scope and approach* for further information on organisations considered.
[2] To read more about OVIC's Information Security Incident Notification Scheme, please visit: https://ovic.vic.gov.au/information-security/ovic-information-security-incident-notification-scheme/

Commonly used terms

OVIC	Office of the Victorian Information Commissioner	**BIL**	Business Impact Level
PDP Act or **the Act**	*Privacy and Data Protection Act 2014* (Vic)	**CSP**	Contracted service provider
VPDSS or **the Standards**	Victorian Protective Data Security Standards	**IACS**	Industrial Automation and Control Systems
VPDSSE or **the Elements**	Victorian Protective Data Security Elements	**ICT**	Information and Communications Technology
PDSP	Protective Data Security Plan	**LLM**	Large Language Model
The Scheme	Information Security Incident Notification Scheme	**LGA**	Local Government Authority
ISU	OVIC's Information Security Unit	**VPS**	Victorian Public Service
SRPA	Security Risk Profile Assessment	**WoVG**	Whole of Victorian Government
OPA	Organisation Profile Assessment		
VISN	Victorian Information Security Network		
IPPs	Information Privacy Principles		

Please see OVIC's VPDSS Glossary for more terms.[3]

[3] Please see https://ovic.vic.gov.au/wp-content/uploads/2022/01/VPDSS-Glossary-V2.1.docx.pdf.

Executive Summary

This inaugural report marks the beginning of a new chapter in documenting and sharing information security progress, challenges and insights. As the first edition, it has been prepared to provide transparency and promote continuous improvement of organisations' information security programs. It serves as both a reflection of where the Victorian public sector is today and the future we seek to shape.

To better understand the state of information security, or data protection, in Victorian regulated organisations, OVIC requires organisations to submit Protective Data Security Plans to OVIC on a biennial basis.

I would like to thank regulated organisations for their commitment to keeping Victorian information and systems safe, and their participation in the monitoring and assurance activities of OVIC.

It is my hope that the insights collected in this report will increase awareness of the importance of information security programs in the Victorian public sector, as well as providing a valuable insight into the need for ongoing attention to the ever-changing environment that we operate in. I hope the information provided in this report is helpful not only to those organisations reporting to OVIC, but other jurisdictions, contracted service providers and the public.

Sean Morrison

Chapter 1
PDSP Insights

Insights presented in this chapter are based upon organisations' self-assessed implementation of the Victorian Protective Data Security Standards (**the Standards**) as reflected in Protective Data Security Plans (**PDSPs**) submitted to OVIC. The data referenced in this chapter reflects either:

- 360 organisations that submitted a PDSP in 2024, or
- 316 organisations that submitted a PDSP in both 2022 and 2024, enabling a comparative analysis.

The Information Security Unit (**ISU**) undertook a

- quantitative analysis of the 360 reporting organisations' PDSPs, and a
- subsequent qualitative analysis of data from a sample of 50 selected organisations as a representation of the fuller 360 organisations reporting in 2024.

Further information on the *Report sources, scope and approach* can be found in the Appendix.

2024 PDSP submissions

The deadline for the latest cycle of PDSP submissions to OVIC concluded 31 August 2024. OVIC received 360 PDSPs, of which

- 304 were submitted on time – received between 1 July 2024 and 31 August 2024
- 56 were submitted late - received between 1 September 2024 and 31 October 2024.

These numbers are made up of both single and multi-organisational PDSP submissions.[4]

A subsequent 12 were submitted well outside the reporting period – received on or after 1 November 2024 up to the drafting of this report (July 2025). These PDSPs are not included in this report's analysis.

Non-compliance with section 89 of the PDP Act

In January 2025, 12 organisations received correspondence from the Privacy and Data Protection Deputy Commissioner, Rachel Dixon, noting they may be subject to further regulatory action by OVIC as a result of failure to submit a current PDSP.[5]

Following receipt of this letter:

- 7 organisations provided a copy of their PDSP to the Information Commissioner
- one organisation was subsequently assessed as not subject to Part 4 of the PDP Act
- 4 organisations remain outstanding, with 3 of those organisations on-track to provide a copy of their PDSP to the Information Commissioner in 2026.

[4] For further detail on multi-organisation PDSP submissions, refer to the Appendix in this report.

[5] This number excludes School Councils, Class B Cemetery Trusts or Committees of Management.

PDSP analysis

Implementation statuses

OVIC's initial analysis evaluated the progress of each organisation's information security program influenced by a self-assessed implementation status against each element under a Standard.

In the PDSP form, organisations were asked to assess the implementation status of each element, including having regard to all the required components. The nominated implementation status should have reflected the degree to which the organisation believed it had successfully addressed each component of an element. These implementation statuses were as follows:

Not commenced
The organisation has not yet defined or planned the work needed to meet the element.

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 (some)
The organisation has commenced aspects of this element with some activities finalised, but additional work needs to be undertaken.

Partial (most)
Most aspects of this element have been implemented. However, activities are not fully completed or have not been fully shifted to business-as-usual.

Implemented
The organisation currently meets all aspects of the element, and this has shifted to a BAU activity.

Not applicable
There is no related information security risk that needs to be managed.

Whilst implementation of an element and its supporting controls indicates progress, effective implementation requires the ongoing management of risks including prioritising, monitoring, evaluating, and updating risks in line with ever-changing information security threats and vulnerabilities.

Having regard to the dynamic risk environment Victorian government organisations operate in, strict adherence to the VPDSS does not guarantee a fulsome and robust information security program. Whilst the analysis offered for each Standard focuses on implementation status, OVIC is unable to comment on risk prioritisation or control effectiveness of an organisation.

Figure 1.A shows the average implementation status of all the elements across the 12 Standards of the 360 organisations reporting in 2024. Overall, organisations indicated that half of the VPDSS elements were implemented and a further 34% of the elements were reportedly underway.

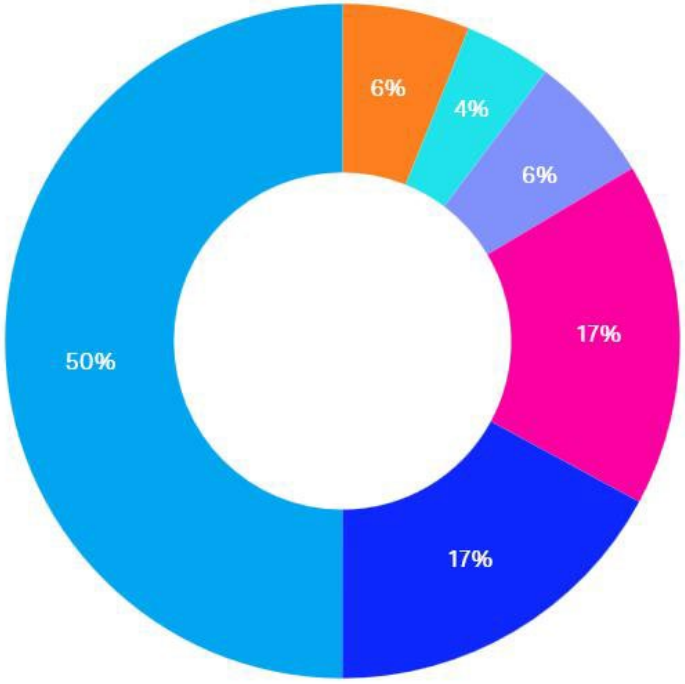


Figure 1.A
Reported status of all elements in 2024

Implementation status - 'not applicable'

Most elements under the Standards will apply to the majority of VPS organisations, however there will be some scenarios where this is not the case. In order to correctly utilise this status, organisations had to determine that there was no related information security risk that needed to be managed.

Where organisations selected an element as 'not applicable' on their PDSP, they were required to provide rationale as to why. Upon review of the PDSPs, the ISU noted that the necessary justification supporting this selection was commonly either not provided or showed a misinterpretation of responsibilities and did not adequately address the element.

A common example was where the organisation noted a third party (e.g. contracted service provider or departmental portfolio agency) was performing an activity or function on behalf of the organisation (e.g. ICT services or facility management). In these scenarios, the reporting organisation may have incorrectly assumed an element was 'not applicable' as they were not directly performing the associated activities or components outlined in the element description. Despite the third party performing these activities on their behalf, the element highlights security components that need to be managed by the reporting organisation. Responsibility for the management and oversight of these risks remains with the reporting organisation and accountability ultimately rests with the public sector body Head of the organisation, not the third party.

In these instances, OVIC considers the selection of 'not applicable' as a discrepancy in the organisation's PDSP. *Chapter 1 – The Standards* contains graphs labelled as *Figure 1.N.E* which show the commonality of this outcome.

PDSP commentary

At the end of each Standard, organisations were given an opportunity to provide additional context and detail to its responses in a free-text box.

The free-text box in the PDSP can:

- offer useful context to the public sector body Head who is ultimately accountable for the information security program
- assist in the ongoing management and continuity of the program (i.e. succession planning should there be changes to staff that drive key pieces of work)
- guide OVIC in gaining an appreciation of the organisation's unique circumstances and why certain responses were given in this instance (i.e. where organisations have recalibrated responses as a result of changing circumstances).

Representative data drawn from the qualitative analysis indicated that 66% of organisations provided additional commentary against each Standard in 2024. Of the 66% of PDSPs that provided commentary, 83% of those contained comments that were relevant to the standard. The remaining 17% of those PDSPs provided comments that were considered by OVIC to not be relevant as they were either a cut and paste from other Standards or other organisations' PDSPs, or generic and unrelated to the correlating Standard.

Maturity insights

The PDSP form also prompted organisations to provide an assessment of the maturity rating for each standard.

For some standards, the elements are sequenced in a particular order of which implementation would inherently influence the selection of the organisation's maturity rating for each standard, i.e. the implementation of certain elements is necessary for the successful implementation of later elements. Applying this principle, where an organisation assessed earlier elements in a standard as 'not commenced' or 'planned', it is unlikely that the organisation's maturity rating will be assessed as 'core', given the foundational aspects of a standard had not been met. For example, the description for the maturity level 'core' is as follows:

> *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.* (emphasis added)

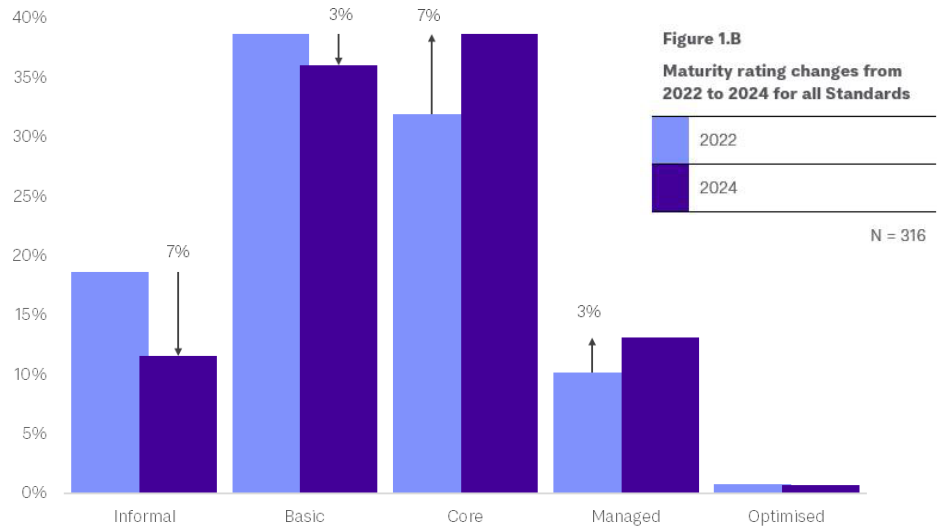
Noting this is a subjective assessment, OVIC observed organisations commonly assessing programs as overly mature while not being able to demonstrate features of the corresponding nominated maturity level.

For example, some organisations selecting implementation statuses under a standard as mostly 'planned' or 'partial,' whilst also selecting a maturity level that suggested the supporting activities were implemented. In this case, the maturity level would be misaligned as the organisation was yet to complete fundamental activities for that standard. Though there is no one-for-one equivalence with implementation status and maturity rating, the descriptors for each maturity level set out expected features of the organisation's security practices and program, and what it means to be at a certain maturity level.[6]

Assessing maturity provides a structured approach to process improvement by providing descriptions that advise organisations of their status in relation to each Standard and provide an opportunity to reflect on where they want to be. OVIC acknowledges that maturity assessment is not necessarily well-understood and can be challenging given the various maturity models in government and private sector. OVIC will review this metric as part of our ongoing VPDSS review schedule.

The following statistics present an overview of the average shifts in maturity ratings in the 316 organisations reporting in 2022 and 2024. The graph shows that some organisations 'walked-back' their maturity rating of certain standards, while some standards saw an average overall increase in maturity rating selection.

As shown in *Figure 1.B*, across all standards (except standard 11), OVIC observed an average increase of 7% in the selection of 'core' as a maturity rating in 2024 compared to reporting in 2022. A contrasting downward shift of 7% in the selection of 'informal' as a maturity rating can also be seen in the accompanying graph. This overall decrease in the lower maturity levels of 'informal' and 'basic' and corresponding relative increase in the 'core' and 'managed' maturity levels across the Standards for 2024 is encouraging. This natural progression reflects a level of comfortability with the Standards, as well as the maturation of information security programs across the VPS that are either in progress, or, implemented and being managed.



[6] 2024 PDSP How-To Guide, provided to organisations as part of the previous PDSP reporting cycle. This is an archived resource published by OVIC that provided instructions to organisations on completing a PDSP submission.

Overall themes

Understanding of Standards

Most organisations presented a consistent, proficient, or practical understanding of the Standards, with some PDSPs showing effort to re-baseline prior responses through the revision of their reported element status and maturity ratings.

Based on thematic insights drawn from the qualitative analysis performed by the ISU, it is encouraging to see that only 6% of organisations were assessed as not understanding the Standards as illustrated in *Figure 1.C.*

This graph can also be read alongside quantitative statistics drawn from the Organisational Profile Assessment (**OPA**) section of an organisation's PDSP, where OVIC saw 14% of organisations indicating a *lack of understanding of the Standards* as a challenge or barrier to implementation of the VPDSS.

OVIC seeks to work with these organisations as part of its monitoring and assurance functions and business outreach program.

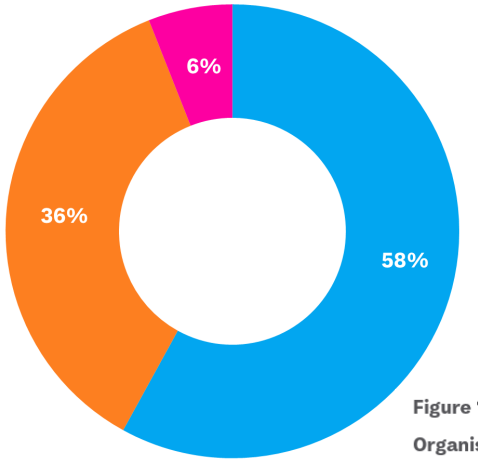


Figure 1.C

Organisations' overall understanding of the Standards

	Consistent, proficient or practical understanding
	Basic understanding
	Not understood

N = 50

ICT focus

OVIC noted a continued strong emphasis on cyber security, ICT-related elements, or the tendency to frame all elements in a standard with an ICT bias in the free-text fields. This meant there was a lack of detail for other domains such as personnel, governance, physical and business continuity and disaster recovery. ICT controls alone will not holistically address cyber security. Organisations need to consider all information security areas when mitigating cyber security risk.

For example, under *Standard 3 – Information Security Risk Management* and *Standard 4 - Information Access* some organisations tended to present ICT-related commentary with little reference to the management of risk and access controls with respect to physical format material and verbal disclosures. OVIC's qualitative review identified roughly 36% of organisations were assessed as having an overall cyber focus.

Third-party arrangements

Many organisations reported lower than expected numbers of third-party arrangements. As such, OVIC prompts organisations to consider other arrangements where third parties are likely to be present. Under the VPDSS, a third-party provider can be any person or entity outside an organisation that accesses, handles, stores or manages any information or systems on its behalf. This definition encompasses scenarios where an individual, company, organisation (public or private), system or tool handles, processes, stores or manages information and/or systems on the organisation's behalf.

Third-party arrangements can take many forms, including but not limited to:

- state contracts (e.g. those addressing storage facilities for hard-copy and soft-copy records, digitisation services, software vendors, transport companies)
- local consultancies brought on by the organisation to deliver a particular project or task
- information sharing arrangements where those external to the organisation have direct access to information and/or systems.

OVIC is conscious of shared support arrangements offered by portfolio departments, where subsidiary organisations rely upon these arrangements for personnel, infrastructure, or services. In each instance, peripheral parties introduce new risks for the organisation to manage. Irrespective of the construct of these arrangements, it is the responsibility of the originating organisation to ensure its information and systems are protected throughout the lifecycle of the engagement.

Cross-functional workgroups

OVIC encourages organisations to utilise internal workgroups with representatives from across the business who contribute subject-matter expertise unique to their security domain or functional work area. By adopting this approach, organisations' information security programs are informed by specialist knowledge and capabilities to develop the organisation's PDSP and manage the subsequent implementation of the VPDSS elements. Representation could be from the following areas:

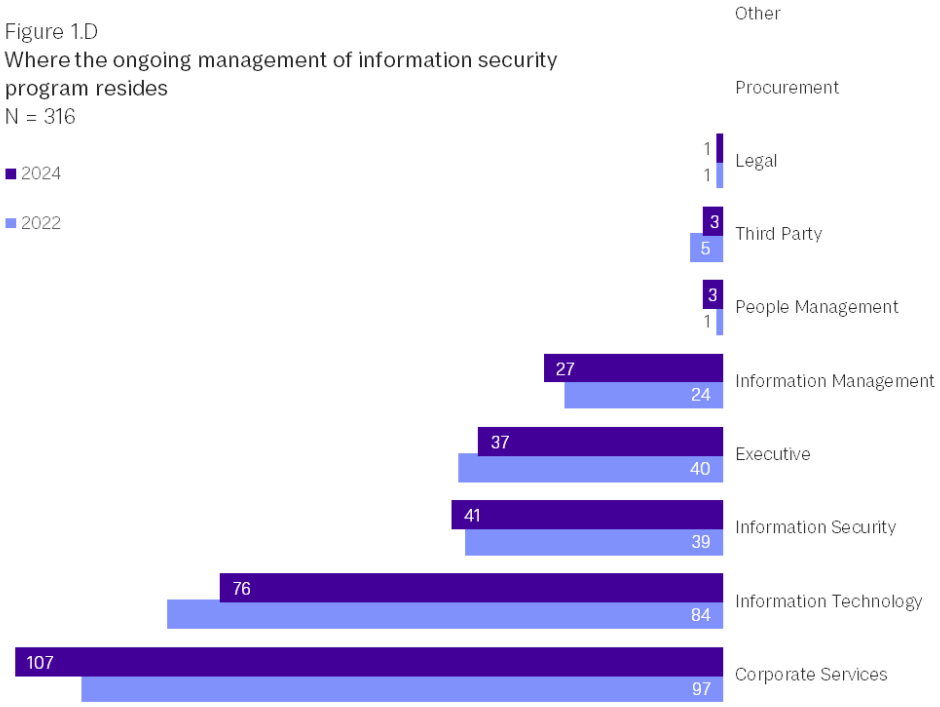
Governance	Facilities and built environment
People and culture	Legal
Risk/Internal audit	Information Technology
Finance	Third-party contracted service providers and/or Departmental Portfolio (where services, support or infrastructure are provided)
Information/Records management	

While it is critical that all areas of the business work together and present a coherent and unified approach in addressing information security risks, one area of the business typically leads the information security program.

Responsibility for the information security program

As illustrated in *Figure 1.D*, a comparative analysis of the 316 organisations' PDSPs in 2022 and 2024 indicates there has been an increase in the ongoing management of the information security program residing with corporate services and information management areas of the organisation. Reporting therefore shows a shift away from the more traditional business area of Information Technology. OVIC recognises that different organisations will refer to and structure their business units in different ways which should be taken into account when considering this data.

Figure 1.D
Where the ongoing management of information security program resides
N = 316



Challenges and barriers

As mentioned above, organisations were asked to nominate any challenges and barriers to the implementation of the Standards. As shown in *Figure 1.E,* a comparative analysis of 2022 and 2024 PDSPs shows similar challenges and barriers across the years. For example, in 2024, resourcing and finance continue to be the highest challenges with:

- 246 of 316 organisations indicating resourcing challenges
- 175 of 316 organisations noting financial concerns.

Interestingly, there was an increase of 18.5% in reliance on third parties from the prior reporting period. Third parties can assist in implementing controls for organisations, however increased reliance on outsourced arrangements can also introduce new information security risks that need to be managed on an ongoing basis.

'Machinery of government' changes also present challenges, with the figure almost doubling from 2022 to 2024. The repercussions of these transitional arrangements continue to impact affected organisations' information security programs. These impacts are also evidenced in the field 'significant change'.

OVIC understands that most VPS organisations will be facing ongoing financial constraints which may lead to resourcing issues. We expect this trend to continue into 2026 reporting.

Encouragingly, there has been a decrease over time in organisations selecting 'lack of understanding of the Standards' and 'capability' as barriers to implementation. This is encouraging and may be due to increased efforts in business engagement and outreach activities led by the OVIC's ISU, coupled with increased stakeholder familiarity with the Standards over time.

Note: *Figure 1.E* shows the selections made by organisations, noting that organisations were able to select multiple challenges and barriers.

Standards

Standard 1 – Information Security Management Framework

> *An organisation establishes, implements and maintains an information security management framework relevant to its size, resources and risk posture.*

Overall implementation status for Standard 1

Figure 1.1.A shows the overall self-assessed implementation statuses for the 13 supporting elements under Standard 1 (including the 2 related IACS elements).[7]

This Standard directs organisations to establish strong governance arrangements to ensure the information security requirements are reflected in organisational planning. By investing in the development of robust governance arrangements, the organisation can direct and control processes for the protection of information and systems.

Figure 1.1.A shows there is a modest implementation status with half of the responses for elements under Standard 1 being fully implemented. This Standard presents foundational activities that support the development of organisations' information security programs. OVIC would expect to see less elements as being selected as 'not commenced' (5%) and 'planned' (7%).

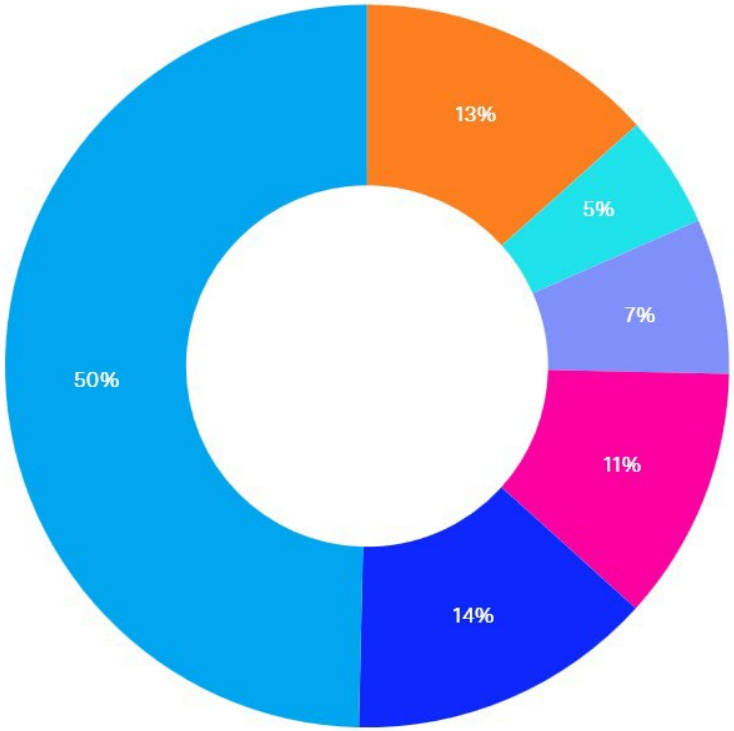


Figure 1.1.A
Reported implementation status of all Standard 1 elements

[7] In December 2022, OVIC introduced additional elements addressing Industrial Automation and Control Systems (**IACS**), to cater for the unique performance and reliability requirements, operating systems and applications of organisations that use this technology.

To read more about IACS and the VPDSS, please see OVIC's *Implementation Guidance for Industrial Automation and Control Systems*: https://ovic.vic.gov.au/information-security/information-security-resources/implementation-guidance-for-industrial-automation-and-control-systems/

Implementation status per element by sector

Figure 1.1.B visually benchmarks various implementation statuses across different sectors to show an average reported implementation status. This gives more detailed insights into how different parts of the VPS are performing against Standard 1.

OVIC notes that larger and more established organisations appear to offer stronger implementation responses for this Standard. This may be due to more stable and consistent governance arrangements, structures, and operating environments.

Only a small portion of Victorian government organisations operate Industrial Automation and Control Systems (**IACS**), as illustrated by only 13.6% of reporting organisations affirming the presence of IACS in their Organisation Profile Assessment (**OPA**). This would explain the high number of organisations reporting E1.120 and E1.130 that specifically relate to IACS as 'not applicable', [8] as presented in *Figure 1.1.B*.

Excluding the Water Corporations and Catchments sector, the majority of sectors indicated these IACS elements as 'not applicable' with some minor variation shown in the Industry and Transport sector.

Figure 1.1.B also shows a lower implementation status for E1.070 which may be explained by a lack of understanding of the specific activities associated with this element. [9] This is further evidenced by enquiries received by the ISU seeking further explanation or assistance. This trend provides valuable insight for OVIC when considering reviews or revisions of the current Standards and associated material.

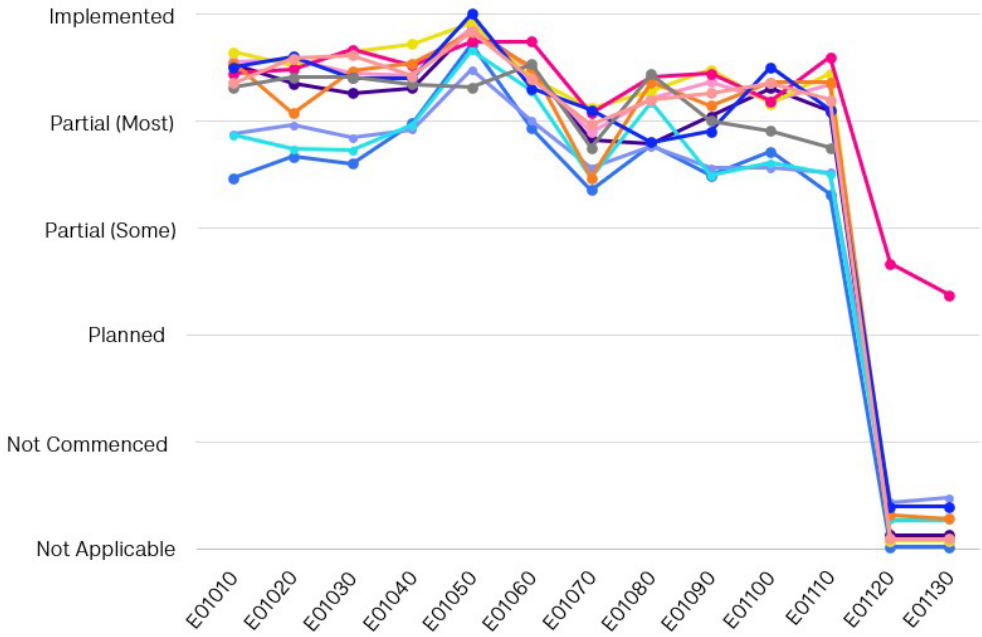


Figure 1.1.B
Average implementation status for Standard 1 elements by sector

Justice, Community and Emergency Services	Water Corporations and Catchments
Finance, Legal, and Administrative	Arts, Sport and Recreation
Health and Human Services	Departments
Industry and Transport	Environment and Land Management
Local Government	Regulatory and Integrity Bodies
Education	N = 360

[8] E1.120 - *The organisation's information security framework defines the relationship between the business areas that support IT security and the business areas that support Industrial Automation and Control Systems (IACS) security.* E1.130 - *The organisation's information security framework differentiates security objectives of the Industrial Automation and Control Systems (IACS) from the enterprise systems.*

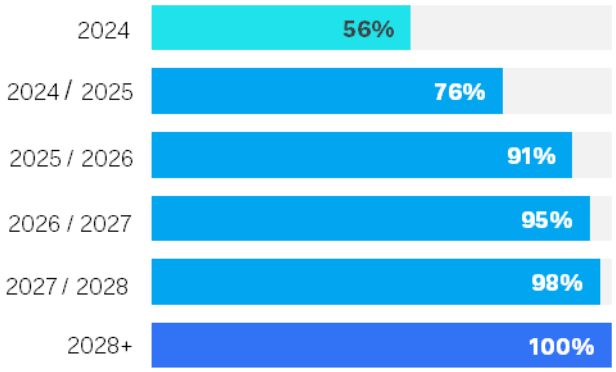
[9] E1.070 - *The organisation identifies information security performance indicators and monitors information security obligations against these.*

Proposed completion dates

The PDSP required organisations to nominate a proposed completion date for each applicable element under the Standard. This nominated date referred to the estimated timeline for the finalisation of all components of the element. This was designed to assist organisations in prioritising their implementation efforts by a selected financial year.

Figure 1.1.C represents the proposed timeline for the implementation of the remaining Standard 1 elements. 56% of applicable Standard 1 elements were reported as implemented, 76% of the applicable elements were projected to be implemented by 2024/2025, and 91% of the elements to be implemented by 2025/2026. Subsequently, organisations projected a relatively steady timeline for the remaining elements yet to be implemented by or around 2028.

Figure 1.1.C
Standard 1 - Current / projected implementation timeline



2022 and 2024 comparison

Average implementation status per element in Standard 1 (2022 v 2024) (excluding IACS elements)

Figure *1.1.D* presents the average implementation status of elements under Standard 1 across 2022 and 2024, showing an overall increase in the implementation status across organisations.

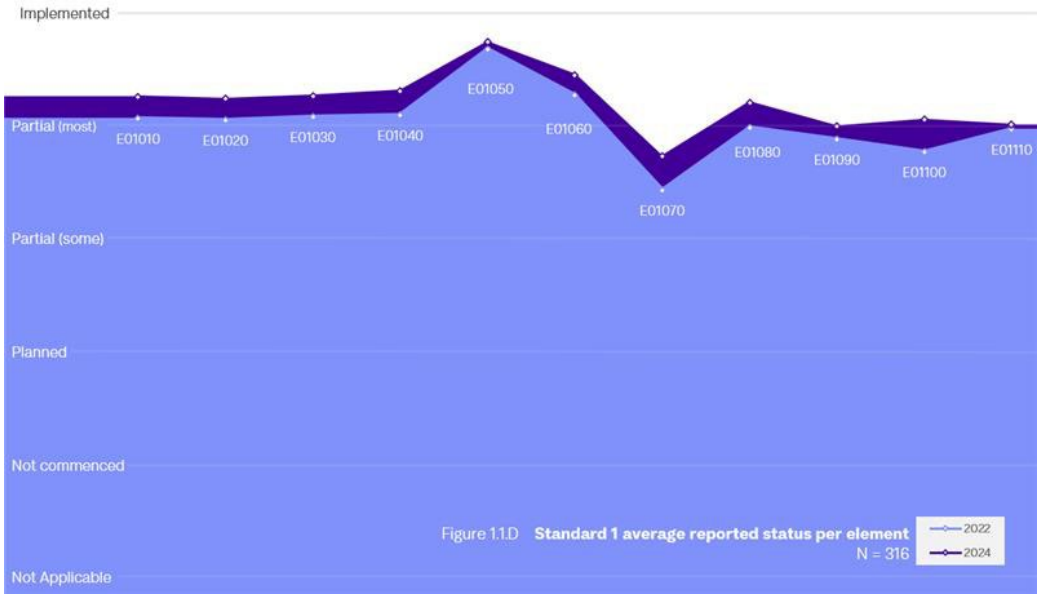


Figure 1.1.D **Standard 1 average reported status per element** N = 316

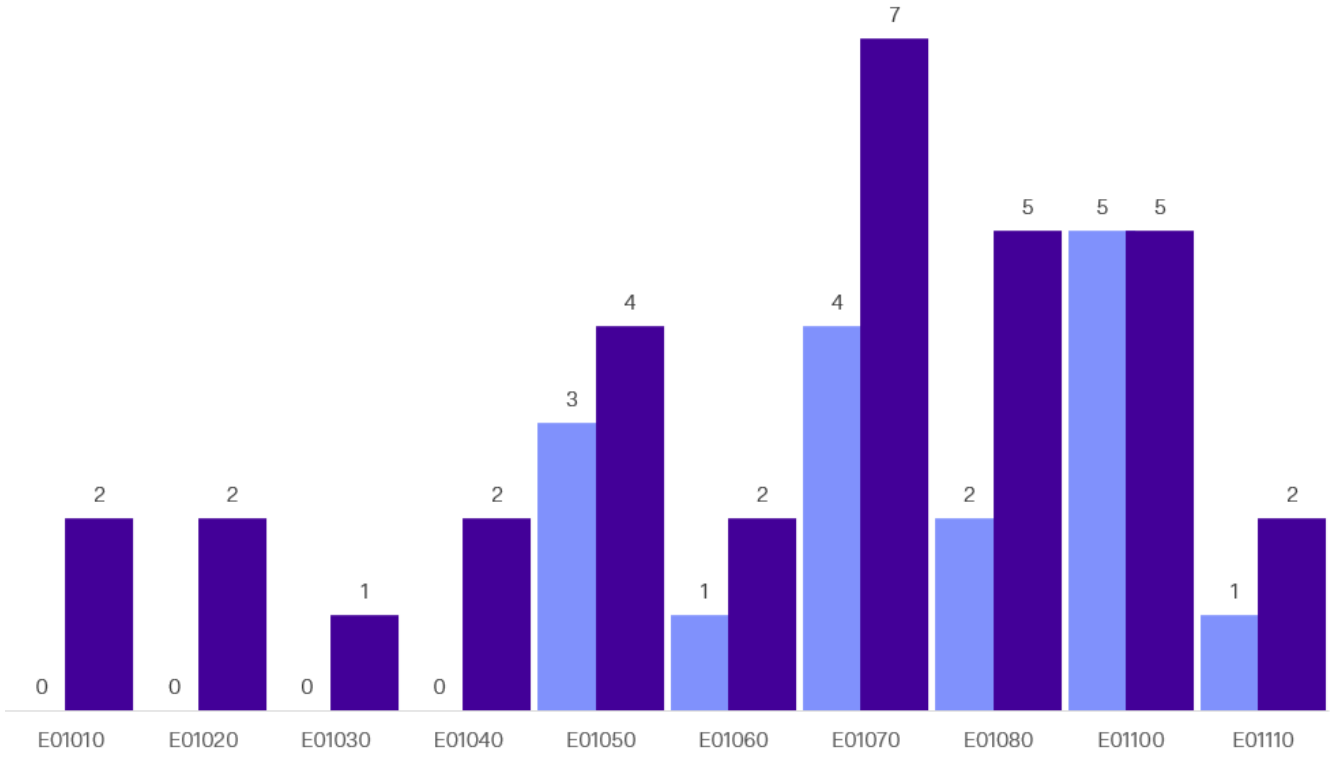
Comparison of Standard 1 elements reported as 'not applicable' (2022 v 2024)

As discussed in the *General Observations* section of this report, some organisations nominated elements as being 'not applicable'. Given the foundational nature of Standard 1, OVIC expected a lower occurrence of elements deemed as 'not applicable'.

Figure 1.1.E shows a total of 16 responses selecting Standard 1 elements as 'not applicable' in 2022 with this figure doubling in 2024.[10] The increase in 'not applicable' elements in 2024 mostly come from E1.070 and E1.080 which relate to identifying performance indicators and providing sufficient information security resources. OVIC understands organisations may not have implemented these elements or may have outsourced their security resources. However, this does not mean these elements are not applicable.

Figure 1.1.E

Count of organisations that selected 'Not Applicable' for Standard 1 elements



[10] The comparative data shown in *Figure 1.1.F* does not represent IACS elements which made up a large proportion of the 13.6% of Not Applicable responses in *Figure 1.1.A*.

Standard 2 – Information Security Value

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

Overall implementation status for Standard 2

Figure 1.2.A shows the overall self-assessed implementation statuses for the 10 supporting elements under Standard 2 (including one related IACS element). This Standard requires organisations to have a consistent approach to identifying and assessing the security value of public sector information. This informs the application of security measures to maintain the confidentiality, integrity and availability of this information and systems.

The graph shows a proportionate distribution across a range of implementation statuses, showing just 40% of elements under Standard 2 as implemented. This is the lowest implementation rate across all Standards. Given this standard represents activities associated with steps 1 and 2 of the Five Step Action Plan,[11] these foundational elements are integral to organisations establishing information security programs.

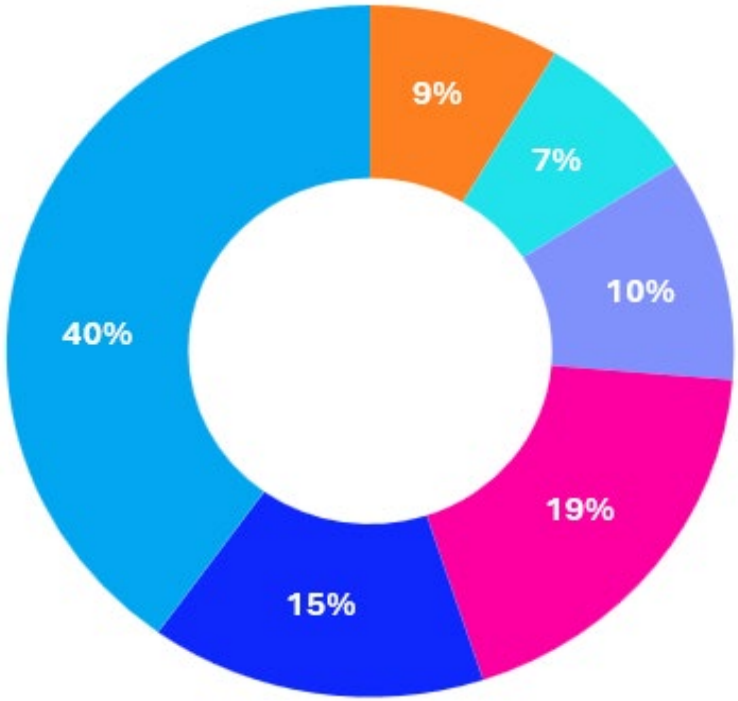


Figure 1.2.A
Reported implementation status of all Standard 2 elements

[11] To read more about the *Five Step Action Plan* please visit: https://ovic.vic.gov.au/resource/the-five-step-action-plan/.

Implementation status per element by sector

Figure 1.2.B shows the average implementation status of each element under Standard 2 broken out by sector.

Early elements in this Standard directs organisations to conduct foundational activities such as identifying, assessing and managing their information assets (E2.020, E2.030, E2.040). The staging of these elements reflects a logical implementation of the supporting activities, creating a solid base for subsequent programs of work.

This is evidenced in *Figure 1.2.B* where strong implementation statuses are featured in the earlier elements. Generally, there appears to be a strong implementation status overall, however the data points to some challenges in elements E2.060 and E2.070.[12] This may be due to a lack of stakeholder understanding of aggregated security value and the information lifecycle.

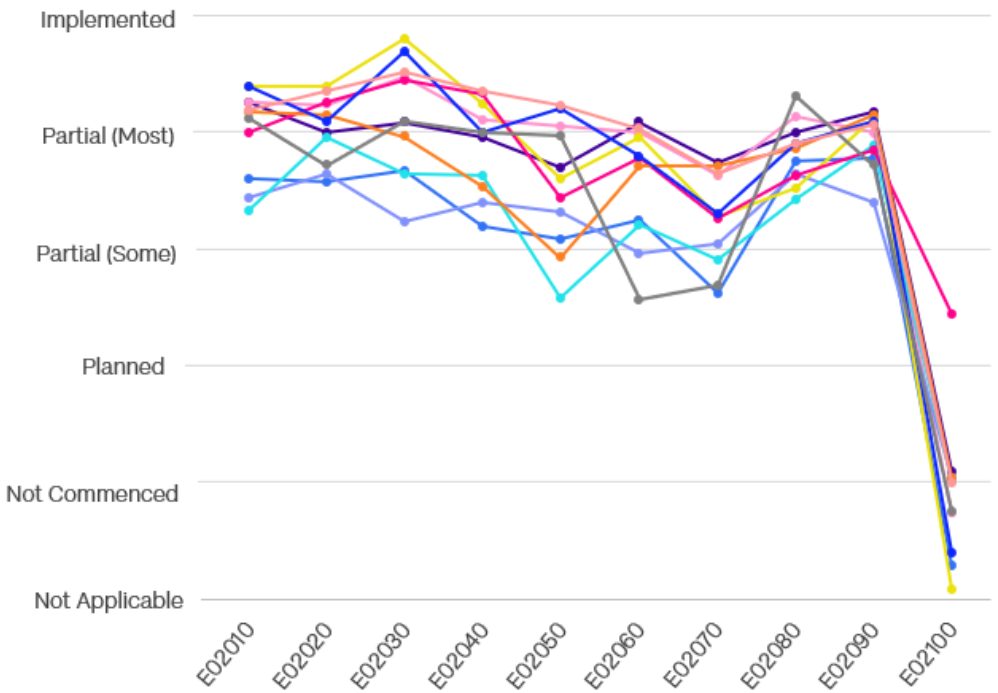


Figure 1.2.B
Average implementation status for Standard 2 elements by sector

[12] 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.*

Protective marking breakdown by sector

In our analysis of the 2024 PDSPs, OVIC considered the responses offered by organisations in the OPA section, comparing these responses against some of the element implementation statuses of Standard 2. A representation of the protective marking breakdown of the sectors is shown in *Figure 1.2.C*. As expected, *Figure 1.2.C* shows the majority of Victorian Government information is between OFFICIAL (BIL 1) and OFFICIAL: Sensitive (BIL 2). There is some work to be done to assess the security value of the information handled by Local Government, Education, and the Art, Sport and Recreation sectors which all have an average of 20% and over as 'Not Assessed'.

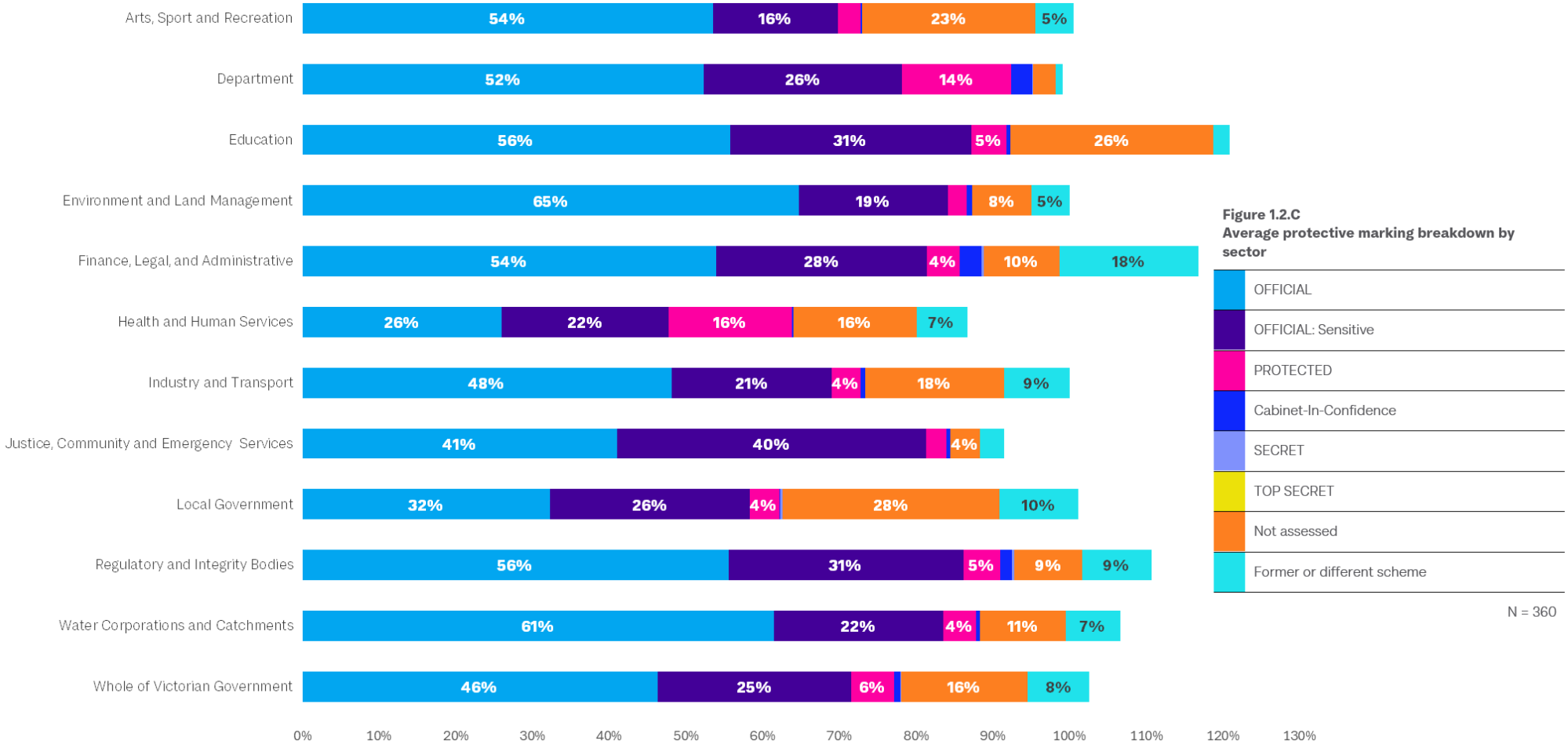
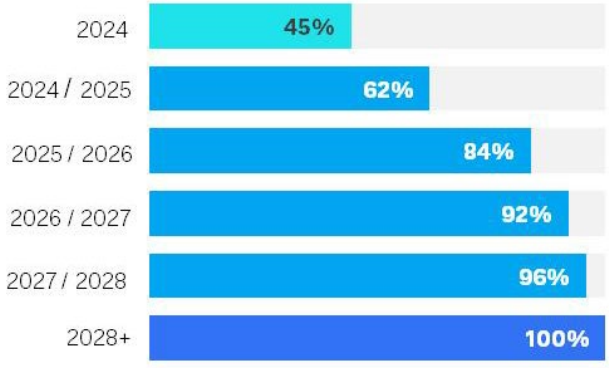


Figure 1.2.C
Average protective marking breakdown by sector

Proposed completion dates

Figure 1.2.D represents the proposed timeline for the implementation of the remaining Standard 2 elements. 45% of applicable Standard 2 elements were reported as implemented with a 17% increase by 2024/2025, and organisations projecting a relatively steady timeline for the remaining elements by or around 2028.

Figure 1.2.D
Standard 2 - Current / projected implementation timeline



2022 and 2024 comparison

Average implementation status per element in Standard 2 (2022 v 2024) (excluding IACS elements)

Figure 1.2.E presents the average reported implementation status of elements under Standard 2 across 2022 and 2024, showing an overall increase in the implementation status across the 316 organisations.

The drop in implementation from 2022 to 2024 in E2.090 may be reflective of a rebaselining of organisations' understanding of the element.[13] This Standard appears to be tracking consistently across the 2 reporting cycles.

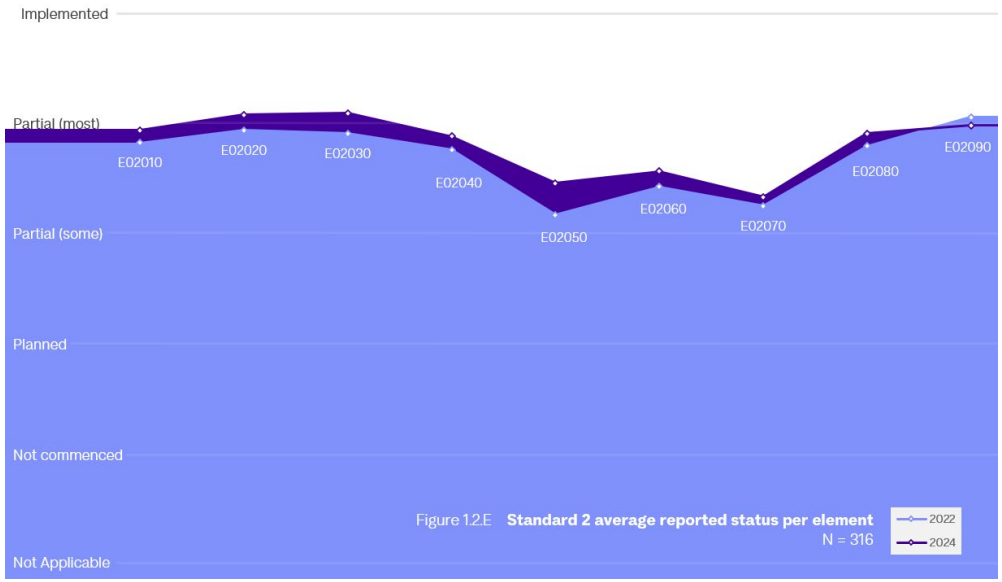


Figure 1.2.E **Standard 2 average reported status per element**
N = 316

[13] E2.090 - *The organisation manages the secure disposal (archiving/ destruction) of public sector information in accordance with its security value.*

Comparison of Standard 2 elements reported as 'not applicable' (2022 v 2024)

Figure 1.2.F shows a 52% increase in the selection of 'not applicable' between 2022 and 2024.

As noted above, activities associated with the elements require organisations to consistently identify and assess the value of its information, driving the application of commensurate security measures.

OVIC encourages organisations to reconsider the selection of 'not applicable' for any element in Standard 2, excepting the IACS element for those organisations where this is not relevant (N.B. IACS element E2.100 has been deliberately excluded from comparison in this graph).

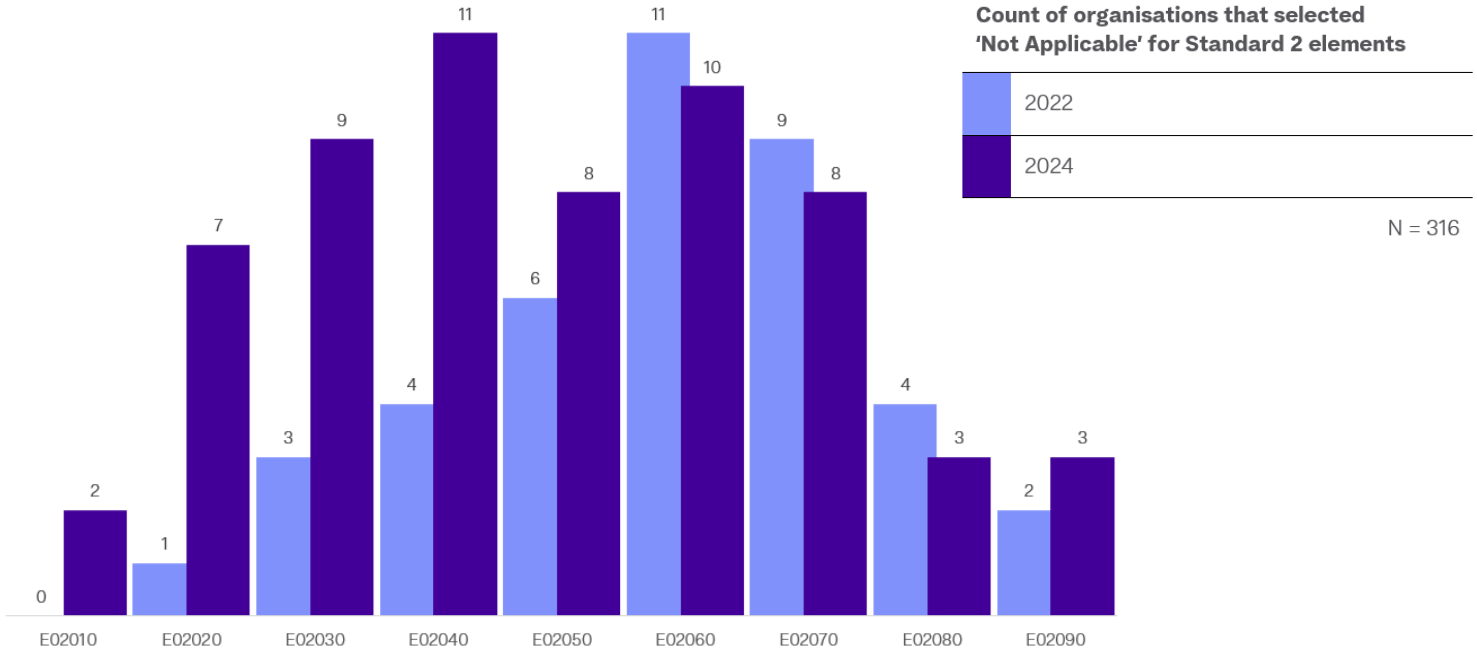
As part of OVIC's qualitative review, some organisations' justifications supporting the 'not applicable' were not in line with instructions in the 2024 PDSP How-To Guide.[14]

This is evidenced in justifications noting that they were a relatively small organisation, had a lack of 'critical assets' or were a subsidiary of a department.

The selection of this status should be based upon the organisation determining there is no related information security risk that needs to be managed, which is highly unlikely for these elements. The inappropriate selection of this status highlights a potential opportunity for clarification and education on this subject as part of OVIC's engagement and outreach program.

Figure 1.2.F

Count of organisations that selected 'Not Applicable' for Standard 2 elements



[14] 2024 PDSP How-To Guide, provided to organisations as part of the previous PDSP reporting cycle. This is an archived resource published by OVIC that provided instructions to organisations on completing a PDSP submission.

Standard 3 – Information Security Risk Management

> *An organisation utilises its risk management framework to undertake a Security Risk Profile Assessment to manage information security risks.*

OVIC has received a number of enquiries concerning Standard 3, with stakeholders seeking guidance on how to undertake information security risk assessments. This may be due to the requirement under the PDP Act to undertake a Security Risk Profile Assessment (**SRPA**) which must include an assessment of any contracted service provider (**CSP**) of the agency or body "to the extent that the provider collects, holds, uses, manages, discloses or transfers public sector data for the agency or body."[15]

OVIC has published resources that align with the Victorian Government Risk Management Framework,[16] designed to assist organisations understand, prioritise and manage information security risks. [17]

Overall implementation status for Standard 3

Figure 1.3.A shows the self-assessed implementation statuses for the 5 supporting elements under Standard 3. Standard 3 has the strongest implementation rate of all the Standards with 59% of the elements implemented. This strong implementation rate is significant as information security risk management helps organisations prioritise the application of controls to protect public sector information and systems. This approach balances the benefits and potential costs of information security activities, ensuring security measures reflect the value of information. Given the Victorian Protective Data Security Framework and Standards (**VPDSF/S**) are based upon sound risk management principles, the implementation of Standard 3 and its supporting elements is critical in establishing an efficient, effective and economic information security program. OVIC encourages organisations who reported 'not applicable', 'not commenced', or 'planned' to invest in these fundamental activities.

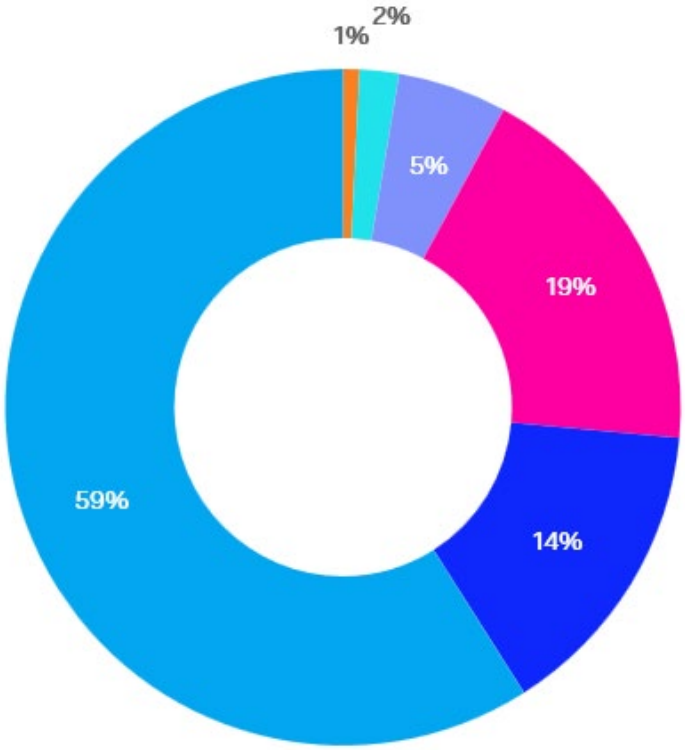


Figure 1.3.A
Reported implementation status of all Standard 3 elements

[15] *Privacy and Data Protection Act 2014* (Vic), sections 89(1) and 89(2).
[16] OVIC's Practitioner Guide to Information Security Risk Management: https://ovic.vic.gov.au/resource/practitioner-guide-information-security-risk-management/ and Practitioner Guide: Control Analytics: https://ovic.vic.gov.au/information-security/practitioner-guide-control-analytics/

[17] To read more about the VGRMF, please visit https://www.vmia.vic.gov.au/tools-and-insights/victorian-government-risk-management-framework

Implementation status per element by sector

Figure 1.3.B shows the average implementation status of each element under Standard 3 broken out by sector.

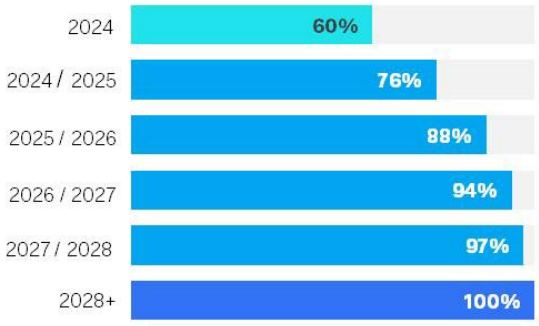
Under this Standard, OVIC observed the departments coupled with Industry and Transport, and Justice, Community, and Emergency Services with weaker implementation status than those from other sectors.

Whilst some of these organisations report they are conducting information security risk assessments, subsequent responses indicate inadequate recording of outcomes and treatment plans in their risk registers.[18]

Proposed completion dates

Figure 1.3.C represents the proposed timeline for the implementation of the remaining Standard 3 elements. 60% of applicable Standard 3 elements were reported as implemented with a slow implementation trajectory for the remaining elements.

Figure 1.3.C
Standard 3 - Current / projected implementation timeline



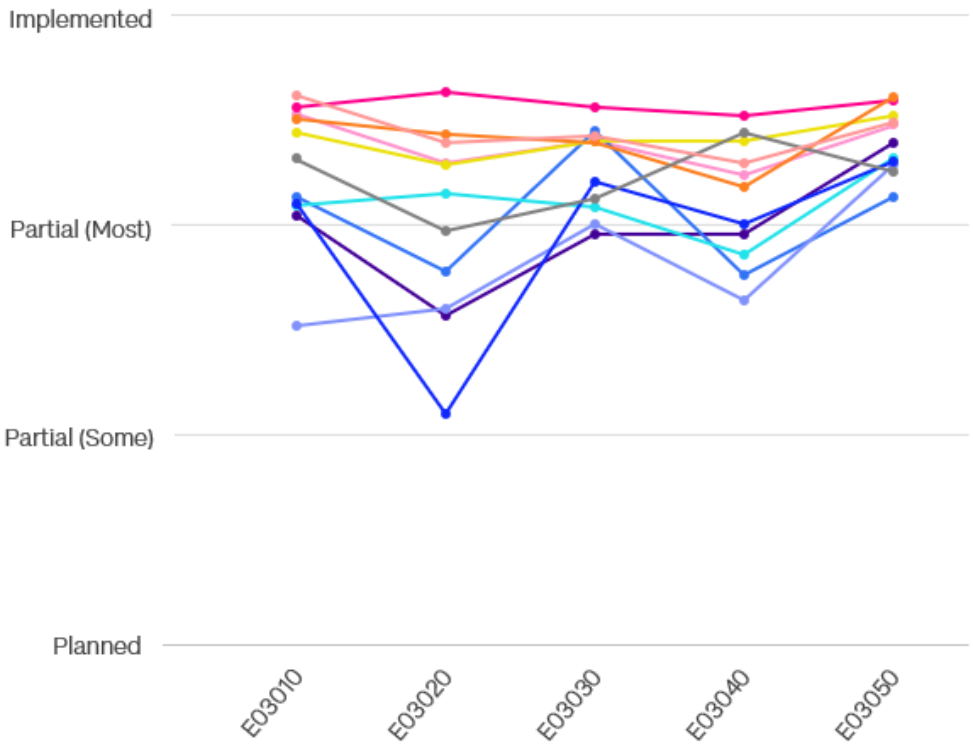


Figure 1.3.B
Average implementation status for Standard 3 elements by sector

Justice, Community and Emergency Services	Water Corporations and Catchments
Finance, Legal, and Administrative	Arts, Sport and Recreation
Health and Human Services	Departments
Industry and Transport	Environment and Land Management
Local Government	Regulatory and Integrity Bodies
Education	N = 360

[18] E3.020 - *The organisation records the results of information security risk assessments and treatment plans in its risk register.*

2022 and 2024 comparison

Average implementation status per element in Standard 3 (2022 v 2024)

Figure 1.3.D presents the average implementation status of elements under Standard 3 across 2022 and 2024. It shows an overall increase in the implementation status across the 316 compared organisations.

Organisations reported strong implementation for each of these elements for the 2 reporting cycles which is encouraging given it is a foundational principle of the VPDSF and VPDSS.

Where organisations reported strong implementation statuses for Standard 3, OVIC expected to see risk references against all the applicable elements in the corresponding PDSP fields. As outlined in the 2024 PDSP How-to guide,[19] organisations were required to record their internal risk references in the Entity Risk Reference field. OVIC expects that an organisation has at least one information security risk recorded in its internal risk register. This helps track and manage information security risks resulting from the SRPA process.

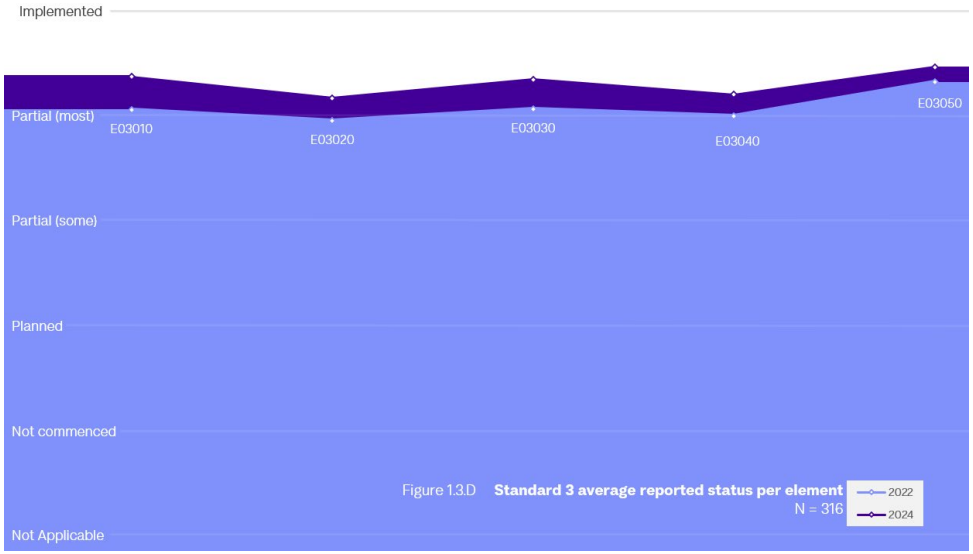


Figure 1.3.D **Standard 3 average reported status per element**
N = 316

Where an entity risk reference was not represented in the PDSP, it may indicate more of a compliance-based approach, and organisations should revisit their submissions account for this discrepancy.

A compliance-based approach focuses on meeting regulatory requirements, industry standards, and legal obligations. In contrast, a risk-based approach involves identifying and assessing potential risks to an organisation's information assets and then implementing controls to mitigate those risks. A risk-based approach is proactive in nature and involves a continuous process of risk assessment and management.

[19] 2024 PDSP How-To Guide, provided to organisations as part of the previous PDSP reporting cycle. This is an archived resource published by OVIC that provided instructions to organisations on completing a PDSP submission.

Comparison of Standard 3 elements reported as 'not applicable' (2022 v 2024)

Of the 316 organisations that reported in both 2022 and 2024, 'not applicable' response rates increased threefold.

As seen *Figure 1.3.E*, elements E3.020 and E3.040 saw a large increase in organisations nominating this status.[20] However, some of the justifications supporting the selection of this status were not in line with instructions in the 2024 PDSP How-To Guide.

OVIC would encourage organisations to reconsider the selection of 'not applicable' given the above stated importance of these elements and the lack of meaningful justifications offered.

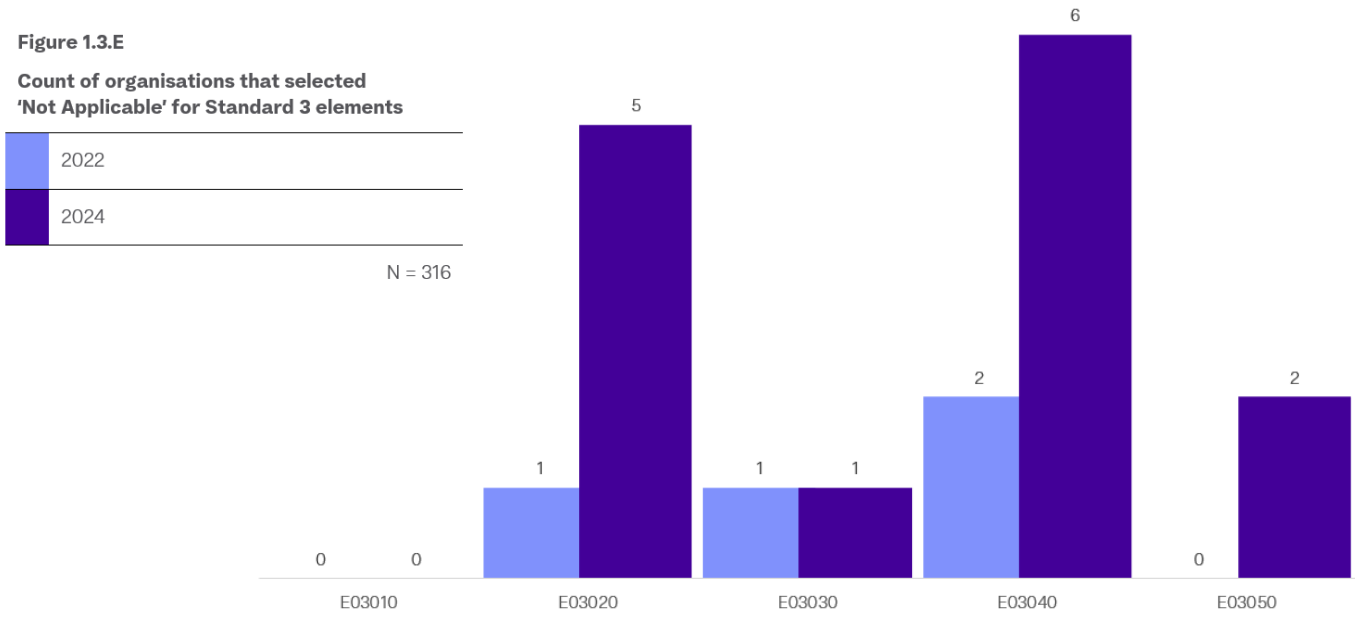
The selection of this status should be based upon the organisation determining there is no related information security risk that needs to be managed. Selecting 'not applicable' for E3.020 and E3.040 would indicate that an organisation has identified it does not need to record or communicate its risks which is unlikely given the nature of these elements.

Consistent with other Standards, certain rationale provided supporting the selection of this status were not in line with instructions in the 2024 PDSP How-To Guide.

Across the 2 reporting cycles, all organisations understand that E3.010 is applicable.

Figure 1.3.E

Count of organisations that selected 'Not Applicable' for Standard 3 elements



[20] E3.020 - *The organisation records the results of information security risk assessments and treatment plans in its risk register.* E3.040 - *The organisation communicates and consults with internal and external stakeholders during the information security risk management process.*

Standard 4 – Information Access

> *An organisation establishes, implements and maintains an access management process for controlling access to public sector information.*

Overall implementation status for Standard 4

Figure 1.4.A shows the overall self-assessed implementation statuses for each of the 7 supporting elements under Standard 4. This Standard directs organisations to implement formal authorisation and management of physical and logical access of public sector information.

As seen in the graph, organisations had a relatively strong implementation rate, with 54% of the elements under Standard 4 reported as 'implemented' in 2024.

A further 22% were 'partial most' and a subsequent 18% were 'partial some.' Just 6% of responses were distributed across the statuses of 'not applicable', 'not commenced', and 'planned' in this Standard.

OVIC is encouraged by these responses, especially considering increasing interest in the adoption of enterprise Generative Artificial Intelligence tools. Implementation of these tools can magnify existing risks to the security of public sector information, including the potential for unauthorised access to information where access permissions may not have been properly configured. This issue (misconfiguration of access controls) is one of the most common causes of data breaches reported to OVIC.[21]

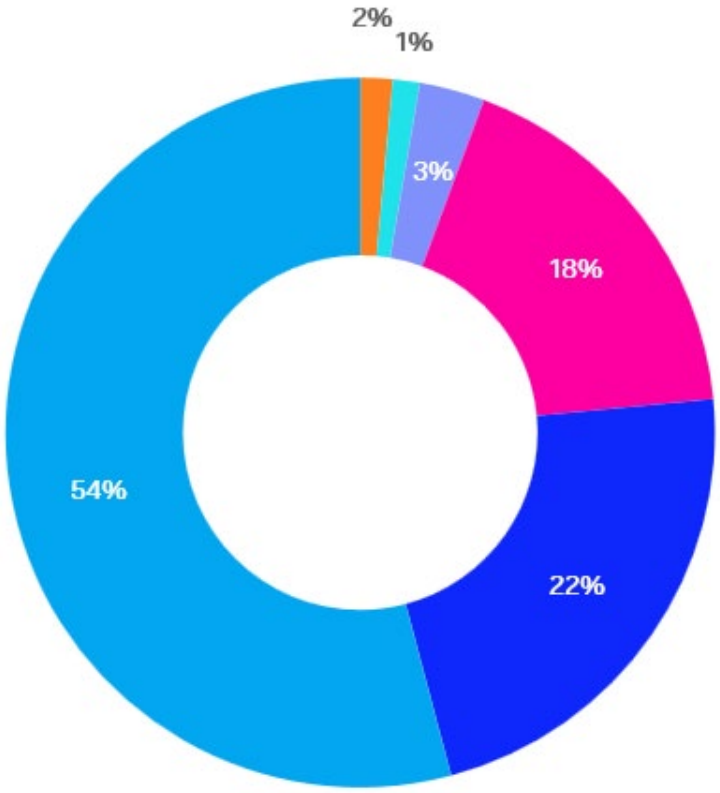


Figure 1.4.A
Reported implementation status of all Standard 4 elements

[21] OVIC Incidents Insights Report: 1 July 2022 – 31 December 2022: https://ovic.vic.gov.au/information-security/security-insights/incidentinsights-report-1-july-2022-31-december-2022/.

Implementation status per element by sector

Figure 1.4.B shows the average reported status of each element under Standard 4 broken out by sector. Under this Standard, OVIC observed the sector encompassing Environment and Land Management organisations, as well as the departments, as having a low reported implementation status than their sector counterparts. As seen in the graph, there appears to be an increase in implementation for elements E4.030 and E4.040 across sectors.[22]

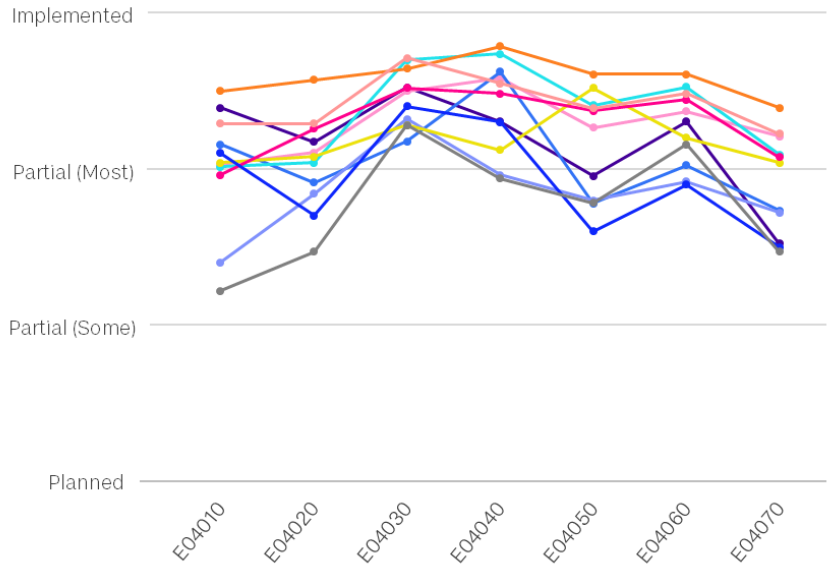


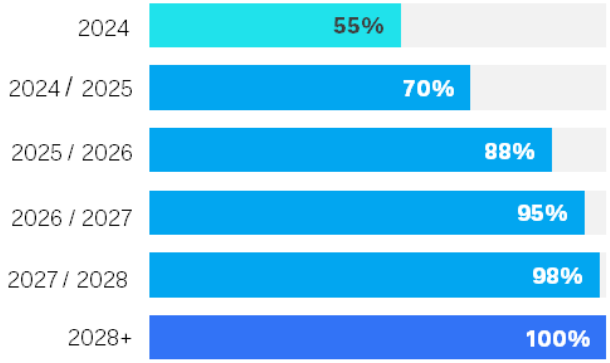
Figure 1.4.B
Average implementation status for Standard 4 elements by sector

Justice, Community and Emergency Services	Water Corporations and Catchments
Finance, Legal, and Administrative	Arts, Sport and Recreation
Health and Human Services	Departments
Industry and Transport	Environment and Land Management
Local Government	Regulatory and Integrity Bodies
Education	N = 360

Proposed completion dates

Figure 1.4.C represents the proposed timeline for the implementation of the remaining Standard 4 elements across the 360 reporting organisations. At the time of submission, 55% of applicable Standard 4 elements were reported as implemented with a slow implementation trajectory for the remaining elements.

Figure 1.4.C
Standard 4 - Current / projected implementation timeline



[22] E4.030 - *The organisation implements physical access controls (e.g., key management, swipe card access, visitor passes) based on the principles of least-privilege and need-to-know.*

E4.040 - *The organisation implements logical access controls (e.g., network account, password, two factor authentication) based on the principles of least-privilege and need-to-know.*

2022 and 2024 comparison

Average implementation status per element in Standard 4 (2022 v 2024)

Figure 1.4.D presents the average reported implementation status of all elements under Standard 4 across 2022 and 2024. It shows marginal change in reporting, year to year, across the 316 organisations.

OVIC anticipated a strong implementation status in 2024 given that 2022 reporting showed an average response rate of 'partial most'.

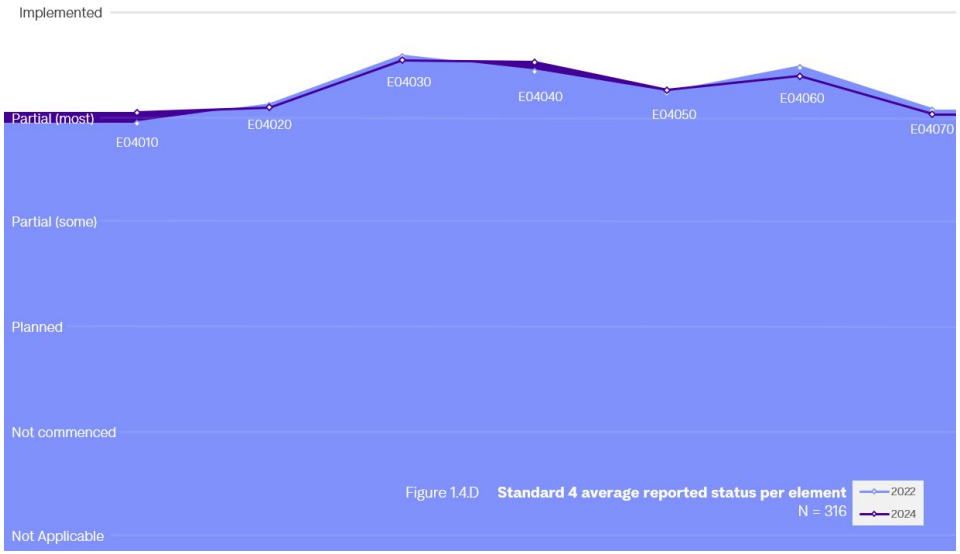


Figure 1.4.D **Standard 4 average reported status per element**
N = 316

Of note, the elements E4.010 and E4.020 are tracking lower than the remaining Standard 4 elements.[23] This may be reflective of organisations prioritising operational activities over governance and documentation aspects.

Responses for this standard appear to be tracking consistently across the 2 reporting cycles.

[23] E4.010 - *The organisation documents an identity and access management policy covering physical and logical access to public sector information based on the principles of least-privilege and need-to-know.*

E4.020 - *The organisation documents a process for managing identities and issuing secure credentials (registration and de-registration) for physical and logical access to public sector information.*

Comparison of Standard 4 elements reported as 'not applicable' (2022 v 2024)

Of the 316 organisations that reported in both 2022 and 2024, OVIC noted a 54% increase in the selection of 'not applicable' elements in 2024.

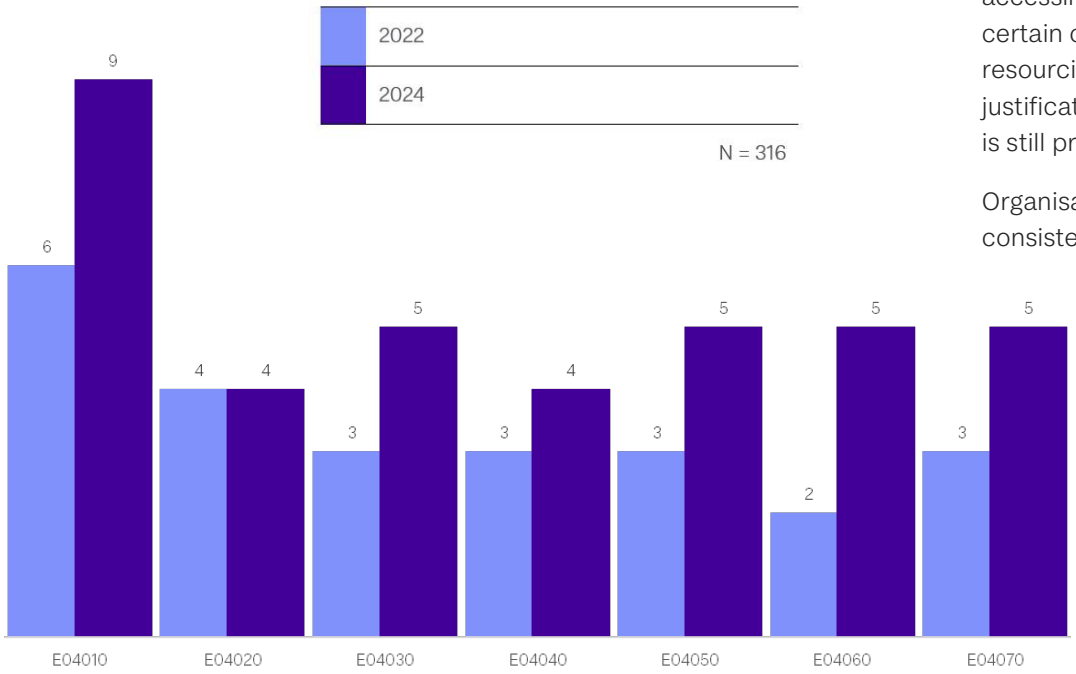
OVIC encourages organisations to reconsider the selection of 'not applicable' given how broadly relevant these elements are to all organisations.

It should be noted that some of the justifications supporting the selection of this status were not in line with instructions in the 2024 PDSP How-To Guide.[24] The selection of this status should be based upon the organisation determining there is no related information security risk that needs to be managed. However, this is highly unlikely for these elements which relate to accessing public sector information. Some of the justifications offered by certain organisations that reported 'not applicable' focused on a lack of resourcing and outsourced providers addressing these responsibilities. These justifications do not meet the criteria for the section of this status as the risk is still present and needs to be appropriately managed.

Organisations reporting 'not applicable' for these specific elements tended to consistently nominate 'not applicable' for elements under other Standards.

Figure 1.4.E

Count of organisations that selected 'Not Applicable' for Standard 4 elements



[24] 2024 PDSP How-To Guide, provided to organisations as part of the previous PDSP reporting cycle. This is an archived resource published by OVIC that provided instructions to organisations on completing a PDSP submission.

> *An organisation ensures all persons understand their responsibilities to protect public sector information.*

Overall implementation status for Standard 5

Figure 1.5.A shows the overall self-assessed implementation statuses for the 7 supporting elements under Standard 5. This Standard directs organisations to build a positive security culture with clear personal accountability. It also reinforces the importance of managing risk across day-to-day operations.

Organisations had a modest implementation rate with 48% of the elements under Standard 5 reported as implemented in 2024. The implementation status of this Standard is low as the activities associated may pose difficulties given tailoring of messaging to different cohorts, and dissemination methods to varied personnel numbers.

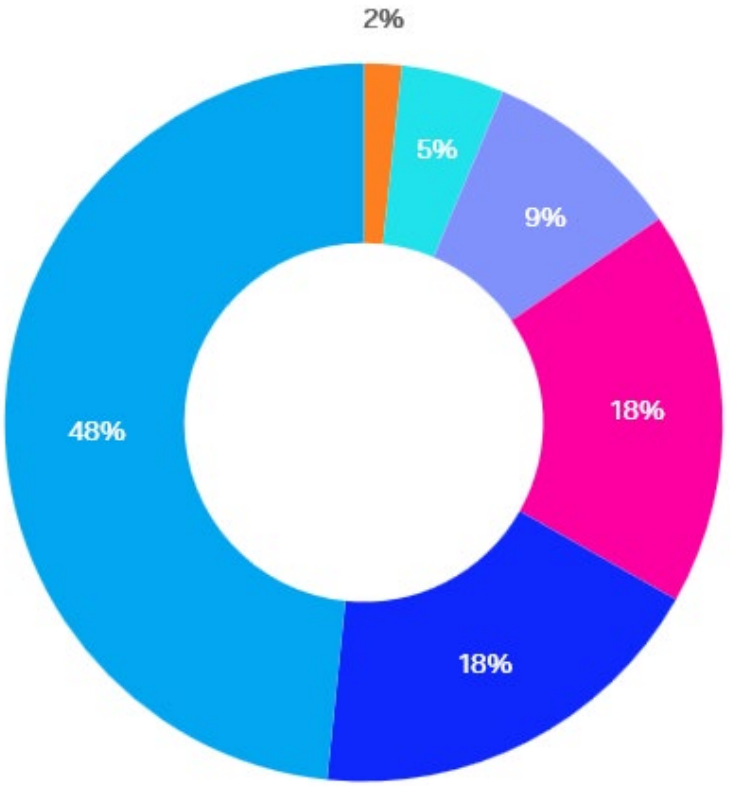


Figure 1.5.A
Reported implementation status of all Standard 5 elements

Implementation status per element by sector

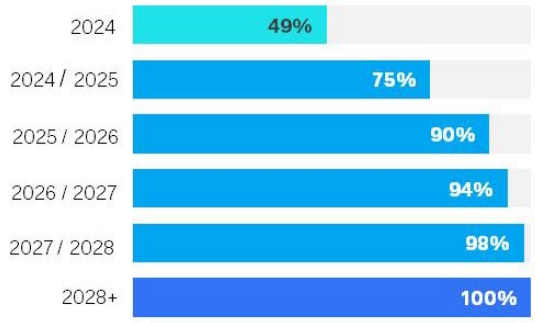
Figure 1.5.B shows the average reported status of each element under Standard 5 broken out by sector.

There appears to be a moderate reported rate of implementation across Standard 5 elements in all sectors. However, OVIC observed lower implementation statuses for the Industry and Transport, Departments, and Environment and Land Management sectors. Across the board, each of the sectors appear to struggle with implementation of E5.040.[25] This may point to challenges in identifying and providing targeted training to those individuals who perform high risk functions for the organisation or have specific security obligations.

Proposed completion dates

Figure 1.5.C represents the proposed timeline for the implementation of the remaining Standard 5 elements across the 360 reporting organisations. At the time of submission, 49% of applicable Standard 5 elements were reported as implemented. Three-quarters of the elements were projected to be implemented by 2024/2025.

Figure 1.5.C
Standard 5 - Current / projected implementation timeline



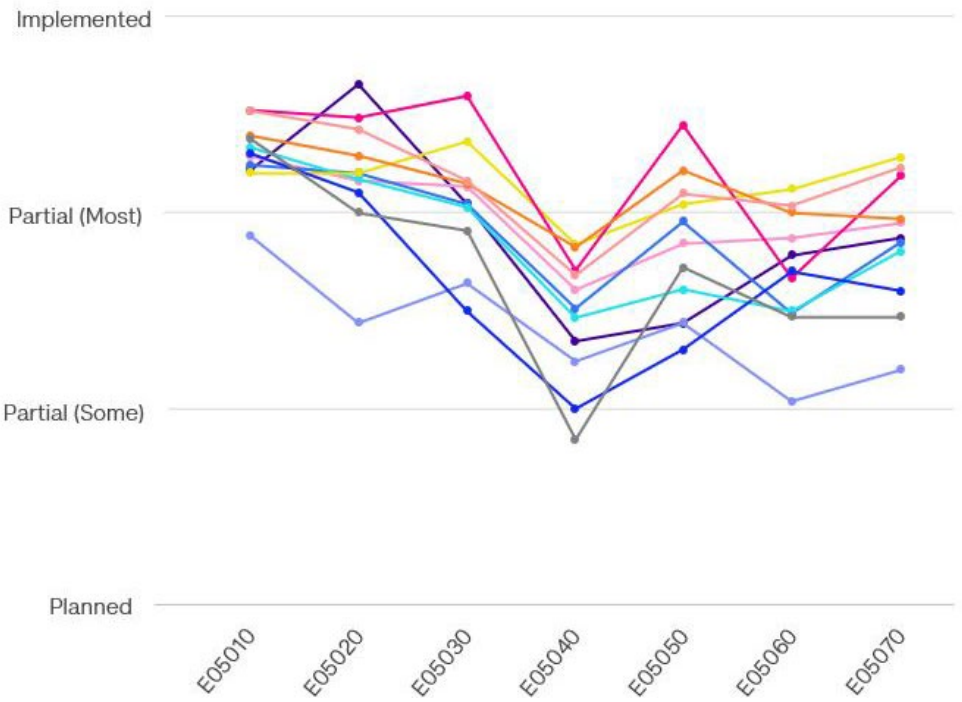


Figure 1.5.B
Average implementation status for Standard 5 elements by sector

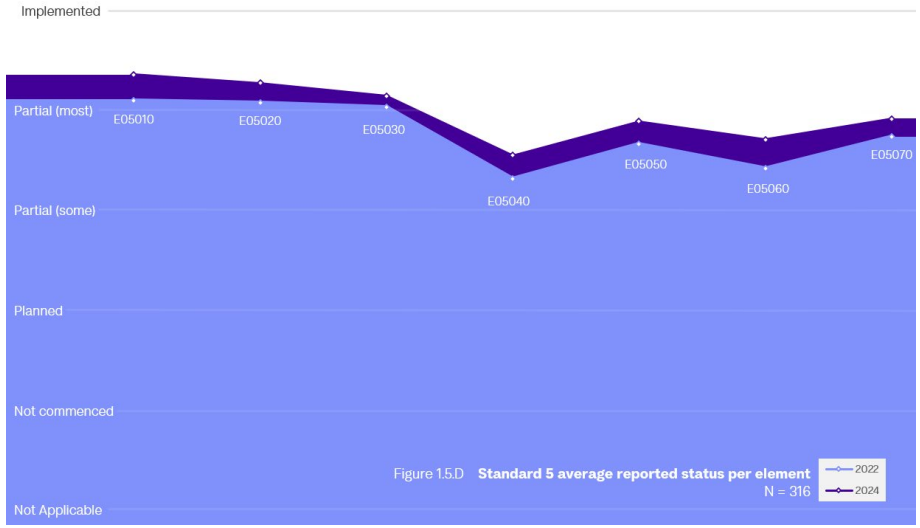
Justice, Community and Emergency Services	Water Corporations and Catchments
Finance, Legal, and Administrative	Arts, Sport and Recreation
Health and Human Services	Departments
Industry and Transport	Environment and Land Management
Local Government	Regulatory and Integrity Bodies
Education	N = 360

[25] E5.040 - *The organisation provides targeted information security training and awareness to persons in high-risk functions or who have specific security obligations (e.g., executives, executive assistants, procurement advisors, security practitioners, risk managers).*

2022 and 2024 comparison

Average implementation status per element in Standard 5 (2022 v 2024)

Figure 1.5.D presents the average reported implementation status of all elements under Standard 5 across 2022 and 2024. It shows an overall slight increase in the implementation status as expected. Responses for this Standard appear to be tracking consistently across the 2 reporting cycles.



Comparison of Standard 5 elements reported as 'not applicable' (2022 v 2024)

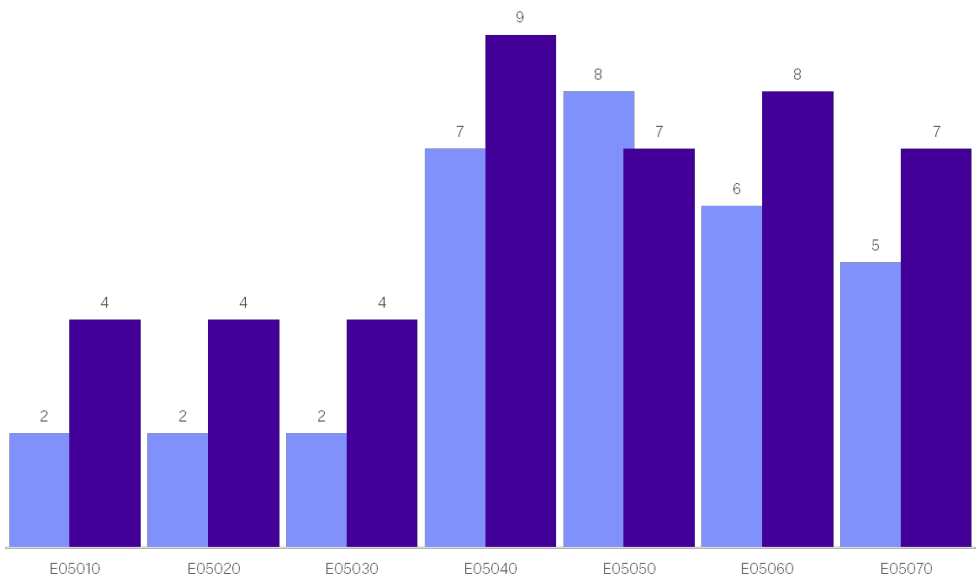
Of the 316 organisations that reported in both 2022 and 2024, OVIC noted a 34% increase in the selection of 'not applicable' in 2024. OVIC encourages organisations to reconsider the selection of 'not applicable' given the significance of these elements.

Some of the justifications supporting the selection of this status were not in line with instructions in the 2024 PDSP How-To Guide.[26] The selection of this status should be based upon the organisation determining there is no related information security risk that needs to be managed. However, this is highly unlikely for these elements given the broad reach of the Standard. (i.e., *all persons*). The justifications offered by certain organisations that reported 'not applicable' appeared to be influenced by a lack of understanding of the elements or a misinterpretation of the meaning of the status. Organisations must provide targeted security training and awareness to external personnel that offer support or services to that organisation. This includes situations where an organisation has limited internal personnel. These do not meet the criteria for the selection of this status as they do not negate the fact that the risk is still present and needs to be appropriately managed.

Organisations reporting 'not applicable' for these specific elements tended to consistently nominate 'not applicable' for elements under other Standards.

Figure 1.5.E

Count of organisations that selected 'Not Applicable' for Standard 5 elements



[26] 2024 PDSP How-To Guide, provided to organisations as part of the previous PDSP reporting cycle. This is an archived resource published by OVIC that provided instructions to organisations on completing a PDSP submission.

Standard 6 – Information Security Incident Management

> *An organisation establishes, implements and maintains an information security incident management process and plan relevant to its size, resources and risk posture.*

Overall implementation status for Standard 6

Figure 1.6.A shows the overall self-assessed implementation statuses selected for the 6 supporting elements under Standard 6. This standard requires organisations to apply a consistent approach for managing information security incidents in order to minimise harm and/or damage to government operations, organisations or individuals.

Organisations had a relatively strong implementation rate. 56% of the elements under Standard 6 were reported as implemented in 2024. Overall, this Standard has one of the highest reported implementation rates in 2024, suggesting organisations are prioritising incident management programs. This may be due to the number of high-profile security incidents seen over the last 2 years.

In conducting our analysis, OVIC observed that 69% of organisations reported E6.040 as implemented.[27] When asked to nominate how many information security incidents were recorded in their internal incident register over the preceding 24 months, 52% of these organisations also reported in the OPA that they had not experienced any incidents (reporting zero) or failed to provide a response at all.

The disparity points to either:

- challenges in the ability to identify, record and manage incidents in a register
- inaccurate implementation status (i.e. no established incident register), or
- a lack of verification of the responses offered in the OPA section of the PDSP.

Further discrepancies were identified in OPA responses where some organisations indicated they had not previously notified OVIC of incidents. However, upon review of internal OVIC records for the Scheme, those same organisations had been listed as notifying OVIC of an incident in the same period. OVIC encourages organisations to cross-check responses offered in their OPA with internal registers and validate any reported figures prior to submission.

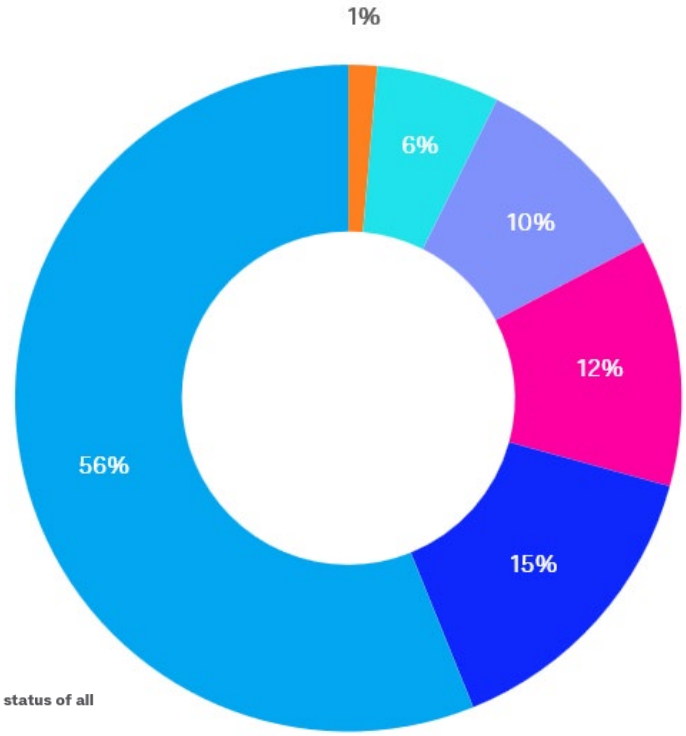


Figure 1.6.A
Reported implementation status of all Standard 6 elements

[27] E6.040 - *The organisation records information security incidents in a register.*

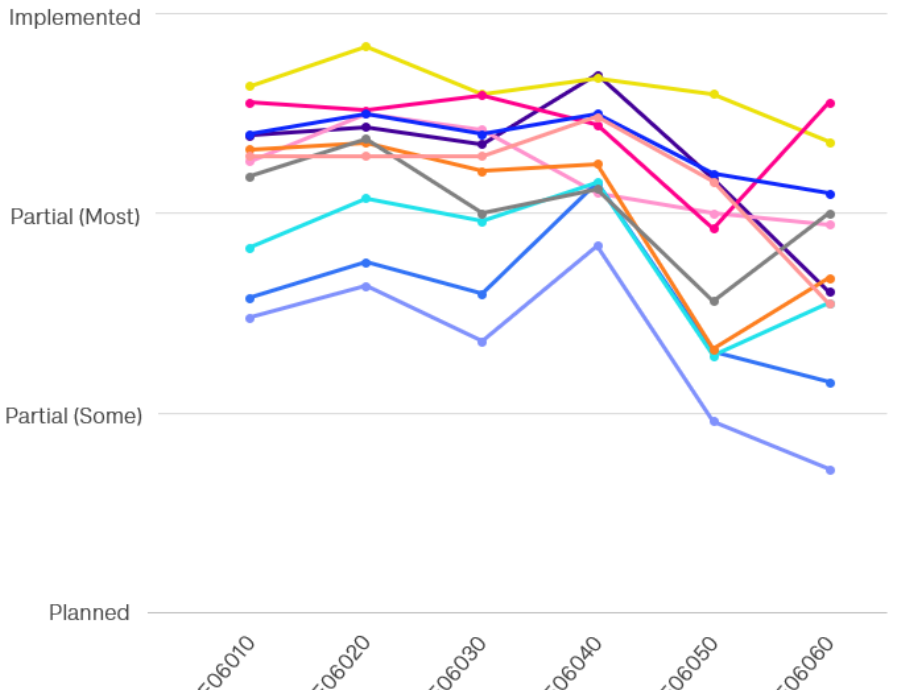


Figure 1.6.B
Average implementation status for Standard 6 elements by sector

Justice, Community and Emergency Services	Water Corporations and Catchments
Finance, Legal, and Administrative	Arts, Sport and Recreation
Health and Human Services	Departments
Industry and Transport	Environment and Land Management
Local Government	Regulatory and Integrity Bodies
Education	N = 360

Implementation status per element by sector

Figure 1.6.B shows the average reported status of each element under Standard 6 broken out by sector. There appears to be a strong reported rate of implementation across Standard 6 elements in the following sectors:

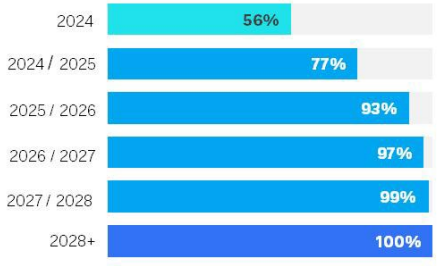
- the departments,
- Education, and
- Water Corporations and Catchment.

However, OVIC observed lower implementation for the Industry and Transport, and Health and Human Services sectors. Across the board, each of the sectors have a low implementation rate regarding the categorisation of incidents.[28] E6.050 was reported as the least implemented element for Standard 6.

Proposed completion dates

Figure 1.6.C represents the proposed timeline for the implementation of the remaining Standard 6 elements across the 360 reporting organisations. At the time of submission, 56% of applicable Standard 6 elements were reported as implemented with a 21% increase in implementation projected by 2024/2025. As referenced in the beginning of this Standard, OVIC's analysis indicates that implementation of this Standard appears to be a priority with close to all (99%) elements implemented by 2027/2028.

Figure 1.6.C
Standard 6 - Current / projected implementation timeline



[28] E6.050 - *The organisation's information security incident management procedures identify and categorise administrative (e.g., policy violation) incidents in contrast to criminal incidents (e.g., exfiltrating information to criminal associations) and investigative handover.*

2022 and 2024 comparison

Average implementation status per element in Standard 6 (2022 v 2024)

Figure 1.6.D presents the average reported implementation status of all elements under Standard 6 across 2022 and 2024. It shows an overall increase in the implementation status for the 316 organisations.

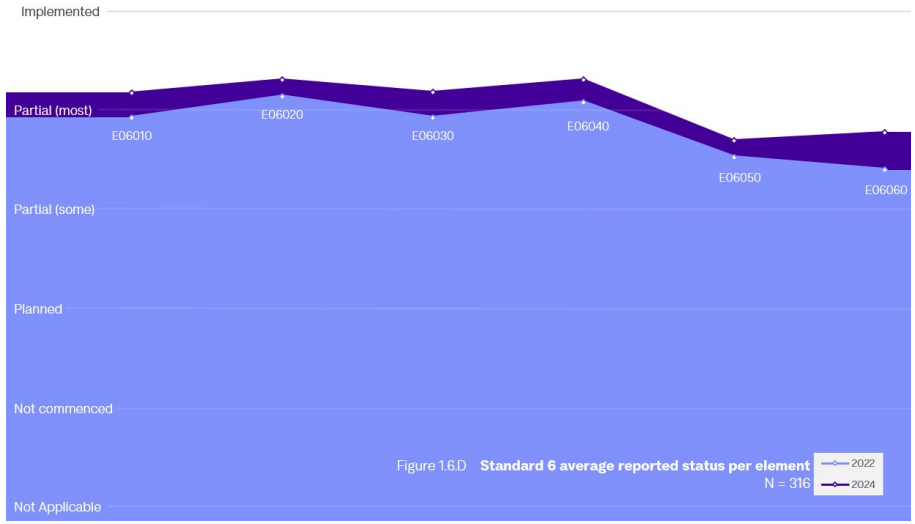


Figure 1.6.D **Standard 6 average reported status per element**
N = 316

OVIC notes that the implementation statuses of E6.050 and E6.060 are tracking lower than the remaining Standard 6 elements.[29] This may be reflective of a misunderstanding in the activities associated with these elements, that is, categorising incidents (e.g. criminal and administrative) and/or the ongoing nature of these activities. Responses for this Standard appear to be tracking consistently across the 2 reporting cycles.

Comparison of Standard 6 elements reported as 'not applicable' (2022 v 2024)

Of the 316 organisations that reported in both 2022 and 2024, OVIC noted a 67% increase in the selection of 'not applicable' in 2024. OVIC encourages organisations to reconsider the selection of 'not applicable' given the significance of these elements.

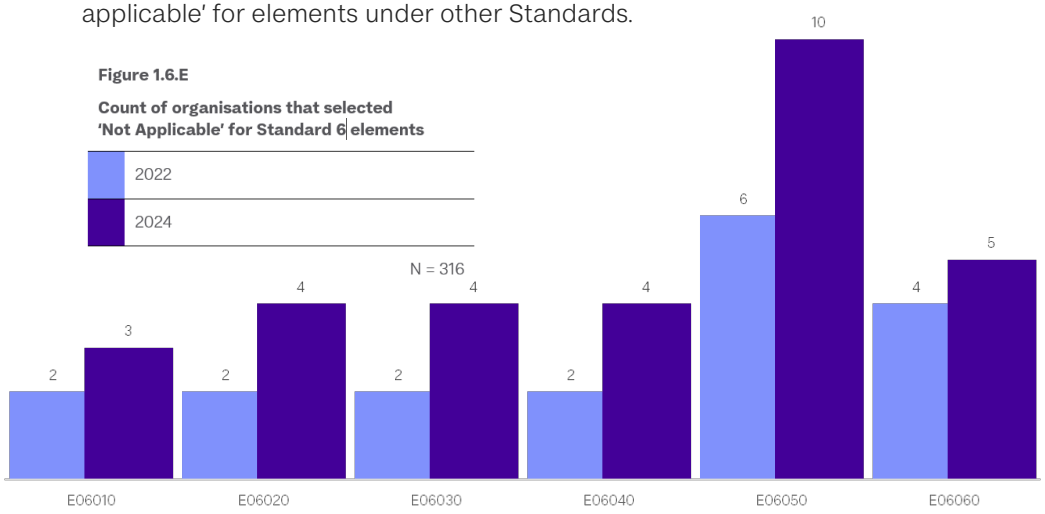
Some of the justifications supporting the selection of this status were not in line with instructions in the 2024 How-To Guide.[30] The selection of this status should be based upon the organisation determining there is no related information security risk that needs to be managed. However, this is highly unlikely for these elements. The justifications offered by certain organisations that reported 'not applicable' focused on:

- size of the organisation
- nature and functions of the organisation, and
- the misconception third parties are responsible for these activities.

These do not meet the criteria for selecting this status as the risk is still present and needs to be appropriately managed. Organisations reporting 'not applicable' for these specific elements tended to consistently nominate 'not applicable' for elements under other Standards.

Figure 1.6.E

Count of organisations that selected 'Not Applicable' for Standard 6 elements



[29] E6.060 - *The organisation regularly tests (e.g., annually) its incident response plan(s).*

[30] 2024 PDSP How-To Guide, provided to organisations as part of the previous PDSP reporting cycle. This is an archived resource published by OVIC that provided instructions to organisations on completing a PDSP submission.

Standard 7 – Information Security Aspects of Business Continuity and Disaster Recovery

> *An organisation embeds information security continuity in its business continuity and disaster recovery processes and plans.*

Overall implementation status for Standard 7

Figure 1.7.A shows the overall self-assessed implementation statuses were selected for the 3 supporting elements under Standard 7. While this Standard has a small number of supporting elements, the activities seek to enhance an organisation's capability to prevent, prepare, respond, manage and recover from any event that affects the confidentiality, integrity and/or availability of public sector information.

Standard 7 had one of the lowest implementation rates across the organisations. Given the Standard only has 3 elements, OVIC expected to see a slightly stronger implementation rate than 46% in 2024. Organisations should invest in better preparedness to ensure public sector information protections are continued when business continuity and disaster recovery plans need to be enacted. The update and maintenance of these plans is also critical to ensure their effectiveness during disruption.

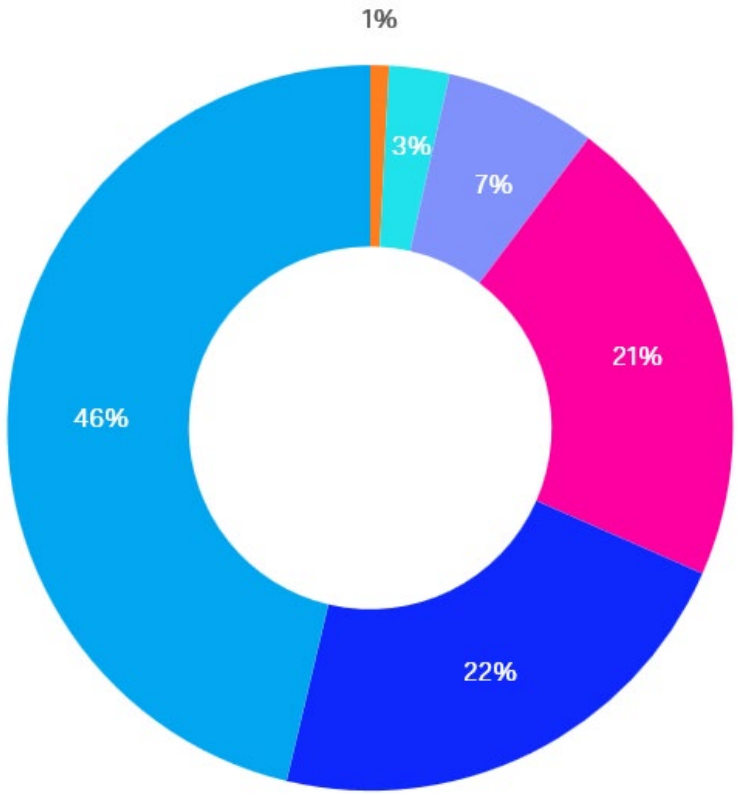


Figure 1.7.A
Reported implementation status of all Standard 7 elements

Implementation status per element by sector

Figure 1.7.B shows the average reported status of each element under Standard 7 broken out by sector. Compared to other Standards, there appears to be a somewhat low to moderate reported implementation status across Standard 7 elements, particularly in the Health and Human Services, Industry and Transport, Justice, Community and Emergency Services sectors as well as departments. This may be due to this Standard not being a key priority for these sectors.

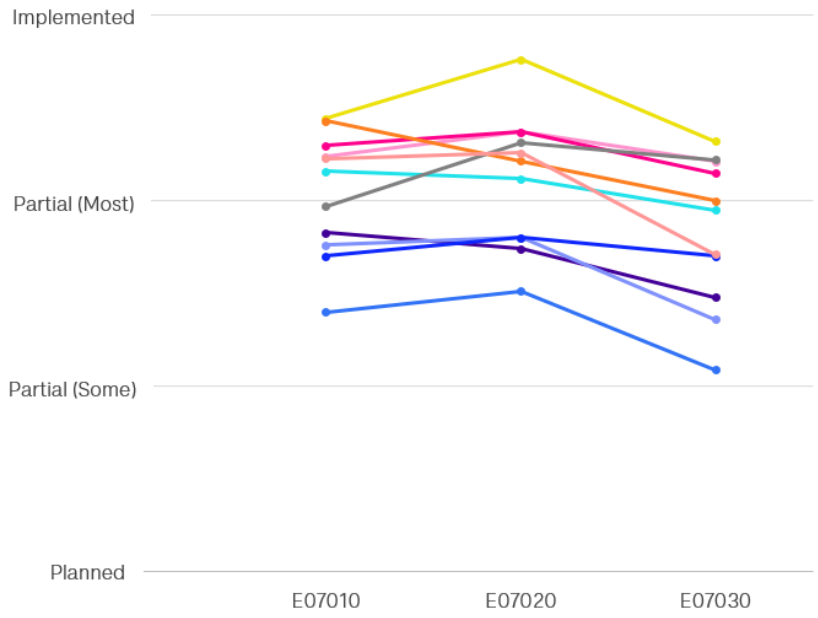


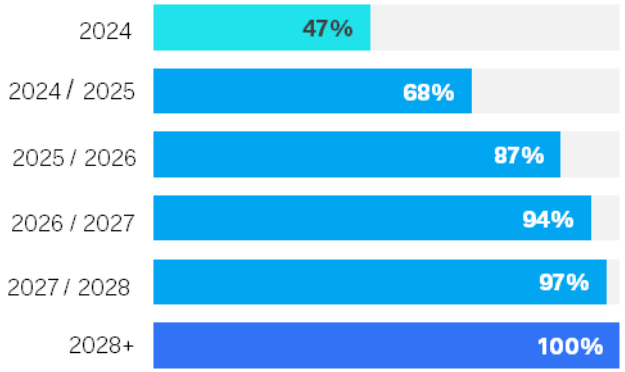
Figure 1.7.B
Average implementation status for Standard 7 elements by sector

Justice, Community and Emergency Services	Water Corporations and Catchments
Finance, Legal, and Administrative	Arts, Sport and Recreation
Health and Human Services	Departments
Industry and Transport	Environment and Land Management
Local Government	Regulatory and Integrity Bodies
Education	N = 360

Proposed completion dates

Figure 1.7.C represents the proposed timeline for the implementation of the remaining Standard 7 elements. 47% of applicable Standard 7 elements were reported as implemented with a 21% increase projected by 2024/2025. The slower implementation timeline may be due to the amount of documentation associated with these elements, coupled with the maintenance and operational testing of this documentation potentially posing a challenge for organisations.

Figure 1.7.C
Standard 7 - Current / projected implementation timeline



2022 and 2024 comparison

Average implementation status per element in Standard 7 (2022 v 2024)

Figure 1.7.D shows little increase in implementation status over a 2-year period. This contrasted with implementation timelines in *Figure 1.7.C* that show organisations' intention to increase implementation by 21% in a single year. When compared with previous implementation rates, this projected increase may be ambitious.

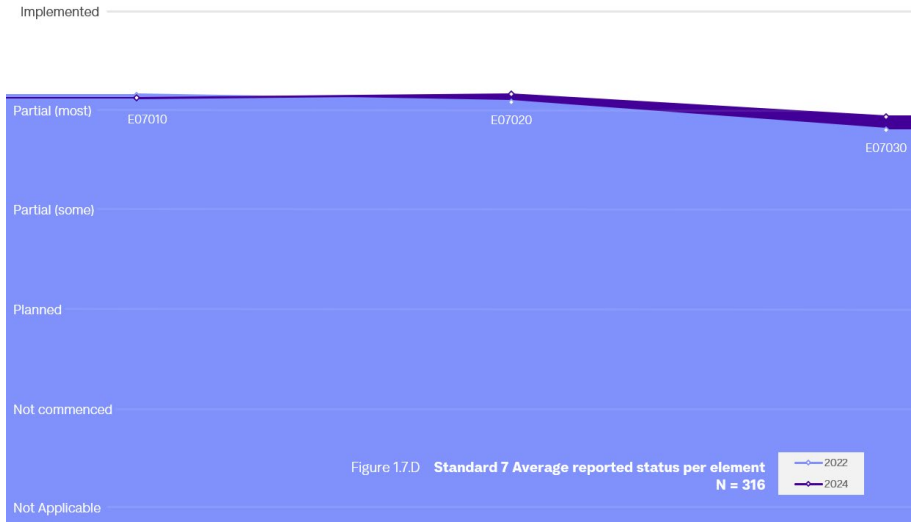


Figure 1.7.D **Standard 7 Average reported status per element N = 316**

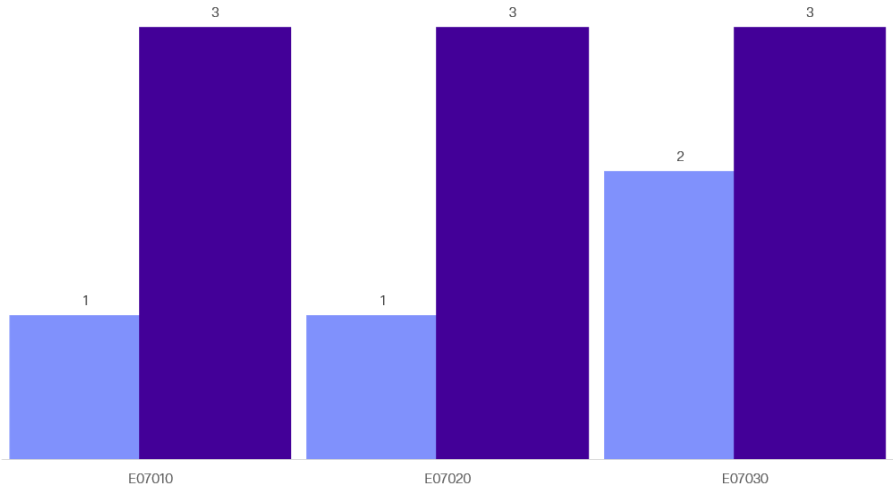
Comparison of Standard 7 elements reported as 'not applicable' (2022 v 2024)

Of the 316 organisations that reported in both 2022 and 2024, OVIC noted a 125% increase in the selection of 'not applicable' in 2024.

Similar commentary offered by OVIC are relevant in the reading of *Figure 1.7.E*. The organisations that reported 'not applicable' for elements, consistently nominated 'not applicable' for elements under other Standards.

Figure 1.7.E

Count of organisations that selected 'Not Applicable' for Standard 7 elements



Standard 8 – Third-party Arrangements

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

Overall implementation status for Standard 8

Figure 1.8.A shows the overall self-assessed implementation statuses selected for the 9 supporting elements under Standard 8. This Standard requires organisations to confirm that its public sector information is protected when it interacts with a third party. The Standard calls on organisations to consider information security risks when an organisation engages a third party, to ensure the public sector information held by the organisation remains protected.

Standard 8 had one of the lowest implementation rates across organisations with 43% of the elements implemented. This implementation rate is reflective of qualitative insights gained through the ISU's engagements with organisations and their understanding of third-party arrangements.

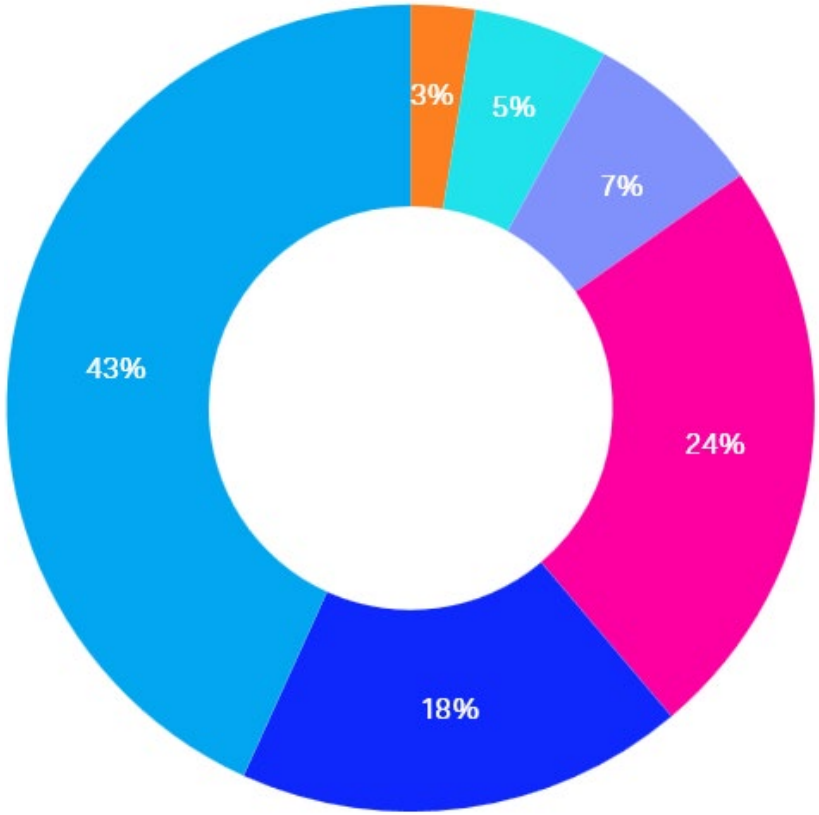


Figure 1.8.A
Reported implementation status of all Standard 8 elements

Implementation status per element by sector

Figure 1.8.B shows the average reported status of each element under Standard 8 broken out by sector.

There appears to be a strong reported rate of implementation across Standard 8 elements in the departments and Education sectors. As the primary source material for E8.070 refers to WoVG guidelines and DataVic access policy,[31] departments are expected to already have programs of work in-place that address these requirements. These programs would enable departments to record strong implementation statuses for this element.

Contrastingly, E8.060 offers lower implementation responses across most of the sectors which may be based upon the challenges associated with the ongoing management of the requirements associated with third-party engagements.[32] This sentiment is reflected in the Standard 8 Audit which is explored further in Chapter 3.

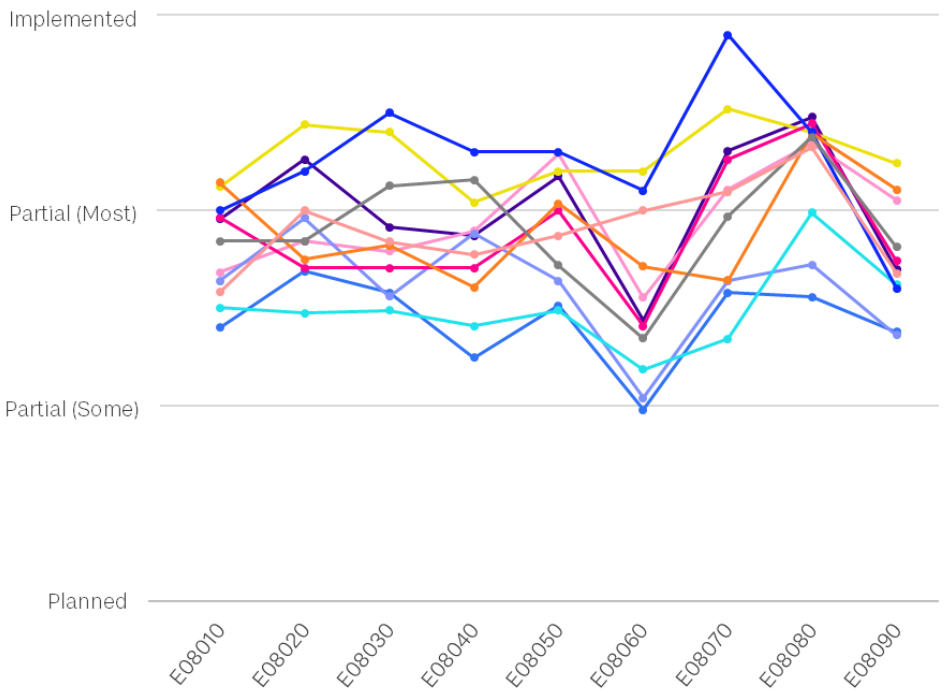


Figure 1.8.B
Average implementation status for Standard 8 elements by sector

Justice, Community and Emergency Services	Water Corporations and Catchments
Finance, Legal, and Administrative	Arts, Sport and Recreation
Health and Human Services	Departments
Industry and Transport	Environment and Land Management
Local Government	Regulatory and Integrity Bodies
Education	N = 360

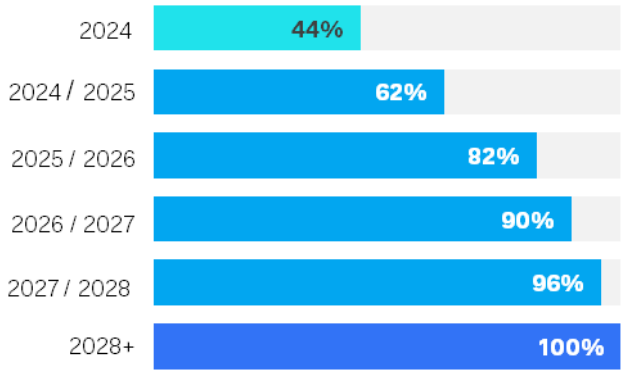
[31] E8.070 - *The organisation documents its information release management requirements (e.g., social media, news, DataVic).* (Primary Source material: IM-GUIDE-06 WoVG Information Management Governance Guidelines, § Custodianship model, DataVic access policy guidelines.)

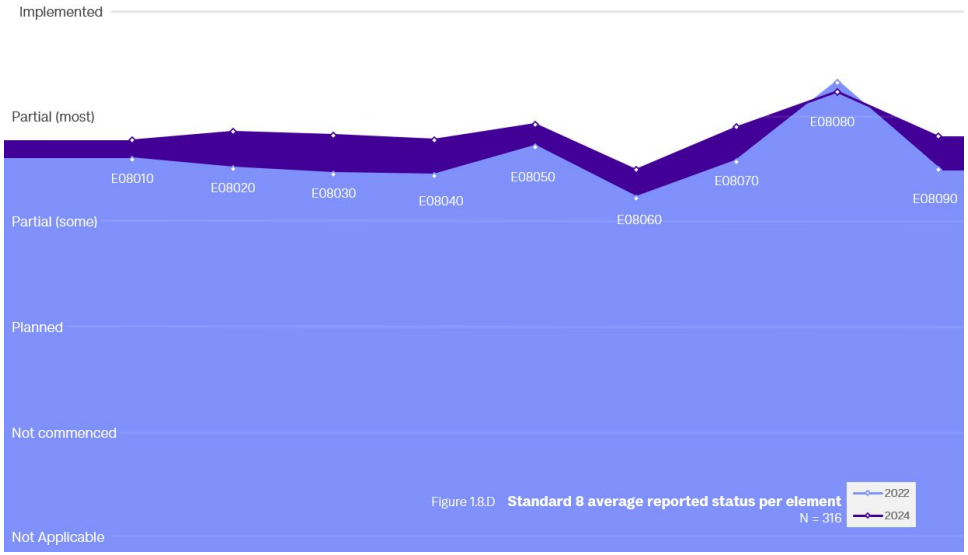
[32] E8.060 - *The organisation monitors, reviews, validates, and updates the information security requirements of third-party arrangements and activities.*

Proposed completion dates

Figure 1.8.C represents the proposed timeline for the implementation of the remaining Standard 8 elements across the 360 reporting organisations. At the time of submission, 44% of applicable Standard 8 elements were reported as implemented with an 18% increase in implementation projected by 2024/2025. Given the breadth and complexity of activities associated with this Standard, a slower proposed implementation timeline is understandable.

Figure 1.8.C
Standard 8 - Current / projected implementation timeline





2022 and 2024 comparison

Average implementation status per element in Standard 8 (2022 v 2024)

Figure 1.8.D presents the average reported implementation status of all elements under Standard 8 across 2022 and 2024. It shows a subtle increase in the majority of the implementation status selections for the 316 organisations.

OVIC notes the slight recalibration of E8.080 in 2024 which may follow an enhanced appreciation of the broad nature of the activities that could fall from this element. [33] However, supporting commentary relating to this particular element was not necessarily offered in 2024 PDSPs.

Responses for this Standard appear to be tracking relatively consistently across the 2 reporting cycles.

[33] E8.080 - *The organisation manages the delivery of maintenance activities and repairs (e.g., on-site, and off-site).*

Comparison of Standard 8 elements reported as 'not applicable' (2022 v 2024)

Of the 316 organisations that reported in both 2022 and 2024, OVIC noted a 69% increase in the selection of 'not applicable' in 2024. OVIC encourages organisations to review the Standard 8 Audit report and reconsider the applicability of the Standard 8 elements to their asset base and operating environment.

The selection of this status should be based upon the organisation determining there is no related information security risk that needs to be managed. This is highly unlikely for these elements. The justifications offered by certain organisations that reported 'not applicable' appeared to indicate some confusion around the relationship of third parties and the risk these entities pose to the engaging organisation's information. Whilst third parties are often relied upon to perform activities, functions or services of a VPS organisation, this outsourcing does not mean that the risk is transferred, rather, it needs to be appropriately managed by the VPS organisation.[34]

OVIC noted that the organisations reporting 'not applicable' for these specific elements tended to consistently nominate 'not applicable' for elements under other Standards as shown in *Figure 1.8.E*.

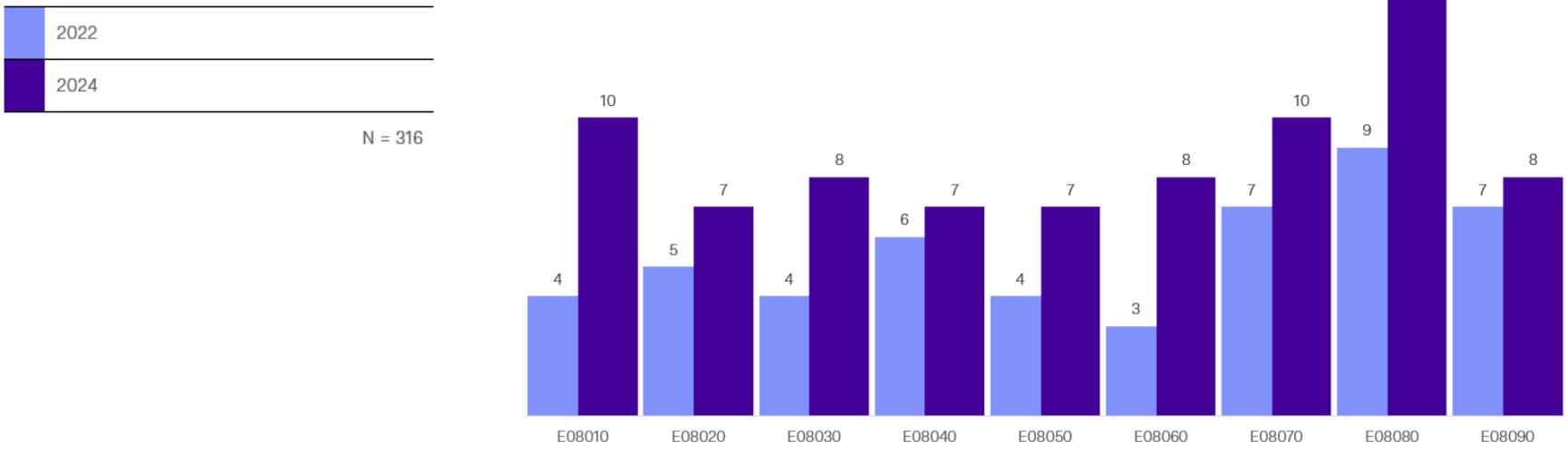
18% of organisations that reported 'not applicable' for these elements also provided conflicting responses in other sections of their PDSP. For example, they signalled the use of third parties in their:

- executive summary of the PDSP
- questions within the OPA section of the PDSP
- free-text fields supporting rationale in each of the Standards
- Generative Artificial Intelligence questions.

OVIC suggests organisations revisit their PDSP submissions if this theme is relevant and reconsider the importance of managing third-party risk.

Figure 1.8.E

Count of organisations that selected 'Not Applicable' for Standard 8 elements



[34] *Privacy and Data Protection Act 2014* (Vic), section 88(2).

Third-party exposure

Under the VPDSS, third parties are defined as

> *Any person or entity external to the organisation. This can include another organisation (public or private), a contracted service provider, or individual.*

Given the breadth of this definition the ongoing management of these third parties can be challenging and can lead to direct impacts on the engaging organisation. This is compounded by the large number of external organisations and suppliers that VPS organisations work with and rely upon.

Over 8,830 third-party arrangements were reported across 360 organisations' 2024 PDSPs. One department noted 1,276 third-party arrangements. Whilst these figures may initially seem quite high, OVIC places greater emphasis on reports from some organisations suggesting they had zero third-party arrangements, or an 'unknown' amount. This indicates a lack of visibility and due consideration of risks posed by third parties and fails to address key requirements under the PDP Act.[35]

OVIC appreciates the challenges in operating a third-party assurance program, however organisations need to invest in actively managing the risks that third parties introduce to try to prevent incidents from occurring or at least minimise their impacts. Third-party breaches continue to be a significant concern in the broader community, and these are often identified as a leading vulnerability of organisations' data given the lack of oversight.

Many organisations operate under the assumption that strong contract clauses address third-party risk. While useful, contracts are limited in their utility given the dynamic risk landscape in which VPS organisations operate. Changes to the third party (e.g. restructures, mergers or acquisitions) can render prior security risk assessments or contractual clauses outdated or irrelevant. This highlights the need for continuous third-party assurance.

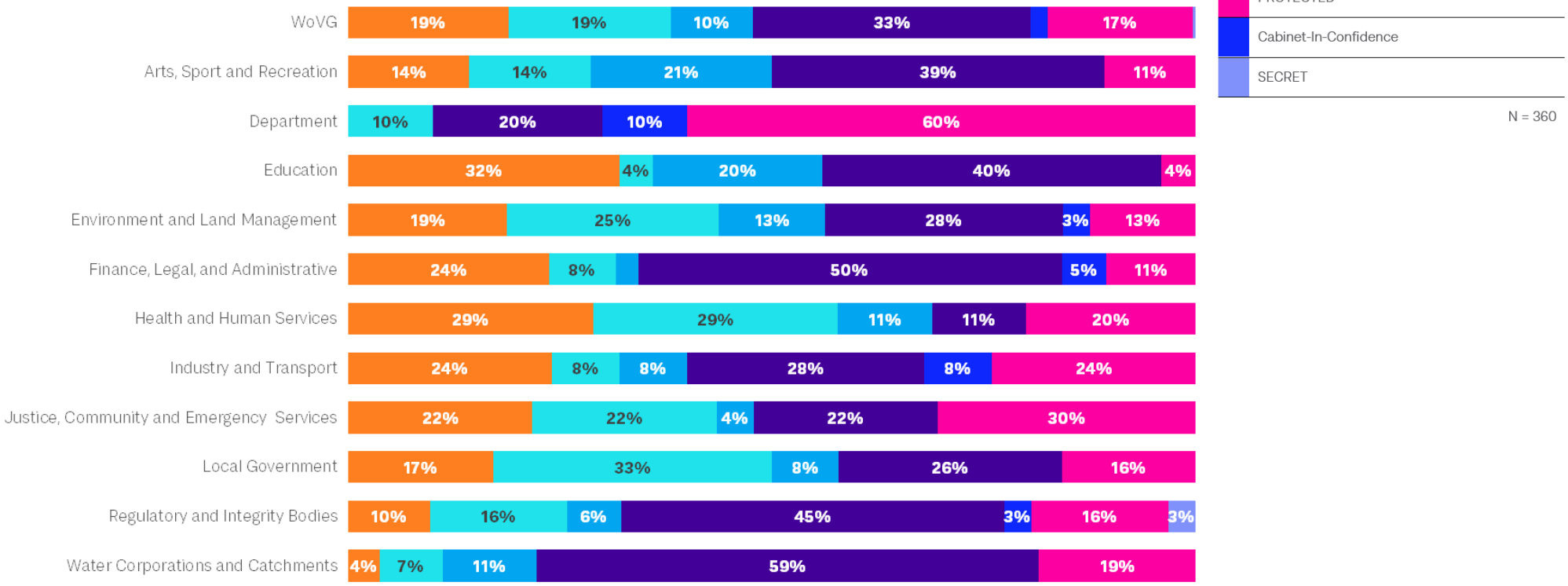
[35] *Privacy and Data Protection Act 2014* (Vic), sections 88(2), 89(2) and 89(3).

Figure 1.8.F highlights the considerable number of organisations that reported third parties as having direct access to sensitive information. This number is unsurprising given organisations' reliance upon third-party support to deliver essential services or undertake core functions.

In contrast, a high number of organisations reported being unaware of the level of direct access their third parties had to public sector information and systems. For the 69 organisations that reported 'unknown' on their PDSP, OVIC encourages critical consideration of how they intend to address this shortcoming and manage third-party risks.

Some organisations reported 'not applicable' for this question. OVIC interprets this response as those organisations believing their third parties did not have direct access to their information or systems. As referenced earlier under Standard 8 commentary, it would be rare for an organisation to have no third parties with direct access to their information and/or systems.

Figure 1.8.F
Highest protective marking accessed by organisations' third parties



N = 360

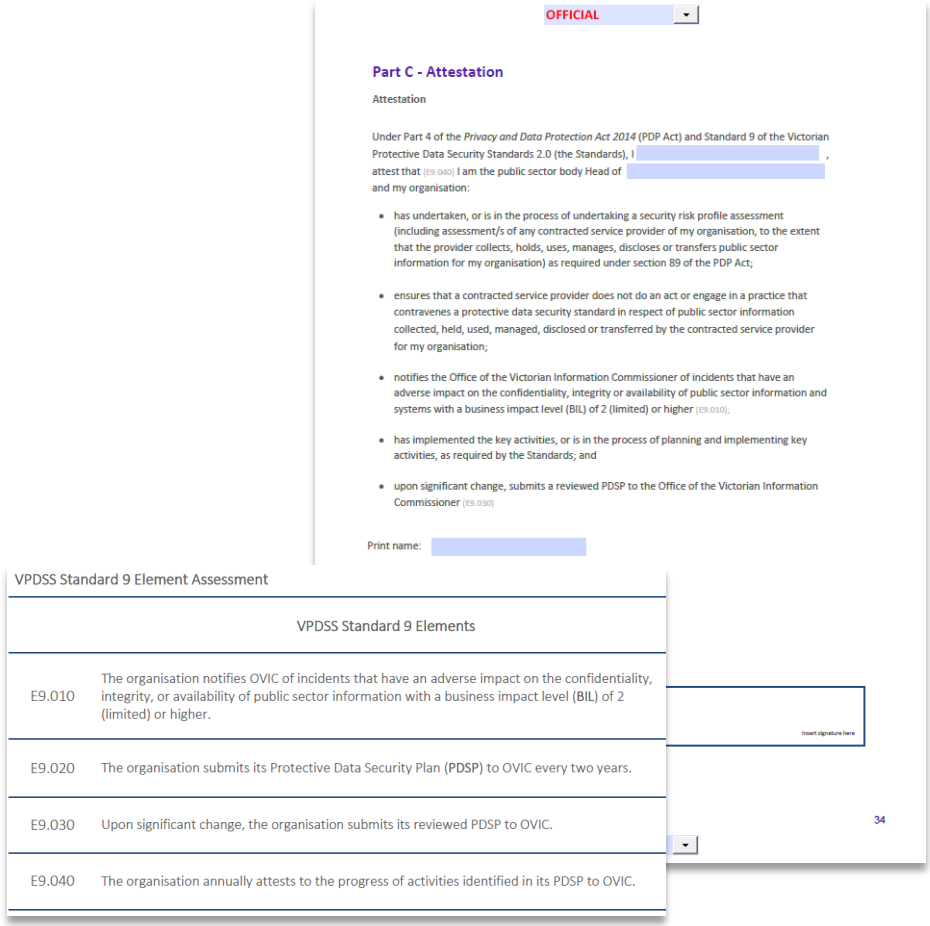
Standard 9 – Information Security Reporting to OVIC

> *An organisation regularly assesses its implementation of the Victorian Protective Data Security Standards (VPDSS) and reports to the Office of the Victorian Information Commissioner (OVIC).*

This Standard contains elements that outline organisations' statutory obligations under Part 4 of the PDP Act, namely the act of submitting a copy of the PDSP to OVIC every 2 years and upon any significant change to the organisation.

It also outlines that an organisation should notify OVIC of security incidents under the incident notification scheme as well as attest annually to the progress of its activities outlined in its previous PDSP.

As these elements are also detailed in the attestation and signed by the nominated agency head, all supporting activities are relevant and considered implemented.



OFFICIAL

Part C - Attestation

Attestation

Under Part 4 of the *Privacy and Data Protection Act 2014* (PDP Act) and Standard 9 of the Victorian Protective Data Security Standards 2.0 (the Standards), I _____, attest that (E9.040) I am the public sector body Head of _____ and my organisation:

- has undertaken, or is in the process of undertaking a security risk profile assessment (including assessment/s of any contracted service provider of my organisation, to the extent that the provider collects, holds, uses, manages, discloses or transfers public sector information for my organisation) as required under section 89 of the PDP Act;
- ensures that a contracted service provider does not do an act or engage in a practice that contravenes a protective data security standard in respect of public sector information collected, held, used, managed, disclosed or transferred by the contracted service provider for my organisation;
- notifies the Office of the Victorian Information Commissioner of incidents that have an adverse impact on the confidentiality, integrity or availability of public sector information and systems with a business impact level (BIL) of 2 (limited) or higher (E9.010);
- has implemented the key activities, or is in the process of planning and implementing key activities, as required by the Standards; and
- upon significant change, submits a reviewed PDSP to the Office of the Victorian Information Commissioner (E9.030)

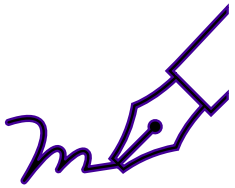
Print name: _____

Insert signature here

34

VPDSS Standard 9 Element Assessment

	VPDSS Standard 9 Elements
E9.010	The organisation notifies OVIC of incidents that have an adverse impact on the confidentiality, integrity, or availability of public sector information with a business impact level (BIL) of 2 (limited) or higher.
E9.020	The organisation submits its Protective Data Security Plan (PDSP) to OVIC every two years.
E9.030	Upon significant change, the organisation submits its reviewed PDSP to OVIC.
E9.040	The organisation annually attests to the progress of activities identified in its PDSP to OVIC.



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.*

VPS organisations employ and engage many thousands of individuals responsible for delivering services and carrying out a wide array of functions on their behalf. Standard 10 requires organisations to mitigate personnel security risks by assessing the continued eligibility and suitability of personnel with access to public sector information.

Overall implementation status for Standard 10

Figure 1.10.A shows the overall self-assessed implementation statuses selected for the 8 supporting elements under Standard 10. While there are only 8 elements under the Standard, each element presents multiple requirements and has its own associated work program. This may account for additional work to be done in this space - 32% of applicable elements are yet to be implemented. Organisations reported a modest implementation rate with 50% of the elements under Standard 10 assessed as implemented in 2024. Of note, 18% of the elements under Standard 10 were reported as being 'not applicable'. This theme will be discussed at *Figure 1.10.E*.

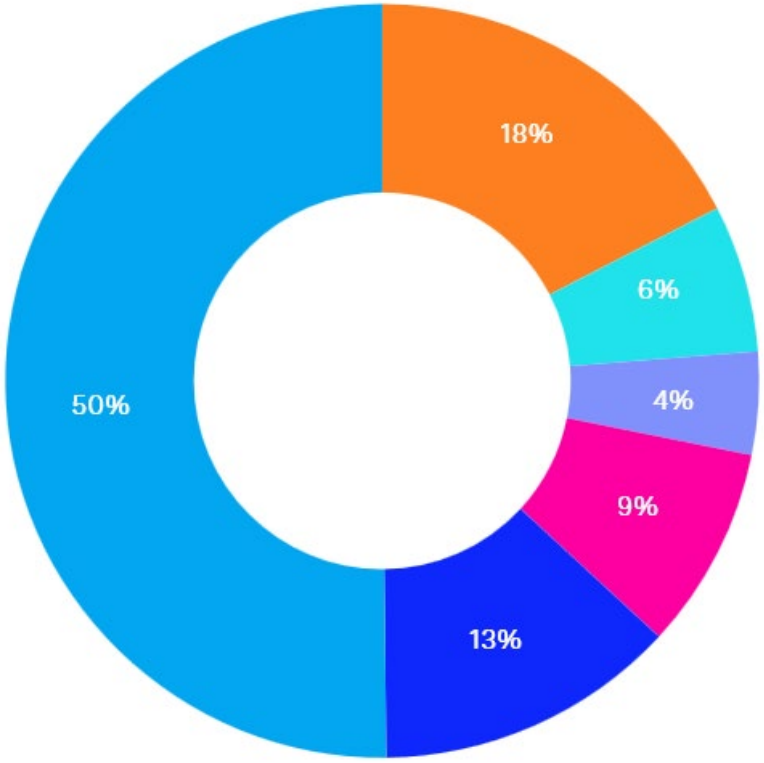


Figure 1.10.A
Reported implementation status of all Standard 10 elements

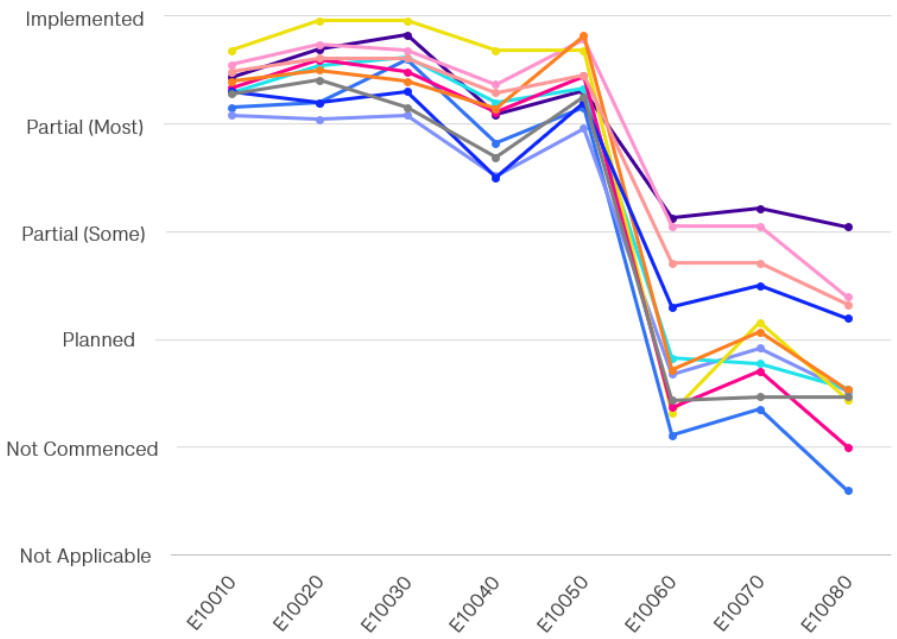


Figure 1.10.B
Average implementation status for Standard 10 elements by sector

Justice, Community and Emergency Services	Water Corporations and Catchments
Finance, Legal, and Administrative	Arts, Sport and Recreation
Health and Human Services	Departments
Industry and Transport	Environment and Land Management
Local Government	Regulatory and Integrity Bodies
Education	N = 360

Implementation status per element by sector

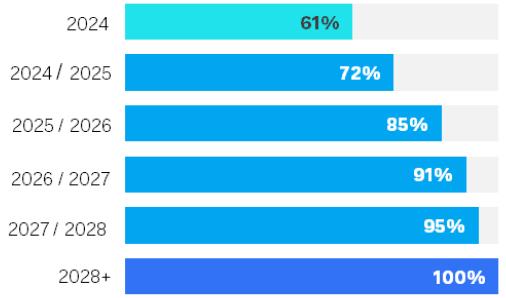
Figure 1.10.B shows the average reported status of each element under Standard 10 broken out by sector.

As depicted in *Figure 1.10.B,* most sectors appeared comfortable with the application of the first 5 elements. However, E10.060, E10.070 and E10.080 under Standard 10 featured a variety of implementation responses.[36] This correlation is due to the features of those 3 elements being associated with roles requiring additional screening based on high-assurance functions and/or handling security classified information.

Proposed completion dates

Figure 1.10.C represents the proposed timeline for the implementation of the remaining Standard 10 elements across the 360 reporting organisations. At the time of submission, 61% of applicable Standard 10 elements were reported as implemented with an 11% increase in implementation projected by 2024/2025. This statistic presents the highest implementation response rate for any of the Standards in 2024.

Figure 1.10.C
Standard 10 - Current / projected implementation timeline



[36] E10.060 - *The organisation develops security clearance policies and procedures to support roles requiring high assurance and/ or handling security classified information.*
E10.070 - *The organisation undertakes additional personnel screening measures commensurate with the risk to support roles requiring high assurance and/ or handling security classified information.*
E10.080 - *The organisation actively monitors and manages security clearance holders.*

2022 and 2024 comparison

Average implementation status per element in Standard 10 (2022 v 2024)

Figure 1.10.D presents the average reported implementation status of all elements under Standard 10 across 2022 and 2024. It shows an overall increase in the implementation status for the first 5 elements.

OVIC notes that the implementation status of E10.060, E10.070 and E10.080 in 2024 are tracking lower than the remaining Standard 10 elements.[37] This may be due to organisations reflecting on outcomes from the Standard 10 Audit, in particular, analysis and recommendations relating to high assurance functions and/or those accessing security classified information, or increased selection of 'not applicable' as seen in the *Figure 1.10.E*.

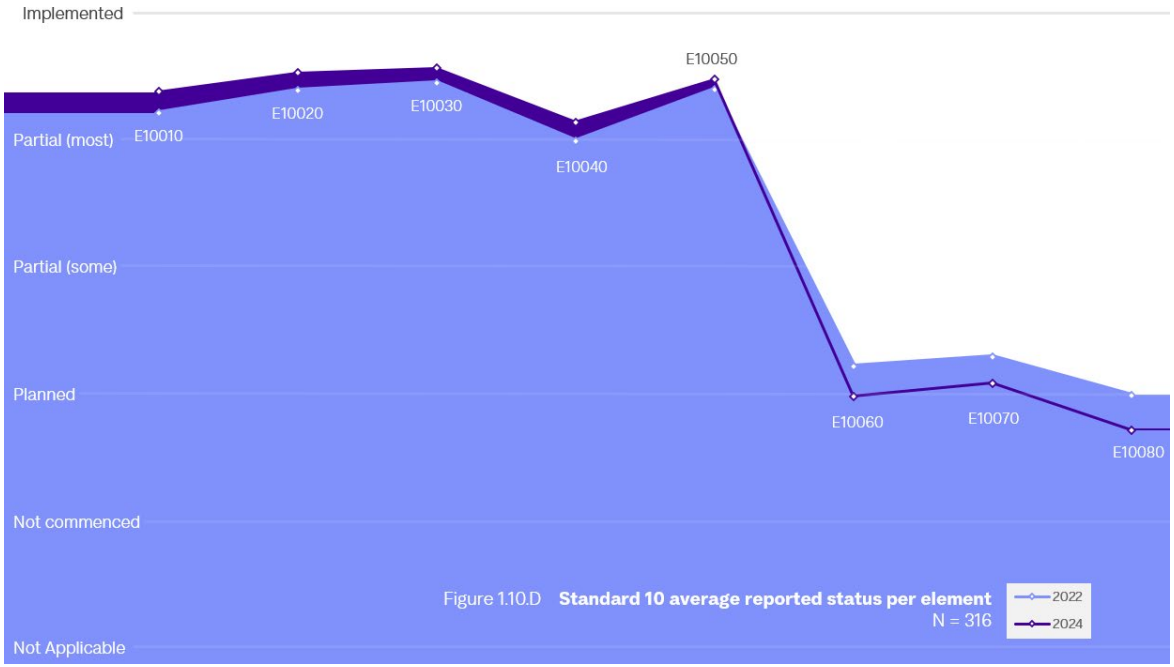


Figure 1.10.D **Standard 10 average reported status per element**
N = 316

[37] E10.060 - *The organisation develops security clearance policies and procedures to support roles requiring high assurance and/ or handling security classified information.*
E10.070 - *The organisation undertakes additional personnel screening measures commensurate with the risk to support roles requiring high assurance and/ or handling security classified information.*
E10.080 - *The organisation actively monitors and manages security clearance holders.*

Comparison of Standard 10 elements reported as 'not applicable' (2022 v 2024)

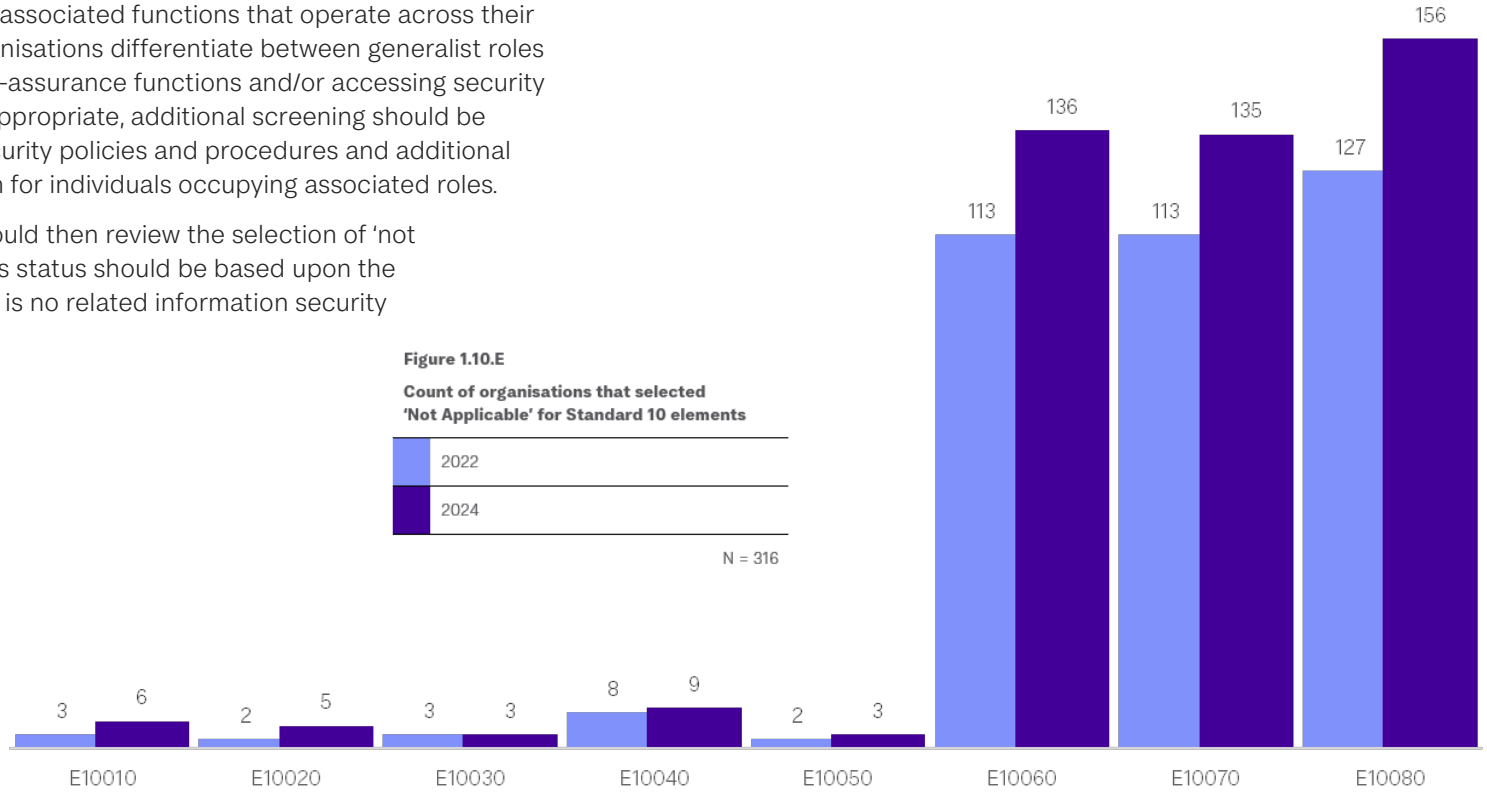
Of the 316 organisations that reported in both 2022 and 2024, OVIC noted a 22% increase in the selection of 'not applicable' in 2024. This, however, does not account for the large number of responses for the last 3 elements under the Standard. The significant number of organisations nominating E10.060, E10.070 and E10.080 as 'not applicable' potentially reflects a limited understanding of what is being described under these elements and the risks they seek to mitigate.

As highlighted in the Standard 10 audit undertaken by OVIC, [38] organisations are encouraged to undertake a workforce review and critically consider the risk profile of the various roles and associated functions that operate across their organisation. This will help organisations differentiate between generalist roles and those associated with high-assurance functions and/or accessing security classified information. Where appropriate, additional screening should be accounted for in personnel security policies and procedures and additional screening activities undertaken for individuals occupying associated roles.

Following this, organisations would then review the selection of 'not applicable'. The selection of this status should be based upon the organisation determining there is no related information security risk that needs to be managed.

Figure 1.10.E

Count of organisations that selected 'Not Applicable' for Standard 10 elements



[38] The full Standard 10 audit (pre-engagement phase of personnel security) can be accessed here https://ovic.vic.gov.au/wp-content/uploads/2024/04/Standard-10-Audit-Report-OVIC-02042024-C.pdf

Standard 11 – Information Communications Technology (ICT) Security

> *An organisation establishes, implements and maintains Information Communications Technology security controls.*

Traditionally, information security has been closely associated with Information and Communication Technology (**ICT**)/cyber security. Historical PDSP reporting to OVIC tends to reflect this with ICT areas of the organisation being responsible for, or driving, the VPDSS program on its behalf. Given this association, OVIC has observed VPDSS implementation programs focussing on data, potentially due to the framing and terminology used in Part 4 of the Act. Consequently, Standard 11 appears to have had dedicated resources applied to the supporting programs as reflected in the following statistics.

This relationship is represented in data taken from the OPA section in the PDSP where OVIC asks which part of the organisation the ongoing management of the information security program resides. Whilst there was a swing away from explicit nomination of ICT as the managing area, there was an increase in the selection of information security and corporate services which OVIC notes as typically including ICT/cyber resources.

Overall implementation status for Standard 11

Figure 1.11.A shows the overall self-assessed implementation statuses selected for the 20 supporting elements under Standard 11. This Standard requires organisations to protect public sector information by implementing ICT controls to maintain secure systems.

Organisations had a relatively strong implementation rate, with 54% of the elements under Standard 11 reported as implemented in 2024. Given the broad range of elements under this Standard, OVIC is encouraged to see an additional 36% of elements reportedly underway.

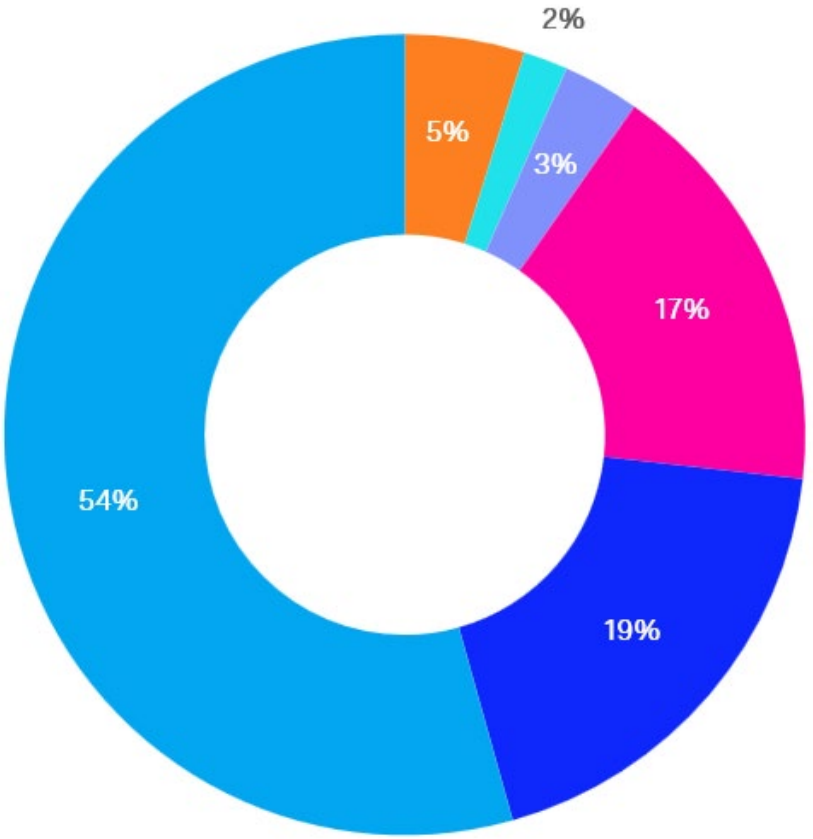


Figure 1.11.A
Reported implementation status of all Standard 11 elements

Implementation status per element by sector

Figure 1.11.B shows the average reported status of each element under Standard 11 broken out by sector.

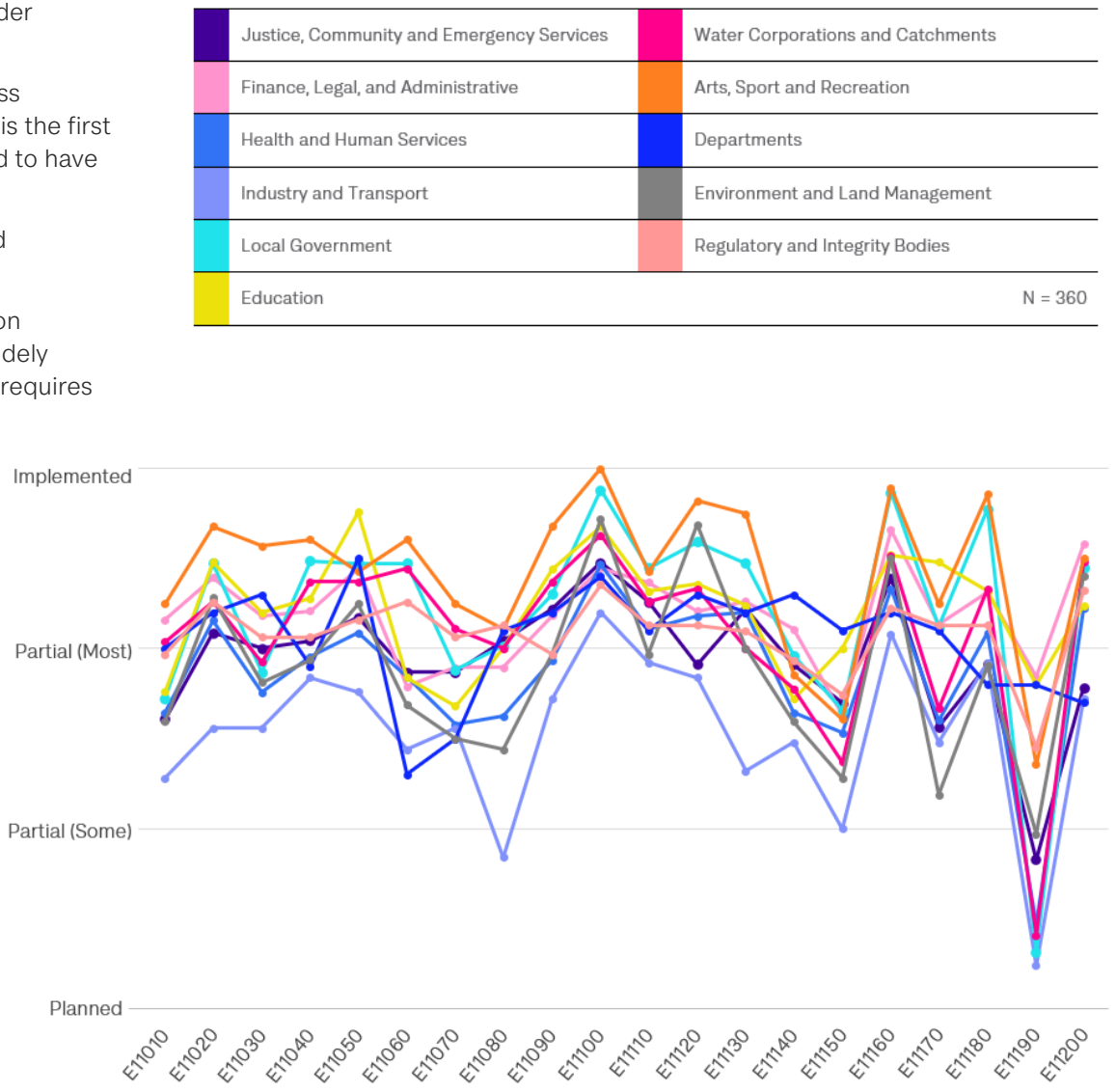
There appears to be a strong reported rate of implementation across Standard 11 elements in the Local Government sector. Notably, this is the first Standard where the Arts, Sport and Recreation sector has appeared to have reported relatively strongly across the whole Standard.

Contrastingly, OVIC observed lower implementation for Industry and Transport, and Environment and Land Management sectors.

Across the board, each of the sectors reported lower implementation statuses for E11.190. This is further evidenced in it being the most widely selected 'not applicable' element across the VPDSS.[39] This element requires organisations manage the secure development lifecycle for all ICT development activities which many organisations may misconstrue as not being a risk they need to manage. However, this element comes into play even when purchasing and implementing commercial off the shelf products, available via Victorian government selection panels, as some form of customisation is generally required.

In addition to this, an outlier in the data presented above for E11.080 suggests more work needs to be done in the Industry and Transport sector around the management of security measures for media given the relatively low reported implementation status.[40]

Figure 1.11.B
Average implementation status for Standard 11 elements by sector



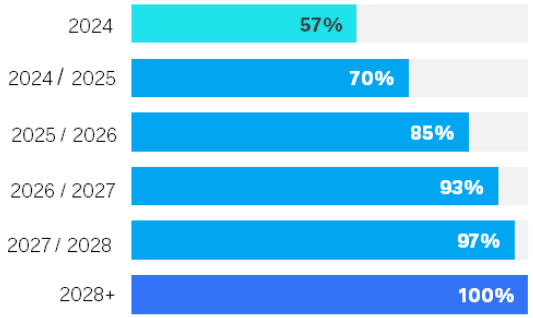
[39] E11.190 - *The organisation manages a secure development lifecycle covering all development activities (e.g., software, web-based applications, operational technology (Supervisory Control and Data Acquisition/ Industrial Control Systems (SCADA/ICS)).*

[40] E11.080 - *The organisation manages security measures (e.g., classification, labelling, usage, sanitisation, destruction, disposal) for media.*

Proposed completion dates

Figure 1.11.C represents the proposed timeline for the implementation of the remaining applicable Standard 11 elements. At the time of submission, 57% of Standard 11 elements were reported as implemented with a 13% increase projected by 2024/2025. This presents a rather tempered response by organisations which may be due to VPS budget constraints by a 14% increase in reported financial challenges as seen in the OPA section of the 2024 PDSP.

Figure 1.11.C
Standard 11 - Current / projected implementation timeline



2022 and 2024 comparison

Average implementation status per element in Standard 11 (2022 v 2024)

Figure 1.11.D presents the average reported implementation status of all elements under Standard 11 across 2022 and 2024 for the 316 organisations.

The graph shows a very consistent implementation rate across the 2 reporting periods with little deviation between the years.

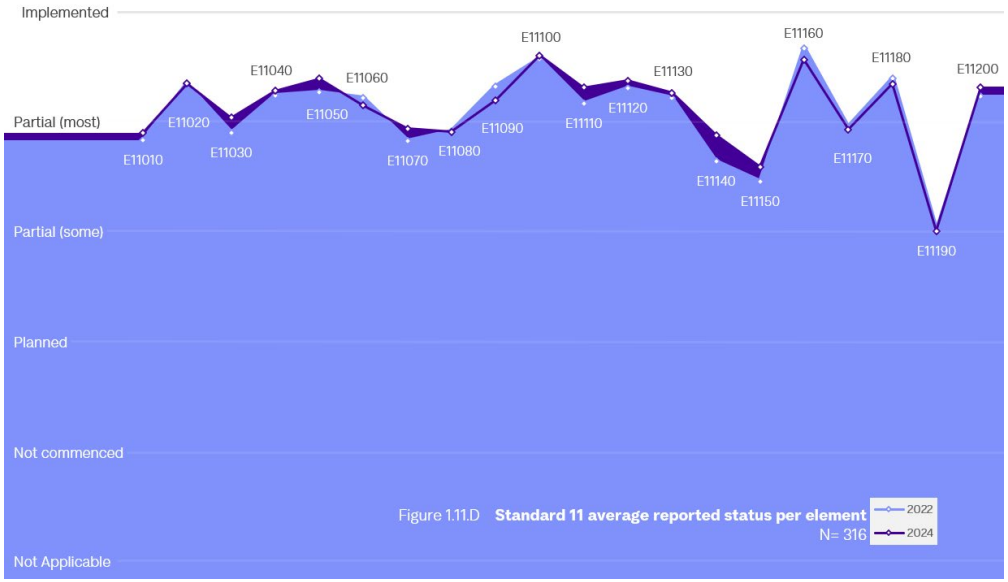


Figure 1.11.D **Standard 11 average reported status per element**
N= 316

Comparison of Standard 11 elements reported as 'not applicable' (2022 v 2024)

Of the 316 organisations that reported in both 2022 and 2024, OVIC noted an 18% increase in the selection of 'not applicable' in 2024.

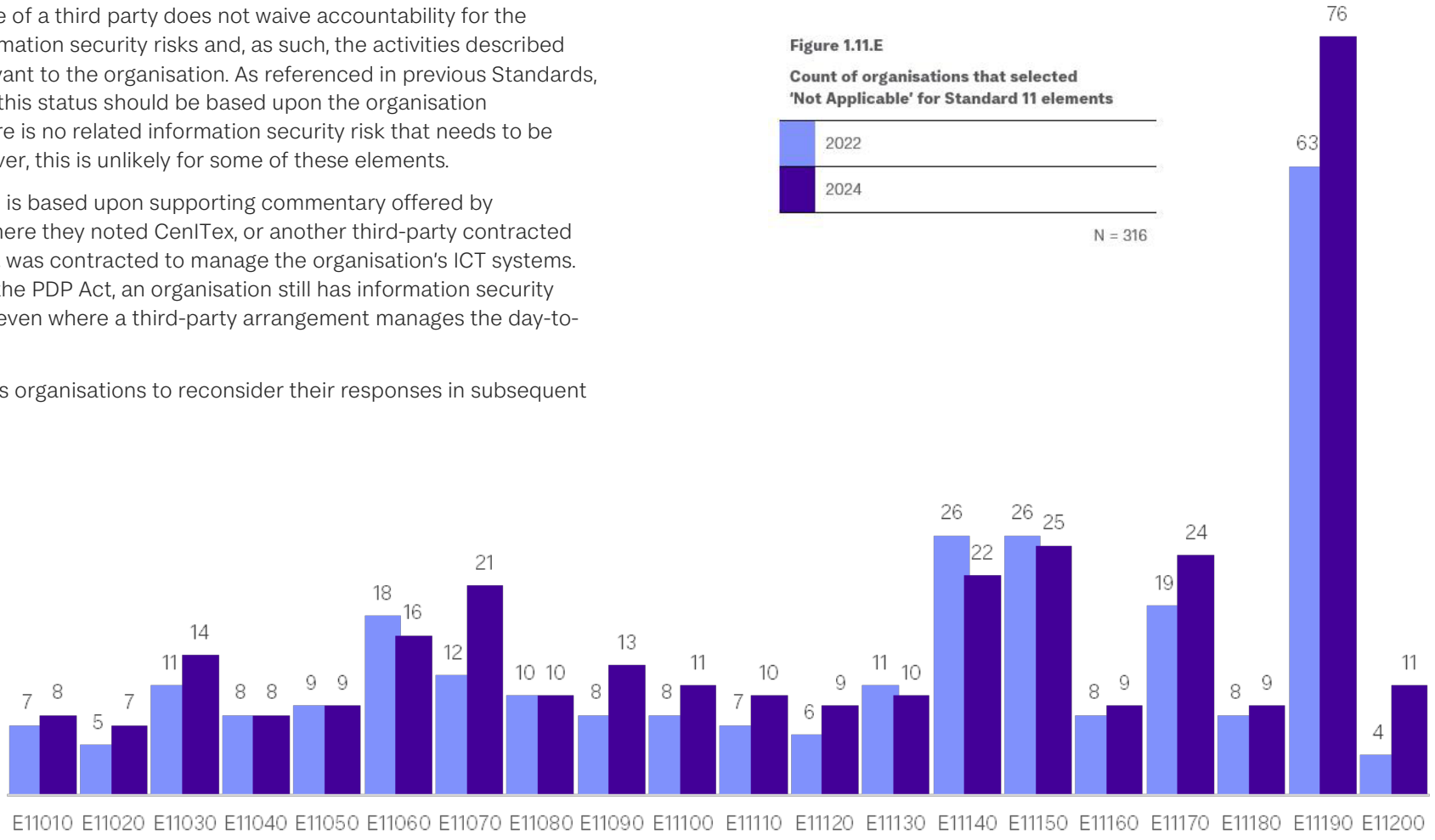
An increase in the number of organisations nominating E11.030, E11.070, E11.170, E11.190 and E11.200 as 'not applicable' in 2024 potentially reflects a reliance upon third parties to deliver the associated works for these elements. However, the use of a third party does not waive accountability for the associated information security risks and, as such, the activities described may still be relevant to the organisation. As referenced in previous Standards, the selection of this status should be based upon the organisation determining there is no related information security risk that needs to be managed. However, this is unlikely for some of these elements.

This observation is based upon supporting commentary offered by organisations where they noted CenITex, or another third-party contracted service provider, was contracted to manage the organisation's ICT systems. Under Part 4 of the PDP Act, an organisation still has information security responsibilities, even where a third-party arrangement manages the day-to-day activities.

OVIC encourages organisations to reconsider their responses in subsequent reporting cycles.

Figure 1.11.E

Count of organisations that selected 'Not Applicable' for Standard 11 elements



Standard 12 – Physical Security

> *An organisation establishes, implements and maintains physical security controls addressing facilities, equipment and services.*

Overall implementation status for Standard 12

Figure 1.12.A shows the overall self-assessed implementation statuses selected for the 6 supporting elements under Standard 12. This Standard requires organisations protect public sector information by implementing layered physical security controls (across facilities, equipment and services) to maintain a secure environment.

Organisations had a modest implementation rate with 48% of the elements under Standard 12 reported as implemented in 2024. However, OVIC is encouraged to see an additional 40% of elements reportedly underway.

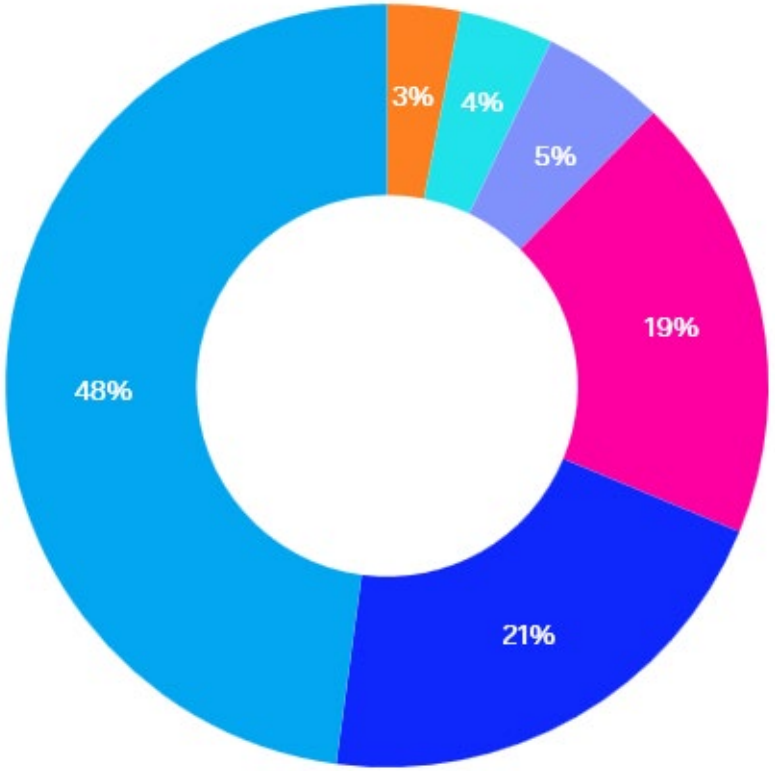


Figure 1.12.A
Reported implementation status of all Standard 12 elements

Implementation status per element by sector

Figure 1.12.B shows the average reported status of each element under Standard 12 broken out by sector.

Across all sectors, there appears to be a relatively consistent reported rate of implementation for each of the Standard 12 elements. This indicates there is no single prioritised area of the physical security program with work needing to be done across each of the elements by each of the sectors.

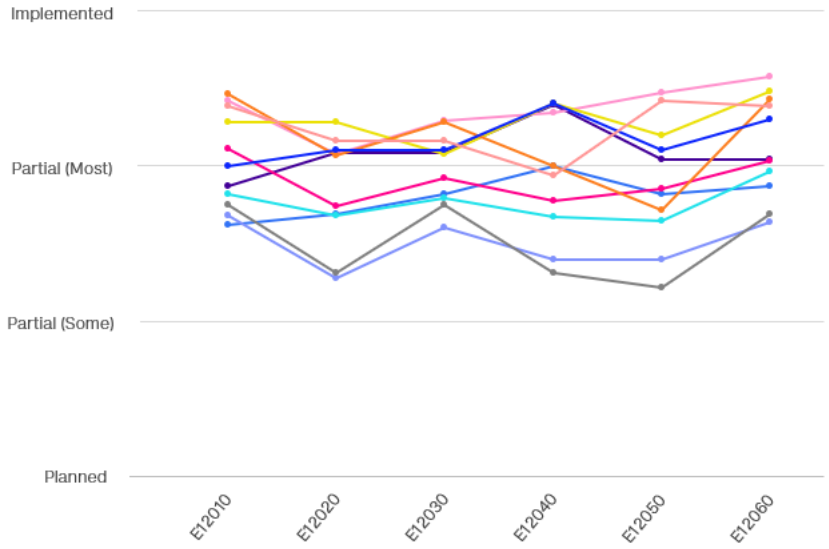


Figure 1.12.B
Average implementation status for Standard 12 elements by sector

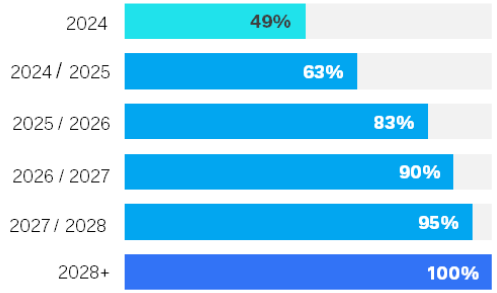
Justice, Community and Emergency Services	Water Corporations and Catchments
Finance, Legal, and Administrative	Arts, Sport and Recreation
Health and Human Services	Departments
Industry and Transport	Environment and Land Management
Local Government	Regulatory and Integrity Bodies
Education	N = 360

Proposed completion dates

Figure 1.12.C represents the proposed timeline for the implementation of the remaining Standard 12 elements across the 360 reporting organisations. At the time of submission, 49% of applicable Standard 12 elements were reported as implemented with organisations projecting an increase of 14% in implementation by 2024/2025.

The proposed uptake may reflect that physical security has not been identified as a leading priority in organisations' overall security programs, compared to the other domains.

Figure 1.12.C
Standard 12 - Current / projected implementation timeline



2022 and 2024 comparison

Average implementation status per element in Standard 12 (2022 v 2024)

Figure 1.12.D presents the average reported implementation status of all elements under Standard 12 across 2022 and 2024. It shows a small increase in the implementation status over time for the 316 organisations.

Responses for this Standard appear to be tracking consistently across the 2 reporting cycles.

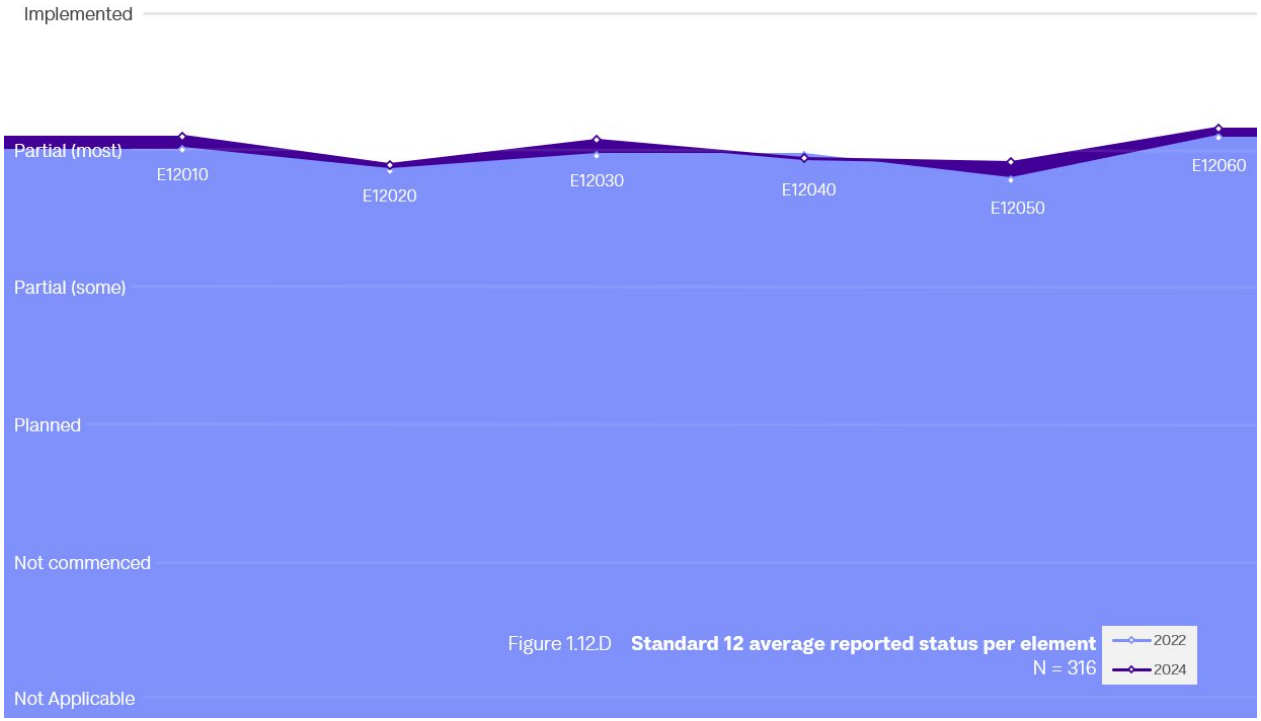


Figure 1.12.D **Standard 12 average reported status per element**
N = 316

Comparison of Standard 12 elements reported as 'not applicable' (2022 v 2024)

Of the 316 organisations that reported in both 2022 and 2024, OVIC noted a 27% increase in the selection of 'not applicable' in 2024. This substantial increase raises concerns for OVIC especially given the justifications offered by some organisations highlighted confusion around the relationship of third parties and the risk these entities pose to the engaging organisation's information.

OVIC understands that organisations often rely on shared service providers to manage security arrangements for their premises when tenanted in a shared facility, however, the outsourcing of these services does not negate the presence of risk that needs to be appropriately managed by the engaging VPS organisation. Even in situations where an organisation has limited influence over the security conditions of their buildings, local physical security controls can be implemented by the regulated organisation to try to mitigate risks. These layered security controls are consistent with the defence-in-depth principles as set out under E12.020.[41]

OVIC strongly encourages organisations to reconsider the selection of 'not applicable' given the relevance of these elements. These elements apply across various settings including arrangements where there is traditional on-site work, as well as situations where there are off-site or remote working conditions. Physical security risks continue, and the maintenance of physical security controls is required to protect public sector information and systems.

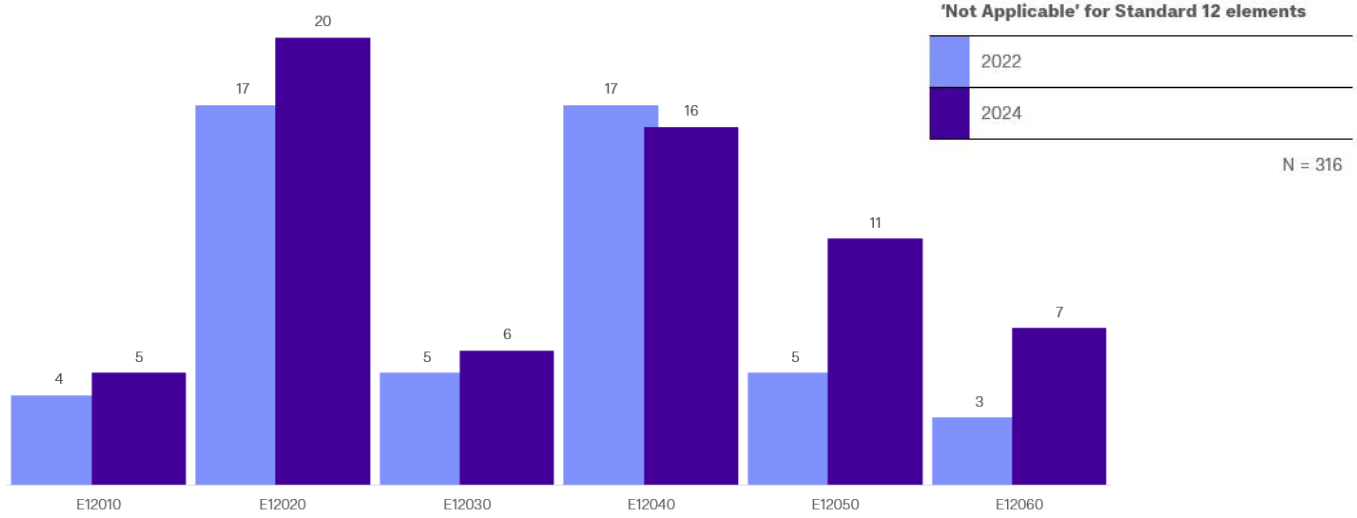
OVIC noted that the organisations reporting 'not applicable' for these specific elements tended to consistently nominate 'not applicable' for elements under other Standards.

Figure 1.12.E highlights a significant shift in reported rates of 'not applicable' for E12.050 and E12.060, from 2022 to 2024. This could be due to a change in the physical security arrangements post-COVID, including potential adjustments in physical security conditions around return-to-work.

Organisations are encouraged to consider the risks when handing information out of the office (including working from home settings, satellite worksites, travelling workforces) and ensure they are continually monitoring the efficacy of physical security measures throughout their lifecycle, to ensure they are fit for purpose and are helping mitigate identified risks.

Figure 1.12.E

Count of organisations that selected 'Not Applicable' for Standard 12 elements



[41] E12.020 - *The organisation applies defence-in-depth physical security measures.*

Generative Artificial Intelligence (AI) Insights

> *Artificial Intelligence – A machine-based system that, for explicit or implicit objectives, infers from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.*

With the rise in the use of Generative Artificial Intelligence, OVIC introduced new questions to the 2024 PDSP form related to this technology. OVIC sought to understand how the VPS was using or planning to use this technology by asking the following types of questions:

- whether Generative Artificial Intelligence is used within the organisation and by its contracted service providers (CSPs)
- what tools are being used or considered
- the type of information being ingested
- the security value of this information.

Organisational use of Generative Artificial Intelligence

In 2024, 48% of organisations reported they were 'not using' Generative Artificial Intelligence, with a subsequent 5% noting that they were 'unsure' if it was being used, and a further 1% leaving this section blank.

As shown in *Figure 1.F*, 20% of organisations reported that they were currently using Generative Artificial Intelligence and a subsequent 26% stated they were 'planning' to implement the technology.

Tools (organisations)

Of those organisations that reported they were using or 'planning' to use Generative Artificial Intelligence technology, a breakdown of the available selections offered on the 2024 PDSP is depicted in *Figure 1.G*.

Microsoft Copilot (124) is the most used tool followed by ChatGPT (75). This higher adoption of Microsoft Copilot may be due to the functionality being rolled out for many Microsoft customers across their Microsoft suite.

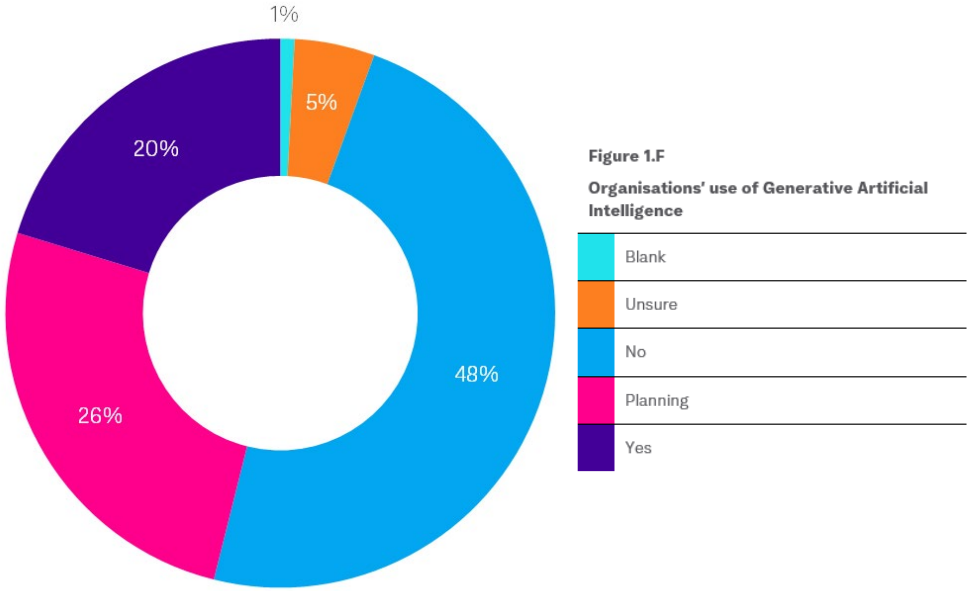


Figure 1.F
Organisations' use of Generative Artificial Intelligence

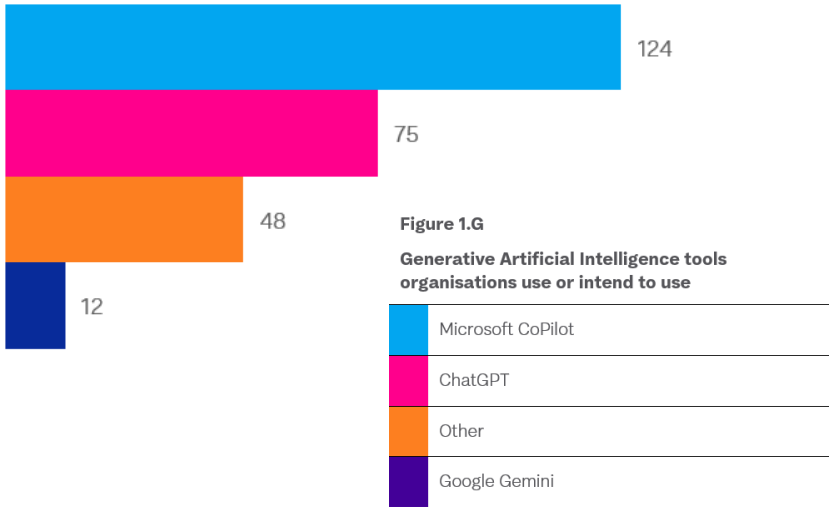


Figure 1.G
Generative Artificial Intelligence tools organisations use or intend to use

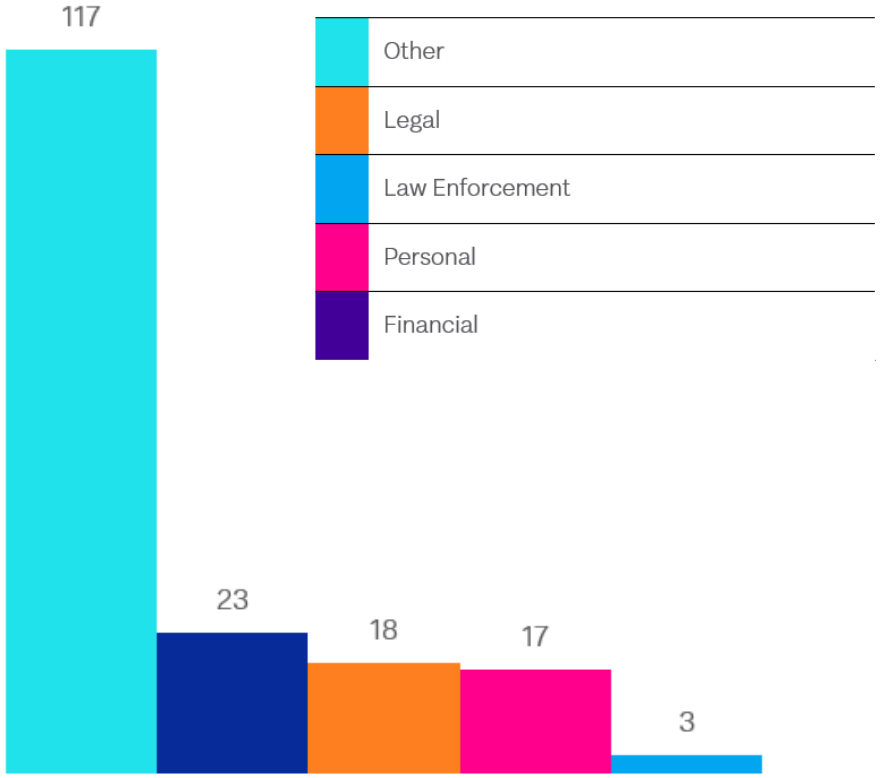
Types of information (organisation)

Of the organisations that use Generative Artificial Intelligence, they were asked to nominate the types of information they were using or proposed to use as inputs into the tools. Responses are shown in *Figure 1.H*, with a common selection of 'other'. The accompanying commentary for this selection ('other') highlighted some significant challenges for organisations either in interpreting this question or identifying different types/attributes of information. The next most selected information type was financial, although the detail regarding what type of financial information that organisations are placing in these Generative Artificial Intelligence tools is not known, that is, whether these tools are being used to make calculations based on certain formulas or analyse financial information and output reports. Organisations that identify personal information being used in Generative Artificial Intelligence tools should consider the guidance/advice provided by OVIC regarding this topic, if they have not already.[42]

OVIC will maintain ongoing oversight of how Generative Artificial Intelligence is utilised across the VPS.

Figure 1.H

Types of information organisations are using / propose to use in Large Language Models



[42] Review OVIC's guidance on Generative Artificial Intelligence and the use of personal information available at https://ovic.vic.gov.au/privacy/resources-for-organisations/use-of-personal-information-with-publicly-available-generative-ai-tools-in-the-victorian-public-sector/

BIL ratings (organisation and CSP)

Organisations' responses to this question were largely dependent upon their implementation of *Standard 2 – Information Security Value*. If organisations were yet to finalise elements associated with Business Impact Level (**BIL**) assessments,[43] they were not well-placed to offer informed responses to this question. As shown in *Figure 1.I*, most (85) organisations place BIL 1 information into Generative Artificial Intelligence tools which demonstrates some level of understanding regarding the risks surrounding the use of this technology. Where BIL 2 (30) and BIL 3 (5) information is placed into the tools, there is no detail regarding whether these are internally hosted Generative Artificial Intelligence systems nor the outcomes of associated risk assessments to support these business decisions.

The number of organisations nominating 'Unknown' may indicate that those organisations are yet to undertake an assessment of the information they intend to use prior to using these models. However, for organisations that have not undertaken an information security value assessment of the information being used by Large Language Models, OVIC strongly recommends they undertake this activity immediately to ensure any information security risks are managed appropriately. Standard 8 responses influenced the responses offered under this section. Most of the information is either at BIL 1 or 'unknown'. The number of responses nominated as 'Unknown' causes some concern for OVIC where organisations are unsure what BIL the information is that their CSPs are entering into Generative Artificial Intelligence tools.

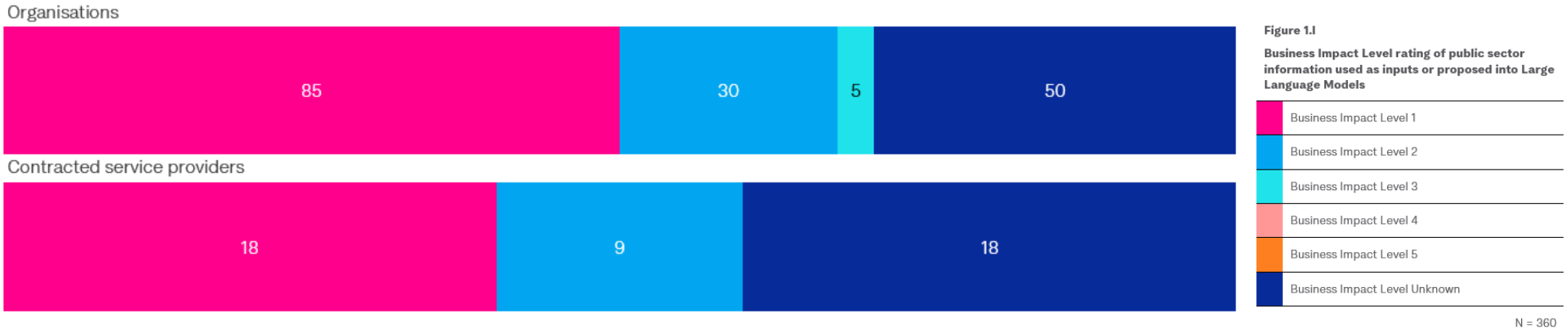
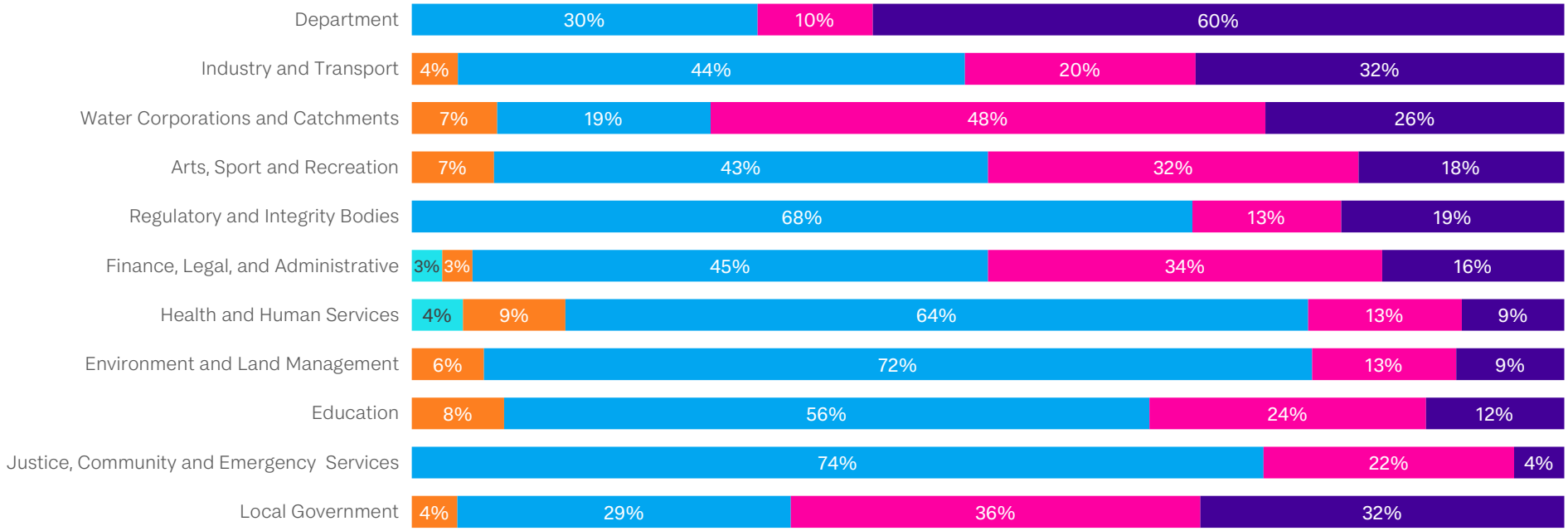


Figure 1.I

Business Impact Level rating of public sector information used as inputs or proposed into Large Language Models

[43] For information on BIL assessments, refer to Section 10 of the VPDSF Practitioner Guide: Assessing the security value of public sector information available at https://ovic.vic.gov.au/information-security/practitioner-guide-assessing-the-security-value-of-public-sector-information-v2-0/



Sector use

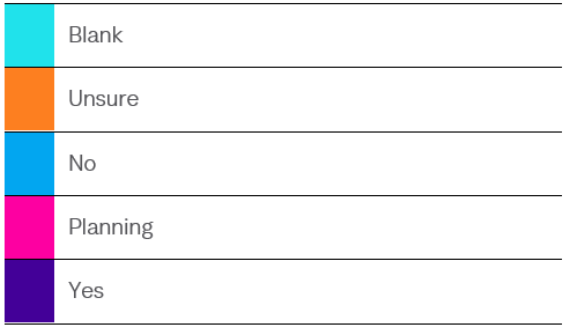
Figure 1.J shows the distributed responses from VPS organisations use of Generative Artificial Intelligence broken out by sector.

The top 3 sectors that responded 'Yes' or 'Planning' to the use of Generative Artificial Intelligence were:

1. Water Corporations (74%)
2. Departments (70%)
3. Local Government (67%)

The Health and Human Services sector and the Environment and Land Management sector have indicated a lower intention to use these tools.

Figure 1.J
Use of Generative Artificial Intelligence across sectors



N = 360

Contracted service provider use of Generative Artificial Intelligence

As shown in *Figure 1.K*, 51% of organisations reported that their CSPs were 'not using' Generative Artificial Intelligence with a subsequent 40% noting that they were 'unsure' if it was being used and a further 2% leaving this section blank.

Figure 1.K shows only 4% of organisations reported that their CSPs were currently using Generative Artificial Intelligence and a subsequent 3% submitted they were 'planning' to implement the technology. Of those organisations that reported their CSPs were using or 'Planning' to use the technology, a breakdown of the available selections offered on the 2024 PDSP is depicted in *Figure 1.L* with Microsoft Copilot and Other being the most commonly used tools.

Tools (CSPs)

Where organisations indicated their CSPs were using tools other than those listed in the PDSP template, they failed to adequately list what those tools were and, as such, provided OVIC with limited insight to offer any dominant themes in this report.

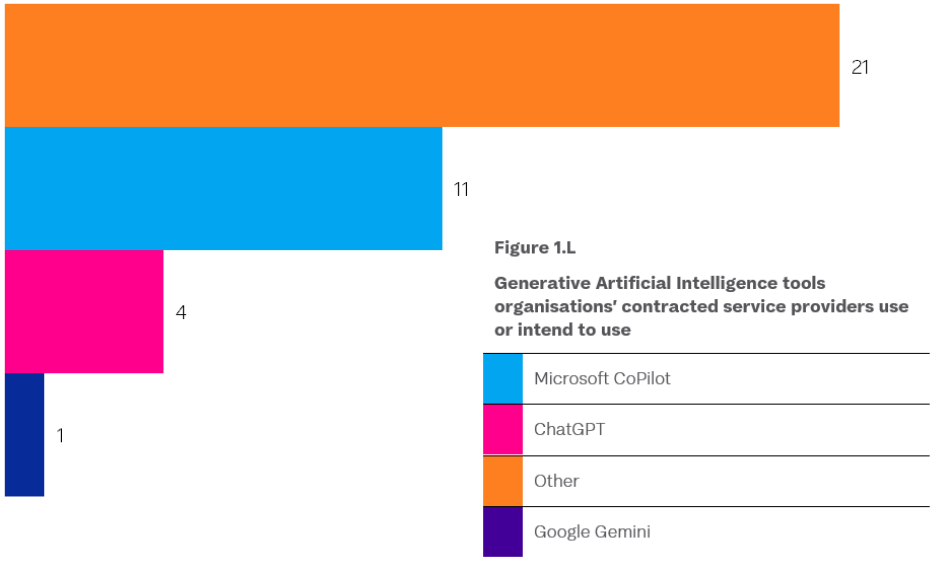


Figure 1.L

Generative Artificial Intelligence tools organisations' contracted service providers use or intend to use

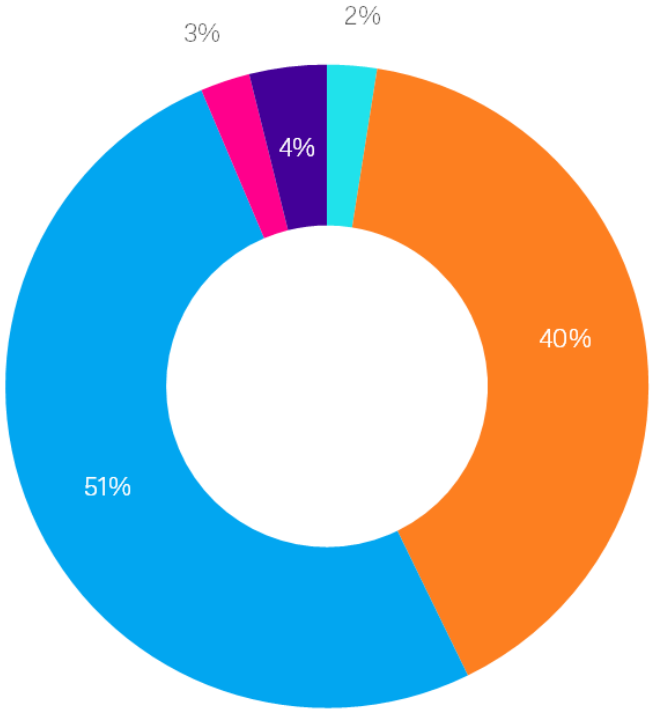


Figure 1.K

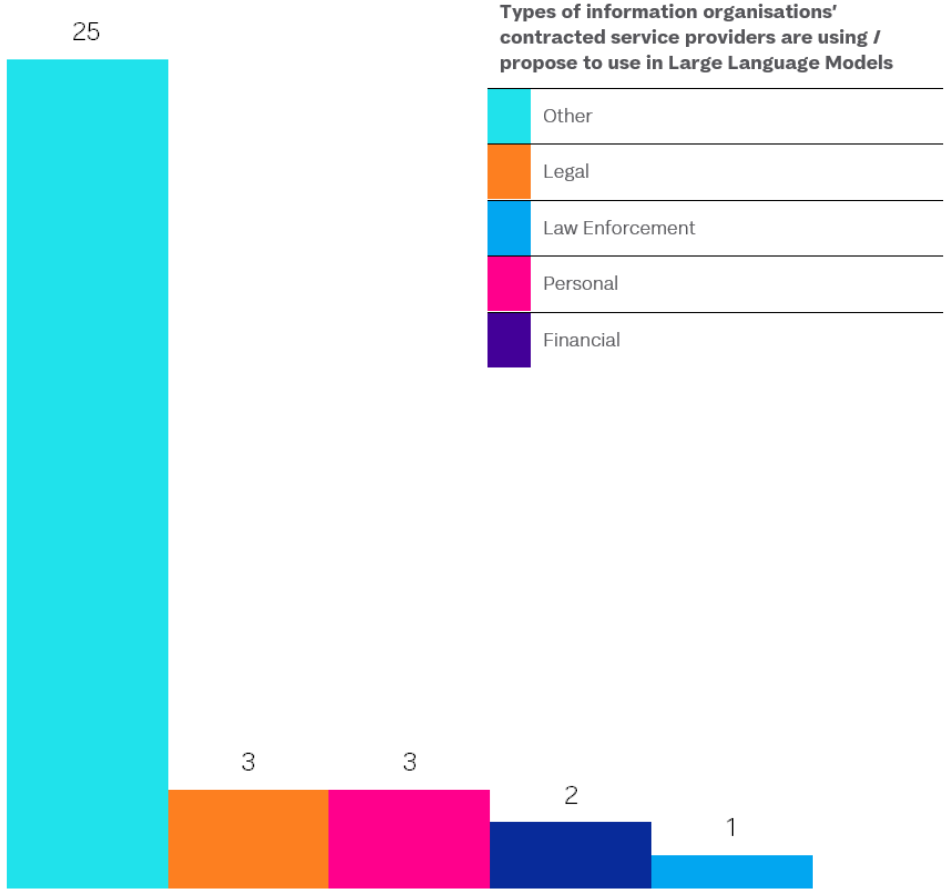
Use of Generative Artificial Intelligence in organisations' contracted service providers

Types of information (CSPs)

OVIC asked organisations to nominate the types of information that CSPs were using or ***proposed*** to use as inputs into Generative Artificial Intelligence tools. *Figure 1.M* shows a common selection of 'Other'. As stated above, the accompanying commentary for the selection of 'Other' highlighted some significant challenges in organisations' interpretation of this question and the ability to identify different types/attributes of information.

Figure 1.M

Types of information organisations' contracted service providers are using / propose to use in Large Language Models



Sector breakdown (CSP use of Generative Artificial Intelligence)

Figure 1.N shows the distributed responses from VPS organisations regarding their CSPs' use of Generative Artificial Intelligence broken out by sector.

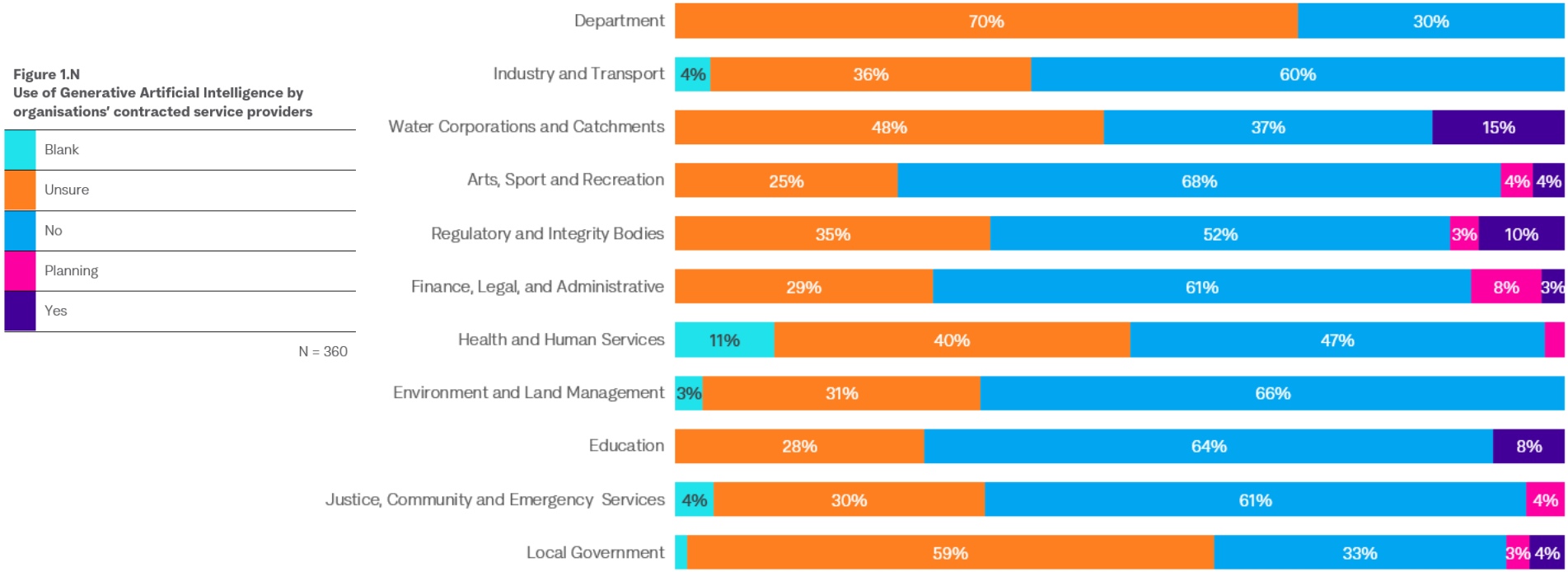
The top 3 sectors that responded 'Yes' or 'Planning' to their CSPs' use of Generative Artificial Intelligence were:

1. Water Corporations and Catchments (15%)
2. Regulatory and Integrity bodies (13%)
3. Finance, Legal and Administrative (11%)

Departments (70% 'Unsure') and the Local Government (59% 'Unsure') sector reporting indicated that they are uncertain whether their CSPs are leveraging Generative Artificial Intelligence. Without clear understanding, organisations risk unknowingly exposing sensitive/significant information in these tools.

OVIC encourages organisations to consider the updated guidance released around the use of these tools,[44] as well as have regard to CSPs' use or planned use of Generative Artificial Intelligence when assessing third-party risk.

Figure 1.N
Use of Generative Artificial Intelligence by organisations' contracted service providers



[44] To read OVIC's publication *Use of enterprise Generative Artificial Intelligence tools in VPS*, please visit: https://ovic.vic.gov.au/privacy/resources-for-organisations/use-of-enterprise-generative-ai-tools-in-the-victorian-public-sector/

To read OVIC's publication *Use of personal information with publicly available Generative Artificial Intelligence tools in the VPS*, please visit: https://ovic.vic.gov.au/privacy/resources-for-organisations/use-of-personal-information-with-publicly-available-generative-ai-tools-in-the-victorian-public-sector/

Control Libraries

A 'control' is defined as a measure that maintains and/or modifies risk.[45] This may include specific policies, procedures, processes and technologies. In an information security context, a control library refers to a central repository or catalogue of selected controls that an organisation uses, or intends to use, to protect information and systems.

On their PDSPs, organisations were required to nominate a supporting control library for each element under the VPDSS. The most common primary sources (control references) were listed as available options on the 2024 PDSP template, including:

- OVIC's Victorian Protective Data Security Standard Element (**VPDSSE)**
- the International Organisation for Standardisation (**ISO**) 27000 series
- Australian Government Protective Security Policy Framework (**PSPF**)
- Australian Government Information Security Manual (**ISM**)
- the US Department of Commerce National Institute of Standards and Technology Standards (**NIST**)
- International Electrotechnical Commission (**IEC**) 62443 series.[46]

Where an organisation opted to use a supporting control library beyond the ones outlined as a primary source of the VPDSS, the organisation must be confident that the control source provides (at a minimum) functional equivalency to what the VPDSS primary source (control reference) described. For organisations that nominated an alternative source (by selecting 'other'), they were prompted to specify the name of the alternative control library in the 'Additional Commentary' field at the end of each standard on their PDSP.

The selection of these alternative sources follows the risk-based approach of the Standards, with OVIC allowing alternative control libraries to be utilised where these sources support the intent of the standard and modify organisational risks.

Themes

Figure 1.0 shows that, in 2024, OVIC's VPDSSE was the most nominated primary control source for each element across all the Standards. This may be due to the VPDSSE drawing from primary sources that are consistent with national and international best practice, or perhaps reflective of the VPDSSE being considered a 'default' control library for many VPS organisations. In addition to this, stakeholders may have been unfamiliar with alternative control sources or may not have been confident that they offered functional equivalency to what the VPDSS primary course (control references) described.

For Standard 4 the ISM was listed as a dominant control library. Whilst Standard 4 does heavily reference logical access requirements, physical access references are contained under this standard. Given this, the use of the ISM for as a control source is unsurprising, however OVIC cautions the over reliance of this control source for elements that contain discrete physical access requirements. In Standard 5, ISO 27000 series and PSPF were reported as the most commonly used supporting control libraries. The reliance on the PSPF as a primary source for this standard aligns with the personnel security nature of the elements.

Similarly, OVIC's VPDSSE was the primary control library selected for elements under Standard 10 with the second most reported control source being the PSPF. This is consistent with the primary sources offered for this standard and reflects the personnel security controls and guidance offered within the PSPF. For Standard 11, the second most reported control source was the ISM. This is consistent with the primary sources offered for this standard and reflects the controls and guidance specific to ICT within the ISM.

Consistent with the other Standards, OVIC's VPDSSE was the primary control library selected by organisations for elements under Standard 12 with the second most reported control source being the PSPF. This is consistent with the primary sources offered for this standard and reflects the controls and guidance specific to physical security within the PSPF.

Organisations need to be careful when selecting alternative control libraries beyond those offered as the primary source material for the elements. Anecdotally, the ISU has identified some instances where the business area responsible for the drafting of the PDSP submission influences the nomination of primary source material which may not necessarily provide the coverage intended by the element.

[45] Drawn from ISO 31000:2018, 3.8 and referenced in the VPDSS Glossary V2.1.

[46] This Control Library specifically relates to Industrial Automation and Control Systems.

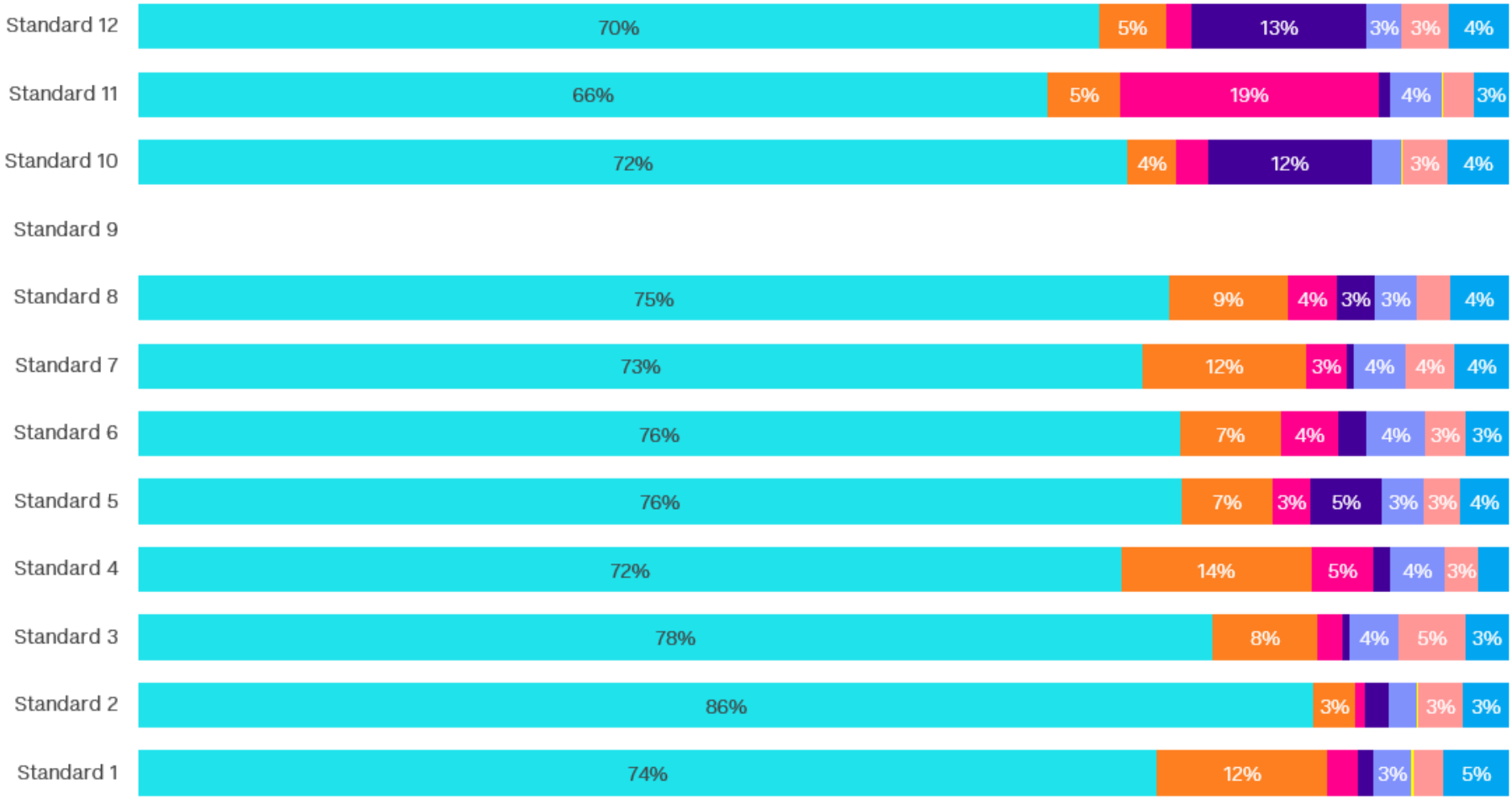


Figure 1.O

Breakdown of primary source selection by Standard

Top 3 elements from 2024

OVIC also measured the elements most selected as being 'implemented', 'not applicable', and 'not commenced/planned'. Of the 360 organisations reporting to OVIC in 2024, 320 of those reported as having implemented VPDSS E1.050 (the nomination of an Information Security Lead). This element, as well as E11.100 and E10.030, reference foundational activities that are easily implemented by organisations or are likely activities already underway as part of its daily business practices. Contrastingly, most reporting organisations do not operate Industrial Automation and Control Systems (IACS) and, as such, elements E1.120, E1.130 and E2.100 are generally not applicable to most environments. The elements most indicated as being not commenced or planned were elements that reflected ongoing activities such as ongoing review, training staff and continual management.
In addition to this, the nature of certain elements often leads to misinterpretation or misunderstanding. Examples of this are seen in responses to VPDSS E2.060 and E2.070, where organisations are prompted to invest in ongoing maintenance and attention to these security activities. The high proportion of responses noting that work was yet to commence or was planned indicate the risk prioritisation of organisations.

Top 3 Elements reported as 'Implemented' in 2024	Number of organisations	**Top 3 Elements reported as 'Not Commenced' or 'Planned' in 2024**	Number of organisations	**Top 3 Elements reported as 'Not Applicable' in 2024**	Number of organisations
E1.050 Executive management nominates an information security lead and notifies OVIC of any changes to this point of contact.	320	E2.070 The organisation continually reviews the security value of public sector information across the information lifecycle.	107	E1.120 The organisation's information security framework defines the relationship between the business areas that support IT security and the business areas that support Industrial Automation and Control Systems (**IACS**) security.	296
E11.100 The organisation manages security measures for email systems.	289	E2.060 The organisation manages the aggregated (combined) security value of public sector information.	93	E1.130 The organisation's information security framework differentiates security objectives of the E1.130 Industrial Automation and Control Systems (IACS) from the enterprise systems.	296
E10.030 The organisation undertakes pre-engagement screening commensurate with its security and probity obligations and risk profile.	275	E5.040 The organisation provides targeted information security training and awareness to persons in high-risk functions or who have specific security obligations (e.g., executives, executive assistants, procurement advisors, security practitioners, risk managers).	85	E2.100 The organisation identifies, documents, and maintains the security attributes (confidentiality, integrity, and availability business impact levels) of its process automation assets in a register.	245

Chapter 2
Information Security Incident Insights

Information Security Incident Notification Scheme

The Information Security Incident Notification Scheme ('**the Scheme**')[47] provides organisations with a central avenue to notify OVIC of information security incidents. The Scheme falls from VPDSS element E9.010, under which VPS organisations notify OVIC of incidents that have an adverse impact on the confidentiality, integrity or availability of public sector information assessed as having a 'limited' business impact or higher (Business Impact Level of 2 or above). Information assessed as being a BIL 2 or higher includes material with a protective marking of OFFICIAL: Sensitive, PROTECTED, Cabinet-In-Confidence or SECRET.

Notification of information security incidents should be made to OVIC as soon as practical and no later than 30 days from identification.

Incidents include compromises of all types of public sector information of various formats such as:

- physical - e.g. printed, photographs, audio or video recorded information
- verbal – e.g. discussions
- electronic – e.g. data held on systems and services.

Breach vs. incident

The terms 'breach' and 'incident' have 2 distinct meanings despite overlapping attributes.

In the context of the VPDSS, an incident is defined as:

> *one or multiple related and identified security events that can harm/damage an organisation, its assets, individuals or compromise its operations. Information security incidents may take many forms, such as compromises of electronic information held on government systems and services and include information in physical formats (e.g., printed, photographs, or recorded information either audio or video) and verbal discussions.*[48]

This includes a compromise of the confidentiality, integrity and/or availability of public sector information held in any format.

In the privacy context, a data breach is defined as occurring when personal information that is held by a public sector organisation is subject to misuse, or loss, or to unauthorised access, modification or disclosure.[49]

[47] To read more about OVIC's *Information Security Incident Notification Scheme*, please visit https://ovic.vic.gov.au/information-security/ovic-information-security-incident-notification-scheme/
[48] For information on definitions under the VPDSS, please visit: https://ovic.vic.gov.au/information-security/victorian-protective-data-security-standards-glossary-v2-1/

[49] For more information relating to a breach of personal information, please visit: https://ovic.vic.gov.au/privacy/resources-for-organisations/managing-the-privacy-impacts-of-a-data-breach/

Information Security Incident Insights Reports

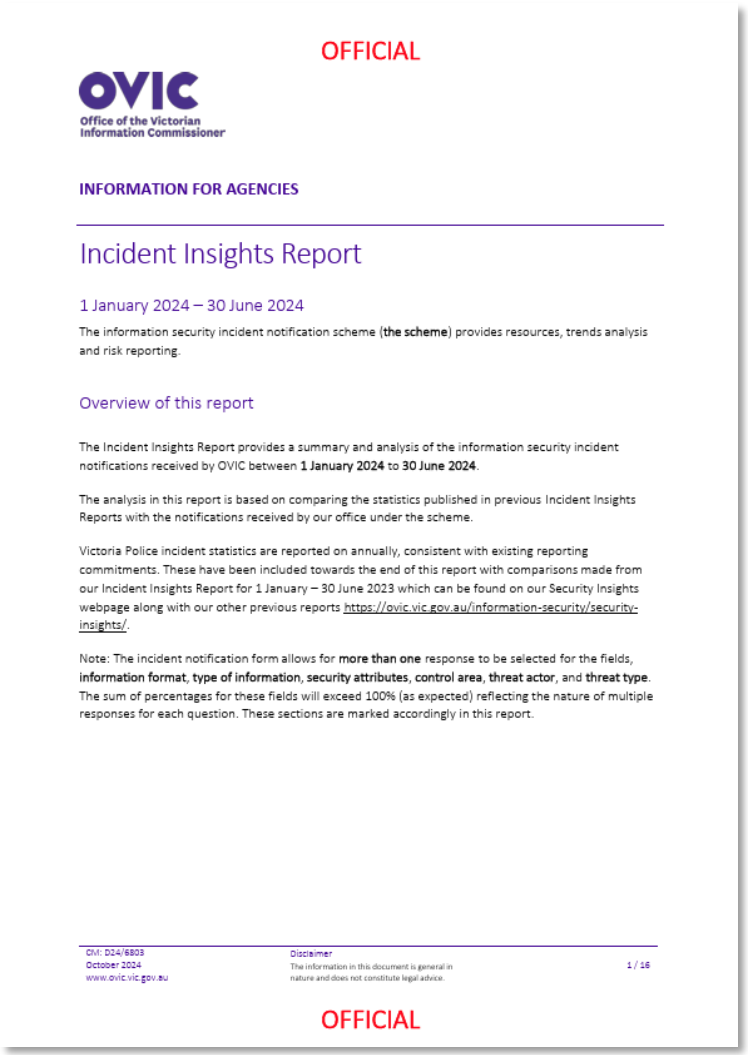
Incident notifications assist OVIC to develop a comprehensive security risk profile of the Victorian government. These can be used for trend analysis and understanding the threat environment as it relates to the protection of public sector information.

OVIC presents these findings, observations and insights in biannual Information Security Incident Insight Reports,[50] and in regular Victorian Information Security Network (VISN) events. These reports and events are designed to:

- assist organisations' risk reporting
- inform risk assessments
- prepare business cases for internal strategic security initiatives.

While the Information Security Incident Insights Reports refer to portfolios, the analysis in this document presents sector-based figures and commentary.[51] These 11 sectors are spoken to in the Annexure of this report. As such, certain organisations' incident data may be represented in an alternative manner to those found in the Information Security Incident Insights Reports.

For portfolio analysis (as opposed to the sectors presented in this report), please refer to the relevant Information Security Incident Insights Report.



OFFICIAL

OVIC
Office of the Victorian Information Commissioner

INFORMATION FOR AGENCIES

Incident Insights Report

1 January 2024 – 30 June 2024

The information security incident notification scheme (**the scheme**) provides resources, trends analysis and risk reporting.

Overview of this report

The Incident Insights Report provides a summary and analysis of the information security incident notifications received by OVIC between **1 January 2024** to **30 June 2024**.

The analysis in this report is based on comparing the statistics published in previous Incident Insights Reports with the notifications received by our office under the scheme.

Victoria Police incident statistics are reported on annually, consistent with existing reporting commitments. These have been included towards the end of this report with comparisons made from our Incident Insights Report for 1 January – 30 June 2023 which can be found on our Security Insights webpage along with our other previous reports https://ovic.vic.gov.au/information-security/security-insights/.

Note: The incident notification form allows for **more than one** response to be selected for the fields, **information format**, **type of information**, **security attributes**, **control area**, **threat actor**, and **threat type**. The sum of percentages for these fields will exceed 100% (as expected) reflecting the nature of multiple responses for each question. These sections are marked accordingly in this report.

D/M: D24/6803
October 2024
www.ovic.vic.gov.au

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

1 / 16

OFFICIAL

[50] To read OVIC's *Incident Insights Reports*, please visit https://ovic.vic.gov.au/information-security/security-insights/#incident-insights-reports

[51] As explained in *Annexure – Data and Analysis*.

Summary – 2-year rolling reflection on incidents

Of the 360 organisations that submitted a PDSP to OVIC in 2024, 130 of those organisations notified OVIC of at least one incident under the Scheme between 1 July 2022 to 30 June 2024.

In the most recent incident reporting period (spanning 1 July 2024 – 31 December 2024), 72% of information security incidents were caused by people. This highlights the importance of the personnel-based standards and why the elements supporting Standards 5 and 10 are so critical in helping mitigate these types of risks.

Sector observations

Figure 2.A shows a sector breakdown of the 1,369 incident notifications made to OVIC over the 2-year period under the Scheme.

Figure 2.A depicts nearly three-quarters of the notifications originating from 2 key sectors; the departments,[52] as well as Finance, Legal and Administrative. In contrast, the following sectors submitted the smallest number of notifications to OVIC over this same period:

- Environment and Land Management (2 incidents)
- Arts, Sports and Recreation (12 incidents)
- Justice, Community and Emergency Services (12 incidents)
- Education (15 incidents).

These incident statistics highlight that no sector is immune to experiencing an incident and encourages participation in the Scheme to assist with an overall understanding of organisations' risk profiles across the VPS.

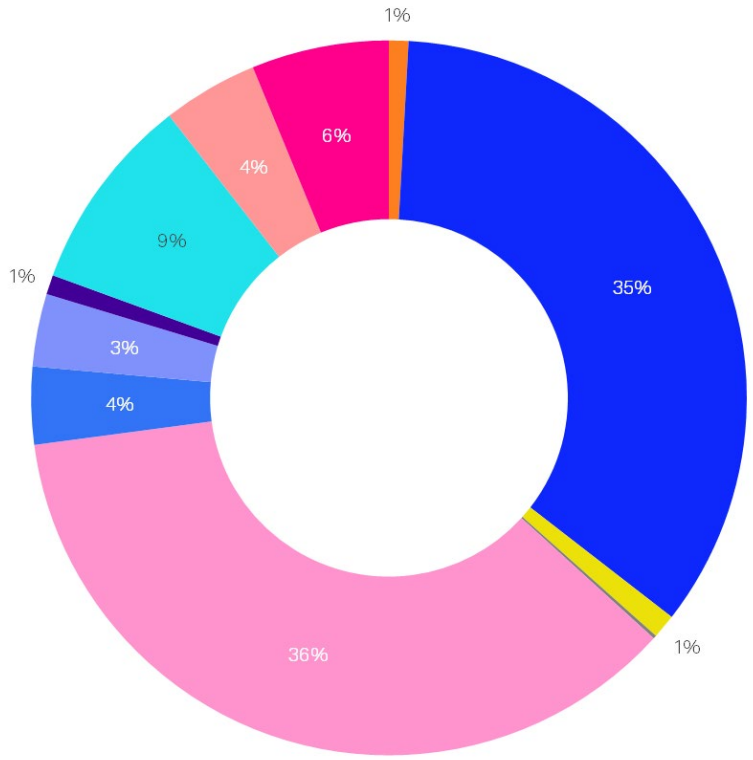


Figure 2.A

Notifications OVIC received by sector

Justice, Community and Emergency Services (1%)	
Finance, Legal, and Administrative (36%)	
Health and Human Services (4%)	
Industry and Transport (3%)	
Local Government (9%)	
Education (1%)	
Water Corporations and Catchments (6%)	
Arts, Sport and Recreation (1%)	
Departments (35%)	
Environment and Land Management (0%)	
Regulatory and Integrity Bodies (4%)	
	N = 1369

[52] Whilst *Figure 2.A* shows a high volume of incident notifications from the departments, OVIC notes that most incident statistics are received from DJCS as opposed to the other departments. OVIC encourages other departments to increase their participation in the scheme.

Figure 2.B contrasts Organisation Profile Assessment (**OPA**) data contained in organisations' PDSPs, with incident notification data received by OVIC under the Scheme during 2022-2024.

In the OPA section of the 2024 PDSP, organisations were asked to nominate the number of information security incidents recorded in their internal incident register over the previous 24 months that affected information assets of a BIL 2 or higher.

As seen in *Figure 2.B,* most of the numbers closely match between the OPA and Scheme, noting that OVIC accepts incidents assessed at any BIL rating. Local Government reported 847 incidents as being recorded in their internal incident register over the past 24 months, however this sector only notified OVIC of 122 incidents under the Scheme over this same period.

Of these, one Local Government Authority (**LGA**) made up the majority of the 847 incidents with other LGAs offering more moderate incident figures. This volume of reporting by one LGA skews the results for the sector.

Whilst it is important that an organisation identifies and records incidents in their internal register, OVIC also encourages participation in the Scheme to inform trend analysis across the sectors.

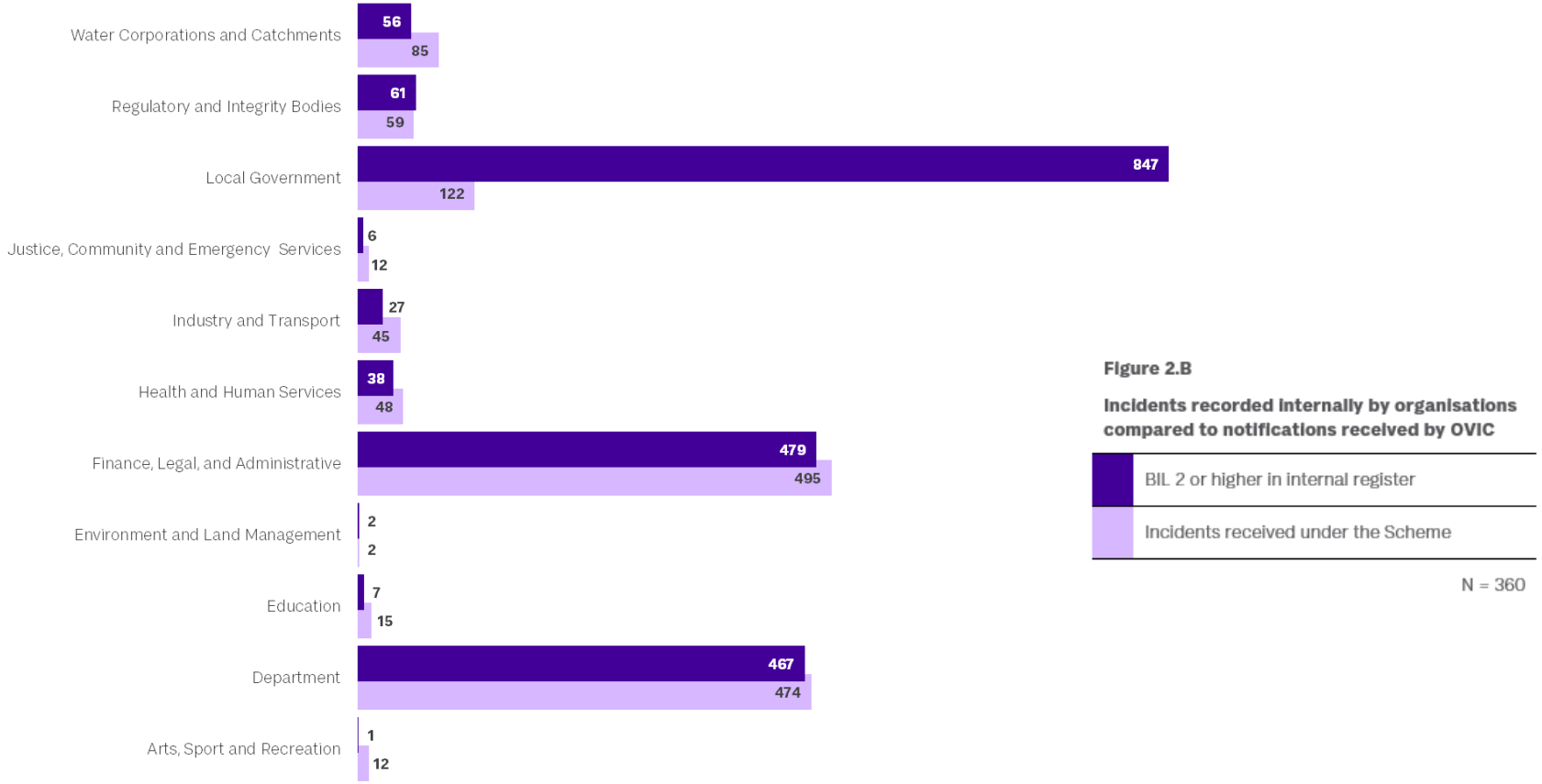


Figure 2.B

Incidents recorded internally by organisations compared to notifications received by OVIC

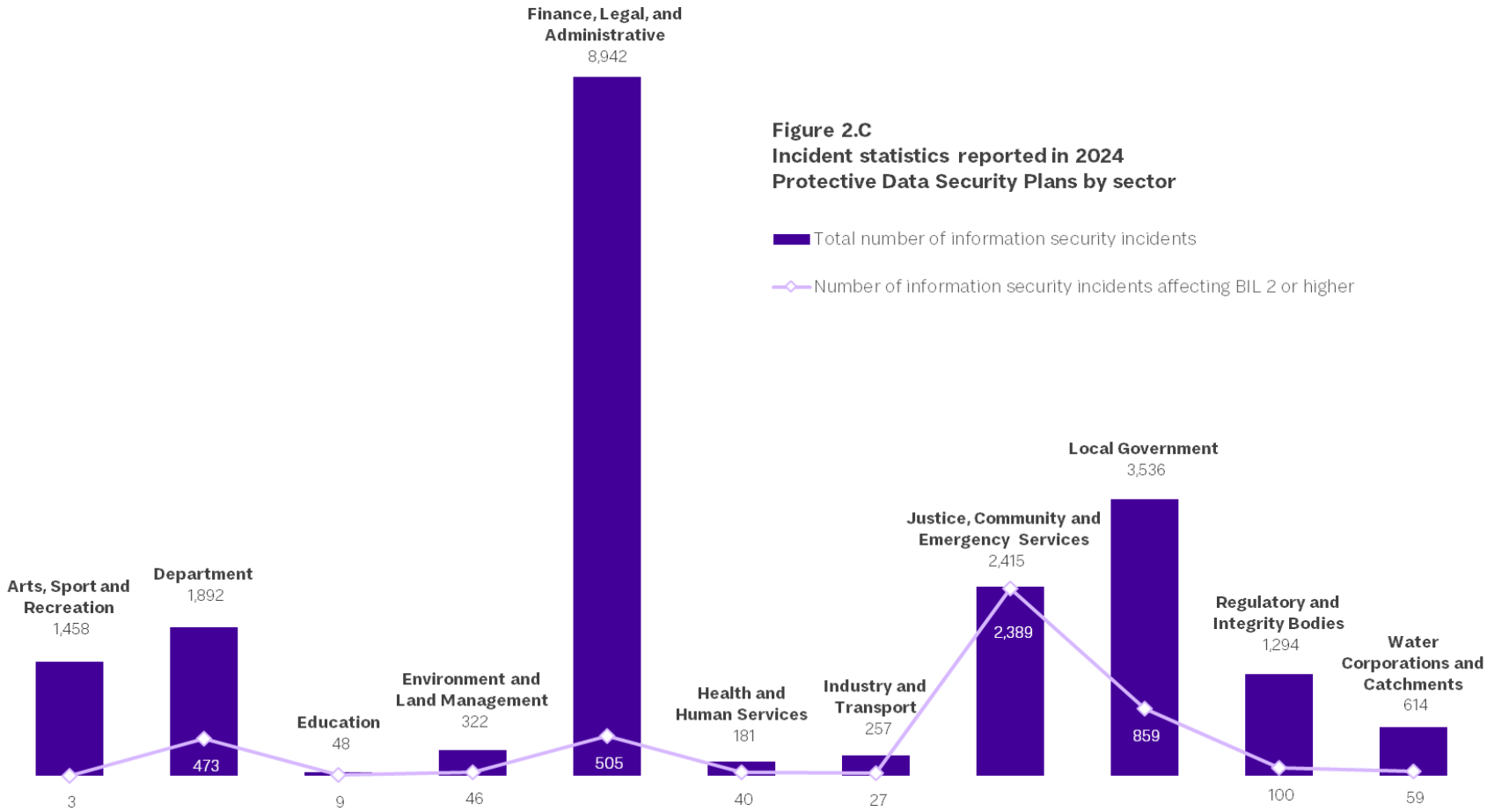


Figure 2.C
Incident statistics reported in 2024 Protective Data Security Plans by sector

Figure 2.C reflects the total number of incidents recorded in organisations' internal incident register contrasted against the total of number of incidents affecting information assets of a BIL 2 or higher.

The columns in *Figure 2.C* present the total number of incidents recorded in an organisation's internal incident register broken out by sector. This data is inclusive of all incidents regardless of BIL rating (e.g. not limited to just a BIL 2 or higher). The total number of incidents reflected in this graph amount to 20,959.

The line in *Figure 2.C* presents the total number of BIL 2 or higher incidents recorded in an organisation's internal incident register. The Justice, Community and Emergency Services sector recorded 2,415 total incidents with 2,389 of these affecting information assets of a BIL 2 or higher. This data is broken out by sector with the Justice, Community and Emergency Services sector accounting for over half of the total BIL 2 or higher incidents for Victorian government as reflected in the OPA of 2024 PDSPs. The total number of incidents assessed as affecting information assets of a BIL 2 or higher amounts to 4,510, or almost a quarter of the total security incidents affecting Victorian government. NB. This data is not reflective of incidents received under the Scheme.

Insights from the Scheme

From July 2023 to December 2023, OVIC observed a significant rise in incident notifications received under the Scheme. Over this period, 9% of incidents indicated authorised third parties were the cause of an incident. This figure more than doubled from incident notifications received by OVIC in the previous reporting year.

January 2024 to June 2024 also saw incident notifications to OVIC under the Scheme where incidents were reported as being caused by a fourth party (i.e. a supplier or contractor of a third party to a VPS organisation). For example, in one incident an authorised third party of a VPS organisation had their managed service provider compromised,[53] and in a separate instance a VPS organisation's contracted service provider had their subcontractor fall victim to a ransomware incident. Whilst OVIC understands that complex supply chains can be difficult to manage, it is important to implement layered security controls to mitigate risks and incidents where possible.

VPS organisations have been significantly impacted by some high-profile incidents where third parties provided services to multiple VPS organisations:

- OracleCMS phone call service provider[54]
- ZircoDATA records and information management service[55]
- Herron Todd White property valuation service.[56]

In these instances, transparent and timely notification to impacted parties is critical to help mitigate risks and lessen the impact of the incident. Due to the information sharing arrangements that operate across the Victorian government, VPS organisations often operate in a somewhat interconnected way. This can mean that security vulnerabilities of a single organisation can have significant ramifications for associated organisations.

Information security risks falling from incident notifications

Incident notifications help build important insights into the risk landscape. Risks signal potential future events that can materialise and manifest in negative ways.

Given the risk-based nature of the VPDSS, it is critical that organisations identify, analyse and evaluate risks in an ongoing manner. This enables organisations to prioritise the roll out of their information security program and deliver more efficient, effective and economic outcomes.

In response to requests for additional assistance in this space, OVIC has published an Information Security Risk Statement Library extracted from each Information Security Incident Insights Report. It reflects risk statements formed from actual information security incident notifications received by OVIC.[57] As new Information Security Incident Insight Reports are released, OVIC intends to update this library with new risk statements.

Organisations are encouraged to review these risks within the context of their own environment to raise awareness of the developing threat environment and consider mitigations where appropriate.

[53] To read Ticketek's media release on the 2024 Cyber Incident, please see: https://www.teg.com.au/statement-regarding-ticketek-cyber-incident/

[54] To read more on the breach, please visit New South Wales Government's website at https://www.nsw.gov.au/id-support-nsw/learn/data-breaches/data-breach-announcements/oraclecms-data-breach

[55] To read OVIC's Media Release on the ZircoDATA incident, please visit: https://ovic.vic.gov.au/mediarelease/zircodata-cyber-incident-involving-victorian-public-sector-information/

[56] To read the Financial Review's article on the Herron Todd White data breach, please see: https://www.afr.com/property/commercial/valuation-firm-htw-suspended-by-banks-after-data-breach-20240411-p5fj33

[57] To read OVIC's *Information Security Risk Statement Library* document, please visit https://ovic.vic.gov.au/information-security/information-security-resources/information-security-risk-statement-library/

Chapter 3
Audits, Reviews, Investigations and Examinations

OVIC conducts audits, reviews and investigations to:

- verify organisations' PDSP reporting
- address concerns arising from information security incidents and/or privacy breaches
- unpack broader PDP Act non-compliance concerns.

Whilst the focus of some of these regulatory activities directly related to the VPDSS, other investigations or reviews performed by OVIC indirectly inform positive information security outcomes. Those outcomes included

- gaining insight into organisations' information security programs
- identifying deficiencies in organisational information security practices
- understanding how organisations sought to manage information security risks
- highlighting tensions, concerns or opportunities around the VPDSS and VPDSF product suite.

This chapter considers more recent audits, reviews and investigations performed by OVIC, and unpacks associated recommendations or actions designed to inform and improve the information security practices of the audited organisations. The chapter also touches on monitoring and assurance activities of other oversight and integrity bodies. OVIC encourages VPS organisations to review the learnings offered from these reviews and consider how they may apply to their own information security program and practices.

OVIC audits

Under section 8D(2)(b) of the Act, the Information Commissioner can audit regulated organisations 'to ascertain compliance with data security standards.' Since 2021, OVIC has conducted 3 audits of organisations' adherence to the Standards, focusing on organisations that have reported strong implementation statuses for the relevant standards.

Audits

Audit of Standard 10 – Pre-engagement screening - Personnel Security (2024)

Under Standard 10 of the VPDSS, public sector organisations must establish, implement, and maintain personnel security controls addressing all persons' continuing eligibility and suitability to access public sector information. Though Standard 10 sets out expectations regarding the full personnel lifecycle, this audit focussed on the pre-engagement phase – that is, time between completion of a merit selection process and a new employee commencing in the organisation.

In the audit, OVIC sought to determine whether the 4 organisations had appropriate policies, procedures, and practices in place that addressed the pre-engagement phase of personnel security, and whether organisations were undertaking appropriate pre-engagement screening checks to assess suitability and eligibility of prospective staff.[58]

Some broad insights from this audit included:

1. some organisations failed to adequately document all pre-engagement screening requirements in a coherent and consistent way, or in a manner that sufficiently reflects best practice.
2. highlighting gaps, duplication, inaccuracies, and outdated content in policy and procedure documents, as well as insufficient coverage of all personnel (particularly temporary resources and contractors), and inconsistent/inappropriate timing of pre-engagement screening checks, meaning crucial checks were not conducted until after commencement in the role.

[58] To read the Standard 10 Audit report, please visit: https://ovic.vic.gov.au/regulatory-action/audit-report-standard-10-of-the-victorian-protective-data-security-standards-personnel-security/

3. disparities in the level of pre-engagement screening undertaken by an organisation contrasted against the level of risk posed by the functions associated with a role, organisational objectives, processes, and assessment of business impact. OVIC notes that different functions are likely to attract different levels of risk.
4. deficiencies in identity verification of personnel.
5. limitations in the management and oversight of third parties who undertook pre-engagement screening checks on the organisation's behalf. There was little comfort for the engaging organisation that all checks were undertaken in a consistent way, meeting relevant standards.
6. pre-engagement screening policies, procedures and practices did not cover additional pre-engagement checks for high-assurance roles, including those with access to security classified information and systems.

In summary, OVIC strongly encourages all VPS organisations to undertake a review of their workforce to determine the risk profile of the various roles and associated functions. This review should aim to ensure personnel security policies and procedures contain adequate pre-engagement requirements for both general and high-assurance roles. Pre-engagement screening practices need to have the appropriate depth and coverage to provide assurance to the organisation that only eligible and suitable personnel are accessing public sector information and systems.

Audit of Standard 8 – Third-party arrangements (2022)

In this audit, OVIC focused on certain aspects of Standard 8 which broadly relate to third-party arrangements. Standard 8 requires VPS organisations ensure that any third parties they engage to collect, hold, manage, use, disclose or transfer public sector information do so in a secure way to ensure it remains secured when outside the VPS organisation's direct control. The standard is further underpinned by elements that require the assessment and mitigation of information security risks before, during and after the engagement.

The audit sought to establish whether the 4 audited organisations had the appropriate procedures and practices in place to ensure third parties managed public sector information that had been shared with them securely. Specifically, this audit considered whether and/or how, the 4 organisations subject to the audit:

- assessed information security risks prior to entering into third-party arrangements
- identified and responded to changes in risks throughout the lifecycle of an engagement
- engaged in an active third-party assurance program to monitor and ensure that third parties were meeting their security obligations (as opposed to simply relying only on contractual clauses)
- the organisation employed measures to protect information at the conclusion of a third-party engagement.[59]

Some broad insights from this audit included:

- an over-reliance on contract clauses that articulate their information security expectations of a third party, left unsupported by accompanying ongoing assurance mechanisms
- the timing of assurance activities (i.e. not necessarily addressing residual risks prior to finalising the arrangement)
- limitations in the ability to identify and respond to risks throughout the third-party arrangement (e.g. when responding to an information security incident, change events and/or periodic scheduled reviews)
- a heavy reliance on third parties to return or destroy information at the end of the engagement without the organisation's input or oversight.

OVIC encourages organisations to consider the broad nature that third-party arrangements can take, ranging from contracted service providers who supply a product or service on, or behalf of, the engaging organisation, through to information sharing partners.

[59] To read the Standard 8 Audit report, please visit: https://ovic.vic.gov.au/regulatory-action/audit-report-standard-8-of-the-victorian-protective-data-security-standards/

Audit of Standard 2 – Information Security Value (2021)

OVIC conducted its first audit of the VPDSS in 2021. Given the foundational nature of Standard 2, this inaugural audit sought to unpack a core activity that informs the development of an organisation's information security program, that is, identifying, recording, and valuing its information assets. Unless organisations invest the appropriate resources in this foundational work, they are limited in understanding what commensurate protections are needed. [60] Agencies are better placed to protect important information assets following an information discovery exercise and subsequent security value assessment.

In this audit, OVIC sought to gain insight into how organisations that reported full implementation of Standard 2 were addressing the supporting elements. OVIC assessed organisations' PDSP responses against their practices and used the observations and findings of the audit to test the organisations' assessments. Some broad insights at the time of this audit included:

1. differences between how organisations assessed themselves against some elements (self-assessed implementation status) and OVIC's assessment, caused by misunderstandings about the requirements of certain elements
2. organisations' information management frameworks were yet to include reference to all security areas (domains)
3. a lack of a consolidated framework for managing security risks across all security areas (governance, information, personnel, ICT, and physical security)
4. work was underway to develop an information asset register, and Business Impact Level tables to assess information's security value, but were not finalised as reported
5. work was underway to apply protective markings to information and systems.

OVIC continues to receive enquiries regarding implementation of Standard 2 and encourages organisations to reach out to the ISU with any questions.

Reviews of Victoria Police

Under the Act, the Information Commissioner is able to conduct monitoring and assurance activities, including audits, to ascertain compliance with data security standards,[61] as well as make reports or recommendations in relation to data security.[62] Further, the Act outlines compliance requirements for Victoria Police under section 94(1) regarding law enforcement data security standards. The information security practices of Victoria Police have been overseen by OVIC and its former offices since 2005.[63] The former offices of the Commissioner for Privacy and Data Protection and the office of the Commissioner for Law Enforcement Data Security conducted numerous reviews and site walkthroughs of Victoria Police, resulting in 271 recommendations since 2008.

Most recently, during the 2023-24 period, Victoria Police commissioned a third party to evaluate the 16 pending recommendations. [64] Following this review, Victoria Police submitted 11 recommendations for closure, stating the recommendations are now "implemented." 11 recommendations have since been finalised, with a further 5 outstanding.

In some instances, Victoria Police has provided responses to address older recommendations, however, the supporting material provided in response to those recommendations, did not provide adequate assurance. For those recommendations, OVIC has determined that Victoria Police does not possess either the necessary resources and/or commitment to implement such recommendations. Given the time elapsed since the recommendations were first made (some recommendations dating back over a decade). OVIC will continue to work with Victoria Police to finalise these recommendations.

As part of its regulatory responsibilities of Part 5 of the Act, ISU continues to:

- review reported information security incidents provided to OVIC
- organise regular meetings with Victoria Police to discuss emerging technology or proposed initiatives within law enforcement
- brief the Privacy and Data Protection Deputy Commissioner on matters impacting law enforcement information and systems, including reported information security incidents
- conduct reviews / monitor the implementation of recommendations.

[60] To read the Standard 2 Audit report, please visit: https://ovic.vic.gov.au/regulatory-action/audit-report-standard-2-of-the-victorian-protective-data-security-standards/
[61] *Privacy and Data Protection Act 2014* (Vic), section 8D(2)(b).
[62] *Privacy and Data Protection Act 2014* (Vic), section 8D(1)(f).
[63] *Commissioner for Law Enforcement Data Security Act 2005* (Vic), sections 4 and 5.
[64] Numbers as of 30 June 2024

Investigations

Under section 8C(2)(b) of the Act, the Information Commissioner can 'examine the practice of an organisation with respect to personal information… for the purpose of ascertaining whether or not the information is maintained according to the Information Privacy Principles (**IPPs**)'.[65] In addition to this, the OVIC Privacy Guidance and Complaints Unit:

- conciliates disputes and handles complaints about possible breaches of the IPPs by the VPS
- assesses compliance with the IPPs
- provides guidance to regulated bodies and the public
- issues reports, guidelines and other materials
- and perform other similar activities.

These activities not only support Part 3 of the PDP Act but provide valuable insights and benefits to organisations' information security practices. Findings falling from privacy-based investigations, audits, reviews and examinations can also inform organisations' information security risk assessments, enhance compliance strategies, and support the development of more robust information security programs under the VPDSS. The following examples serve as useful resources for our shared stakeholder base across Parts 4 and 5 of the PDP Act to strengthen their overall privacy and information security programs.

Investigation into the use of ChatGPT by a Child Protection worker (2024)

In February 2024, the Privacy and Data Protection Deputy Commissioner made a public statement under section 8C(1)(f) relating to the use of ChatGPT by VPS organisations.[66] Guidance offered in the statement relates to VPS organisations' use of any Generative AI tool that is publicly available (platforms or software that can be accessed via web browser or application). Generally, publicly available tools have minimal controls for how information entered is used or protected.

In September 2024, OVIC published an investigation report into the use of ChatGPT by a child protection worker at Department of Families, Fairness and Housing (**DFFH**).[67] The investigation found that the:

- content generated by ChatGPT and then used by a child protection worker when drafting a Protection Application report contained inaccurate personal information – which downplayed risks to the child in the case
- the child protection worker entered a significant amount of delicate personal information into ChatGPT, including names and information about risk assessments relating to the child. By doing so, they disclosed this information to OpenAI, an overseas company, and released it outside control of DFFH.

As a result, OVIC issued a compliance notice to DFFH requiring the department take specified actions to ensure compliance with the IPPs. The actions primarily concern implementing and maintaining security controls preventing child protection staff from using Generative Artificial Intelligence text tools and other applications.

This investigation was primarily borne out of a breach of the privacy principles. There were intrinsic learnings and outcomes in the management of risks and controls in the Generative Artificial Intelligence space, and an influence on the information security practices of the organisation.

Investigation into Datatime Services Pty Ltd data breach (2022)

In November 2022, Datatime Services Pty Ltd (**Datatime**) – a contracted service provider (CSP) to several VPS organisations – suffered a data breach in the form of a ransomware attack where a malicious third party had unauthorised access to the personal information of thousands of Victorians.

OVIC decided to investigate under the PDP Act to determine whether Datatime had committed serious, flagrant or repeated contraventions of the IPPs and whether it was appropriate to issue a compliance notice. Ultimately, Datatime was voluntarily wound up in October 2023. This severely limited the amount of information OVIC could gather and meant it was not possible to formally determine compliance with the IPPs or decide whether to issue a compliance notice.

[65] *Privacy and Data Protection Act 2014* (Vic), section 8C(2)(b).
[66] To read the Public Statement please visit: https://ovic.vic.gov.au/privacy/resources-for-organisations/use-of-personal-information-with-publicly-available-generative-ai-tools-in-the-victorian-public-sector/
[67] To read OVIC's investigation report, please visit: https://ovic.vic.gov.au/regulatory-action/investigation-into-the-use-of-chatgpt-by-a-child-protection-worker/

Despite this, OVIC issued a report about the investigation as the circumstances contain valuable lessons for both organisations and CSPs.[68] This is especially so, given the increasing prevalence of cyberattacks, including those involving third parties to government organisations. Organisations subject to the VPDSS are encouraged to review their information security incident management framework and third-party assurance programs with a view to apply any learnings.

Examination into privacy and information handling training at Victoria Police (2021)

On 30 September 2021, OVIC commenced an examination into the privacy and information handling training at Victoria Police. The objective was to examine whether the training provided to Victoria Police personnel meets the requirements of IPP 4.1 under the PDP Act. IPP 4.1 outlines that an organisation must take reasonable steps to protect the personal information it holds from misuse and loss, and from unauthorised access, modification, or disclosure.

During this examination, OVIC gathered information from relevant Victoria Police personnel on how training is developed, delivered, and evaluated. This focussed on information handling and privacy both generally and in the context of family violence investigations.

The examination found that as of February 2022, Victoria Police had not provided any privacy-specific training to its members for more than a year.[69] The examination also found a lack of resources within its Privacy Unit and Education Unit. Victoria Police has accepted the findings of the examination and has provided further resourcing to its privacy team. It has also undertaken to review privacy and information handling education annually. OVIC will continue its engagement with Victoria Police to promote, support, and ensure reasonable steps are taken to protect the personal information of Victorians.

FOI investigations, audits, reviews and examinations

Under section 61O of the *Freedom of Information 1982* (Vic) (**FOI Act**), the Information Commissioner may, on the Commissioner's own motion, investigate the failure by an agency or principal officer to perform or exercise a function or obligation.

While the following regulatory activities centre upon public access (otherwise referred to as freedom of information) reviews, investigations or audits, they offer complementary insights and benefits to information security stakeholders. This is based upon the shared concerns of maintaining the confidentiality, integrity and, most importantly for FOI, the availability of public sector information.

Public access processes often expose how information is handled, stored and disclosed, revealing gaps and opportunities in an organisation's broader information security practices. Shared stakeholders are prompted to consider outcomes of these regulatory activities and perform updated risk assessments to help mature their information and data management strategies.

[68] To read the report, please visit: https://ovic.vic.gov.au/regulatory-action/investigation-into-datatime-services-pty-ltd-data-breach/

[69] To read the examination, please visit: https://ovic.vic.gov.au/mediarelease/examination-report-into-privacy-and-information-handling-training-at-victoria-police-published/

Process versus Outcome: Investigation into VicForests' handling of a series of FOI requests (2022)

The Information Commissioner commenced an investigation into VicForests' handling of a series of FOI requests on 16 March 2022. The objective of the investigation was to determine whether VicForests complied with the FOI Act and the Professional Standards in the handling of the FOI requests, and in its dealings with the Information Commissioner in relation to the handling of a complaint made against VicForests. The investigation report was tabled in the Victorian Parliament on 8 March 2023. [70]

At the time of the report, OVIC found that VicForests focussed on technical legal processes above other considerations and missed opportunities to help the applicant make a valid FOI request. This came at the expense of providing fair access to information. Based on these matters, the Commissioner found that VicForests acted inconsistently with its responsibility under sections 3 and 16(1) of the FOI Act to make the maximum amount of government information available promptly and inexpensively to the public.

OVIC notes that there are lessons for all Victorian government agencies and statutory authorities in the investigation report. Organisations should provide the mechanisms for Victorians to access government information about themselves quickly and easily, balanced with the appropriate protections as outlined under the VPDSS.

Investigation into impediments to timely freedom of information (2020)

On 15 September 2020, OVIC commenced an investigation to identify factors contributing to delay in the release of government-held information in Victoria under the FOI Act. This own motion investigation is the first of its kind to be undertaken under the FOI Act.

The objective of the investigation was to examine the FOI practices of 5 Victorian agencies to identify the factors contributing to delayed FOI decision-making and information release at those agencies, and to make findings and recommendations to improve the timeliness of FOI decision-making at those agencies and across Victoria generally. The Own Motion Investigation Report was tabled in the Victorian Parliament on 1 September 2021.[71]

In 2022, OVIC released a subsequent report reflecting on the follow-up actions of the examined agencies.[72] At the time of writing, the Information Commissioner noted that of the 5 agencies subject to the investigation, 2 showed a marked improvement in timeliness in FOI decision-making over the 12 months since the report was tabled. The remaining 3 agencies continued to experience significant delays.

Authorised and timely access to information is a central tenant of the VPDSS. OVIC encourages organisations to consider the intersecting nature of the PDP Act and FOI Act requirements and the subsequent obligations in the framing of their information security programs.

Regulatory activities of other Victorian Government oversight and integrity bodies

In addition to the regulatory work that OVIC performs, the regulatory programs of other Victorian government oversight and integrity bodies hold significant relevance to OVIC's work. These bodies often probe or investigate issues related to the transparency, accountability and use of information, as well as looking into issues relating to governance, and risk management – all of which intersect with OVIC's responsibilities.

Findings, recommendations and enforcement actions falling from these oversight bodies highlight emerging risks and often point to best practice that can be adopted by our often-shared stakeholder base. A sample of some of these bodies' more recent reviews that also have a direct relationship to VPDSS activities are captured below.

[70] To read the investigation report, please visit https://ovic.vic.gov.au/wp-content/uploads/2023/03/Process-versus-Outcome-Investigation-into-VicForests-handling-of-a-series-of-FOI-requests.pdf

[71] To read the own motion report, please visit: https://ovic.vic.gov.au/regulatory-action/own-motion-investigation-report-impediments-to-timely-foi-and-information-release/

[72] To read this report, please visit: https://ovic.vic.gov.au/wp-content/uploads/2022/10/IOC-%E2%80%93-Impediments-to-timely-FOI-and-information-release-twelve-months-on-Report.pdf

Investigation - Operation Turton (2024)

In September 2024, the IBAC tabled special report Operation Turton which investigated allegations of unauthorised access and disclosure of sensitive information by employees of the Metropolitan Fire Brigade (**MFB**). IBAC identified 5 separate instances where MFB employees accessed or disclosed sensitive information without authorisation. This led to privacy breaches, compromised internal investigations and prevented MFB from operating effectively. IBAC made recommendations to improve workplace culture and information security.[73] The MFB was replaced by Fire Rescue Victoria (**FRV**) on July 1, 2020, as a result of the Fire Services Reform in Victoria, which amalgamated parts of the MFB and the Country Fire Authority. Recommendations made by IBAC call on FRV to consult with OVIC on the adequacy of its information security under the PDP Act. OVIC is working with FRV on this matter.

Investigation - Operation Grey (2021)

In June 2018 IBAC commenced Operation Grey,[74] to investigate allegations of false record keeping by senior staff within the Dispute Settlement Centre of Victoria (**DSCV**), an agency of the then Department of Justice and Regulation to meet performance targets.

It was alleged that senior staff at DSCV improperly caused false reporting on a Victorian Government Budget Paper No. 3 (**BP3**) performance measure during the 2017-18 financial year. The performance measure related to the number dispute resolution advisory services DSCV provides annually. IBAC's investigation confirmed that data had been modified but did not substantiate allegations of corrupt conduct in relation to those modifications, noting there was no evidence of undue pressure by senior managers to meet DSCV's BP3 targets or any wider culture of meeting performance measures at all costs.

Whilst the investigation did identify organisational issues regarding the absence of written authorisation for data modification, a lack of separation of duties and poor management of case deletion scripts used to make bulk modifications to the database. OVIC encourages organisations to consider the vulnerabilities identified during the investigation.

Research reports - Unauthorised access and disclosure of public sector information (2020)

IBAC produced 3 reports on corruption risks related to the unauthorised access and disclosure of information within the VPS,[75] Victoria Police and local government. While Victoria Police and the local government sector form part of the VPS, due to the unique risks of each sector, and the associated need for tailored prevention strategies, IBAC produced individual reports on each.

Unauthorised access and disclosure of public sector information are forms of information misuse and may constitute corrupt conduct. These activities can also enable other corrupt conduct. The reports highlight common risks across the public sector, the factors that drive information misuse, and outlines strategies to prevent and detect misuse. OVIC strongly encourages VPS organisations to consider the details of these reports and integrate any learnings into the development of their information security programs.

[73] To read IBAC's report, please visit: https://www.ibac.vic.gov.au/investigation-uncovers-problematic-culture-at-MFB
[74] To read this report, please visit: https://www.ibac.vic.gov.au/publications-and-resources/article/investigation-summary---operation-grey
[75] To access copies of these reports, please visit: https://www.ibac.vic.gov.au/publications-and-resources/article/research-summary---unauthorised-access-and-disclosure-of-public-sector-information

Investigation into a former youth worker's unauthorised access to private information about children (2022)

The Victorian Ombudsman investigated a former youth worker's unauthorised access to private information about children and published a report in September 2022.

The Ombudsman found that, among other issues, the department's failure to regularly audit user access to information facilitated the extent of the data breach and warnings regarding the need to further scrutinise privacy compliance went unheeded.

As a result, the Ombudsman recommended the *Worker Screening Act 2020* (Vic) be amended to allow officers to consider and act upon other forms of information likely to be relevant to the risk of a person with access. This includes the power to temporarily suspend a person's working with children clearance in limited circumstances.[76]

Insights from this investigation highlight the importance of adopting a risk-based approach to personnel security, the critical steps that need to be accounted for in pre-engagement screening and reinforcing the need for ongoing personnel security management programs across the personnel lifecycle.

Investigation into improper conduct by a Council employee at the Mildura Cemetery Trust (2019)

The report into the investigation (released in 2019)[77] concerned Mildura's Murray Pines and Nichols Point Cemeteries, managed by the Mildura Cemetery Trust. It concerns allegations of:

- illegal exhumations of deceased persons
- conflicts of interests in promoting and selling memorial chairs for personal benefit under the guise of the Trust
- misuse of position
- improper receipts of payments for cemetery services
- allegations of gross incompetence and neglect of professional standards in the operation of a public cemetery's operations.

The Ombudsman's report highlights a lack of internal oversight and governance controls coupled with vulnerabilities in the organisation's information management / information security practices. OVIC encourages organisations to consider these themes when reviewing their own information security risks.

[76] To read the Victorian Ombudsman's report, please visit: https://www.ombudsman.vic.gov.au/our-impact/investigation-reports/investigation-into-a-former-youth-workers-unauthorised-access-to-private-information-about-children/#
[77] To read this report, please visit: https://www.ombudsman.vic.gov.au/our-impact/investigation-reports/investigation-into-improper-conduct-by-a-council-employee-at-the-mildura-cemetery-trust#cemetery-trusts

Cybersecurity: Cloud Computing Products (2023)

In August 2023, the Victorian Auditor-General's Office (**VAGO**) conducted an audit, Cybersecurity: Cloud Computing Products, examining the effectiveness of agencies' Microsoft 365 cloud-based identity and device management controls. VAGO noted that 'cybersecurity threats in Victoria are real and growing. The Department of Premier and Cabinet reported that 90 per cent of Victorian Government agencies experienced cybersecurity incidents last year.'

Outcomes of the audit included an assessment that the audited agencies' Microsoft 365 cloud-based identity and device controls were not fully effective.[78]

Insights from this audit can help inform the development of organisation's ICT and third-party assurance programs which are critical to the VPDSS.

Security of Government Buildings (2019)

In 2019, VAGO conducted an audit on the physical security, as it related to protective security, which also included information and personnel security. The audit assessed whether DTF (the lead agency responsible for coordinating office accommodation for its government clients across Victoria) provided sound and timely guidelines and support to agencies. They further assessed whether current security arrangements at 2 sample agencies were able to withstand unauthorised access and antisocial behaviour. VAGO undertook a series of covert tests of physical security measures, access control and security culture, at a selection of occupied government buildings.

The security infrastructure at the facilities VAGO examined was deemed adequate, but its effectiveness as a deterrent to unauthorised access was undermined by human error, enabled by a weak security culture. This weak security culture among government staff was a significant and present risk that they noted must be urgently addressed.

At one site, VAGO noted that its auditors were able to access 'discarded, sensitive information too easily. Unauthorised access to sensitive information has the potential to jeopardise the welfare and anonymity of already vulnerable government clients.' [79]

In its report VAGO expressed concern that there was 'no clear, strategic leader for policy, oversight and coordination of the 3 domains of protective security across government agencies. This precludes the better integration and coordination of protective security arrangements.'

OVIC encourages organisations to consider outcomes of this audit report when assessing their physical security risks. This is complemented with efforts that need to be made around the training and awareness of personnel, whilst critically considering the management of third-party risks.

[78] To read VAGO's report, please visit: https://www.audit.vic.gov.au/report/cybersecurity-cloud-computing-products?section=
[79] To read the report, please visit: https://www.audit.vic.gov.au/report/security-government-buildings?section=#page-anchor

Chapter 4
Business Engagement and Outreach Program

OVIC's Information Security Unit (**ISU**) has built an effective business engagement outreach program that is focused on enhancing stakeholders' understanding of Part 4 of the PDP Act, the Victorian Protective Data Security Standards (**VPDSS**) and Victorian Protective Data Security Framework (**VPDSF**), as well as supporting OVIC's broader monitoring and assurance functions. The program is designed to build strong relationships with stakeholders across VPS and industry, offering personalised interactions strengthening OVIC's role as a key integrity body.

The team supporting this program delivers Victorian Information Security Network (**VISN**) forums and events, proactively reaches out to individual stakeholders to discuss issues or themes and helps develop new products. The team has conducted 12 VISNs over the last 4 years with topics ranging from public sector insights to legislative reporting. In addition to this, the ISU responds to a vast array of enquiries, facilitates meetings and discussions across the VPS and participates in networks, forums and training sessions of partnering agencies, regulated organisations and industry events. The team seeks out opportunities with other regulators and integrity bodies, as well as industry groups, ensuring consistent information security messaging.

The ISU also takes part in various external information sessions, public sector reference groups, roundtables and committees. OVIC's continued engagement in these local, national, and international settings ensures we maintain our standing as an active leader in the information security community and a trusted advisor to the Victorian government.

The program

OVIC's Information Security Unit

As part of the outreach program, the ISU is tasked with identifying and monitoring organisations subject to Parts 4 and 5 of the PDP Act. This includes gathering detailed information regarding an organisation's formation, functions and establishment. The administrative overhead of tracking organisations establishment or cessations, coupled applicability assessments under Parts 4 and 5, requires ongoing consideration. The ever-changing landscape of the public service (e.g. Machinery of government changes, establishment of new bodies, cessation of existing ones) presents an ongoing challenge for the team to monitor adherence to the Standards. The number of individual organisations captured by Parts 4 and 5 of the Act is projected to increase in the future, subsequently affecting the quantity of work. This is further discussed in Chapter 5 – Futures.

The ISU handles a high volume of requests for repeated introductory sessions where new stakeholders have been recruited by regulated organisations or the responsibility for the information security program transitions to a new business area. In addition to this, the reduction in staffing numbers in regulated organisations can lead to a loss of corporate knowledge. The continuing nature of these consultations illustrates the demand for additional foundational education and training material to be developed for the VPS.

Stakeholders

Newly established or newly identified organisations often require assistance from the ISU. This involves clarification on applicability questions and requests for an outline of the Framework, Standards, accompanying product suite, and reporting obligations to OVIC.[80] Feedback from stakeholders suggests that these sessions prove to be helpful in understanding and meeting their obligations.

OVIC acknowledges that the VPS also faces a vast array of intersecting and competing legal, regulatory and administrative requirements. This can lead to confusion and additional administrative overhead for organisations regulated by Parts 4 and 5 of the PDP Act. Further, machinery of government changes and significant changes to an organisation's operating environment or security risks relevant to the organisation as defined under the PDP Act,[81] affect their ability to consistently and effectively engage in the process of implementing the Standards.

Additionally, stakeholder understanding of the distinction between the requirements set out under Part 3 of the Act (Privacy) and that of Part 4 (Protective Data Security / Information Security) and Part 5 (Law Enforcement Data Security), can lead to confusion on the interpretation and application of the legislation.

Part 4 of the Act uses particular terms that are often mistakenly conflated with well-established concepts. This can lead to incorrect assumptions about the coverage and application of the VPDSF and VPDSS, notably:

- privacy focus, due to the staging of the name of the Act (Privacy and Data Protection)
- cyber connotations (based on the use of the term 'data' as opposed to information)
- associations with General Data Protection Regulation provisions of Europe, which focus on personal information and privacy protections.

OVIC acknowledges that the level of understanding and maturity varies greatly across our stakeholder base and these confusions are not shared by all.

External Factors

As described in Part 4 of the Act, the ISU's product needs to reflect and remain consistent with national and international standards. As such, the team is guided by, and makes reference to, various external control sources that have their own lifecycle (ISM, PDSP, AS/ISO). These resources are often updated, thereby making it necessary to ensure VPDSS and VPDSF material remains responsive to the dynamic threat environment. OVIC's active participation in local, national, and international working groups, forums and committees provides an opportunity to continually advocate for VPS organisations and shared stakeholders. It also ensures material continually promotes best practice and reduces the regulatory burden on VPS organisations where possible.

[80] The *Five Step Action Plan* resource outlines practical activities designed to assist in managing information security risks in a cyclical nature. It is designed to support information security practitioners and inform executive leadership of an organisation's ongoing activities. To read more, please visit: https://ovic.vic.gov.au/resource/the-five-step-action-plan/.

[81] *Privacy and Data Protection Act 2014* (Vic), section 89(4).

ISU Performance Statistics

The ISU captures data from outreach and engagements per financial year. We monitor the number of enquiries and consultations, as well as hosting multiple VISN events every year, whilst receiving, processing and analysing hundreds of PDSP/attestations per reporting cycle.

Enquiries

2020/21 - *Attestation year*

3,505

2021/22 - *PDSP year*

2,404

2022/23 - *Attestation year*

1,997*

2023/24 - *PDSP year*

3,067

Consultations

2020/21 - *Attestation year*

397 (Inclusive of 56 PDSP Insights sessions)

2021/22 - *PDSP year*

356

2022/23 - *Attestation year*

245 (Inclusive of 23 PDSP Insights sessions)

2023/24 - *PDSP year*

323

Statistics presented across the years, speak to the significant demand placed on ISU.

Of note, the number of enquiries received by OVIC relating to information security obligations tends to change based on the reporting cycle for that period (i.e., attestation year or PDSP year). Enquiries also fluctuate when guidance and product are released, as well as machinery of government changes and 'significant change' notifications by organisations.

** Whilst these numbers are reflective of the majority of interactions handled by the team, they are not all encompassing. In more recent years the team has refined its internal processes, moving away from more manual administrative tracking to a more automated method. This automation has improved the efficiency and effectiveness of the team and led to more accurate data collection.*

ISU conducted an average of 330 consultations per year, at roughly 45 minutes per session.

Conservatively, this amounts to a total of 248 hours per year, generally attended by 2 ISU resources.

As noted above, the number of consultations can vary depending on the reporting cycle, product releases or regulatory activities being performed by OVIC.

Chapter 5
Futures

As an integrity and oversight body, OVIC is committed to continuously improving our product suite and accompanying business engagement and outreach program, promoting the highest information security standards across the VPS.

As an office, we aim to evolve and enhance key VPDSS and VPDSF products by leveraging data-driven insights drawn from stakeholder feedback, regulatory activities and supporting business intelligence. OVIC continues to work on streamlining internal processes and increasing transparency in the work we do, building public trust in our brand and ensuring we respond to the dynamic threat environment.

We are committed to helping build a secure VPS to meet future information security demands. The context in which we operate continues to evolve with the advancement of new technologies and the continued release of new administrative, legal and regulatory requirements for organisations. Strong and sustained support is critical to ensuring OVIC has the resources, legislative support and policy alignment needed to secure public sector information and systems.

Where to next?

The case for legislative reform

Under section 85 of the PDP Act, the Information Commissioner may review or amend the VPDSF, ensuring it is consistent with other information security standards, including international standards.

As part of ensuring the VPDSF is consistent and up to date with Australian and international standards, OVIC has proposed several strategic reforms to the PDP Act, including:

- implementation of a mandatory incident notification scheme that establishes the requirement for VPS organisations to notify OVIC of certain incidents, including requiring the organisation to notify affected individuals in the case of potential harm
- extend and clarify the organisations captured by Part 4 of the PDP Act to explicitly and clearly include local government, universities, hospitals and health service providers
- power to issue a compliance notice for entities who fail to meet reporting requirements
- power to access or compel the disclosure of information for audits, examinations and investigations.

If supported by government, these pieces of legislative reform would increase the efficiency and effectiveness of OVIC and promote a more consistent application of information security practices across the VPS.

Proposed VPDSF and VPDSS product reforms

In our commitment to continuously improving our product suite, OVIC has an ongoing program to consider the currency and relevance of key resources supporting the VPDSS and VPDSF. Historically, this has included updates to the:

Victorian Protective Data Security Framework

(the Framework or VPDSF)

The first version of the Framework (V1.0) was released in 2016 under the former Privacy and Data Protection Commissioner, David Watts.

In 2018, the Office of the Commissioner for Privacy and Data Protection (**CPDP**) merged with the Office of the Freedom of Information Commissioner (**FOIC**) ushering in the role of Victoria's first Information Commissioner, held by Sven Bluemmel. Following this merger, the team critically considered the Framework's content and released a step-change version (V1.1) to the document, including the release of a foreword by the inaugural Privacy and Data Protection Deputy Commissioner, Rachel Dixon.

A wholesale review of the Framework was completed in 2020, in conjunction with the release of the updated Standards. The review focused on ensuring the content reflected the monitoring and assurance activities of VPS organisations and OVIC, including a refreshed Commissioner's foreword.

In 2023, OVIC released an update to the Framework which included minor amendments to ensure the currency of references, clarification on the scope of the Framework to include 'public sector information' and 'information systems', and an updated Commissioner's foreword.

OVIC intends to review the Framework under the direction of the new Information Commissioner, Sean Morrison.

Victorian Protective Data Security Standards

(the Standards or VPDSS)

The VPDSS were first issued in 2016, under the former Privacy and Data Protection Commissioner, David Watts.

In 2019, OVIC recast the Standards and released VPDSS V2.0 as well as supplementary material taking the form of VPDSS Implementation Guidance.[82] This product release included:

- merging 18 mandatory Standards down to 12
- removing former 'protocols' and introduction of supporting 'elements'
- mapping the new elements to primary control sources.

In 2021 and 2023, further revisions were made to the VPDSS Implementation Guidance with a view to maintain currency of source material and add / adjust relevant elements as needed.

Following the review of PDSPs in the 2024 reporting cycle and feedback from stakeholders, OVIC signalled an intention to reform the VPDSS with a view to uplift and renew the full product suite.

In communications to our stakeholders, OVIC signalled that the review would focus on maintaining currency of the Standards and offer clarity to users on what is expected from them. The release of the revised suite of resources will precede any education and training needed following the reissue of the Standards.

OVIC will engage in formal consultation with impacted organisations to ensure that due consideration is given to the voices of different cohorts. This will enable the revised resources to reflect those cohorts' varying resources and maturity levels.

[82] The VPDSS Implementation Guide is available here https://ovic.vic.gov.au/information-security/victorian-protective-data-security-standards-implementation-guidance/.

Protective Data Security Plan (templates)

To coincide with the release of VPDSS 1.0, OVIC published a 'high-level' PDSP template (including attestation) in 2018. Organisations used this high-level PDSP template to account for either single or multiple organisations' reporting (multi-organisation PDSP). This combined reporting was designed to support scenarios where subsidiary organisations effectively operated as a business unit of the primary organisation. However, OVIC noted a range of issues following a review of the 2018 and 2020 PDSP returns. These related to the identification and management of information security risks of subsidiary organisations versus those of a primary organisation. Additional issues centred on different control environments which, in some cases, were not reflected in multi-organisation PDSPs.

In 2022 OVIC strengthened the multi-organisation PDSP reporting model, requiring all organisations (primary and subsidiaries) to seek approval from OVIC prior to adopting the model, and to confirm all parties' ability to meet certain PDSP reporting criteria. This strengthened approach resulted in more targeted insights from smaller subsidiary organisations that had not meaningfully engaged in PDSP reporting prior.

OVIC seeks to deliver efficient, effective and economic analysis of PDSPs and enhance monitoring and assurance efforts.

VPDSS reporting models

Product reform plays a key role in modernising outdated approaches. It incorporates new evidence and technologies and ensures our regulatory tools remain fit for purpose. Given the volume of organisations that are subject to Part 4 of the PDP Act, the ISU is assessing current reporting models to enhance OVIC's visibility of information security practices across the VPS.

School / School councils integrated schools

As reported by Victorian Auditor General's Office (**VAGO**) in their 2018 audit of school councils in government schools, the Auditor-General acknowledged the complex and unique governance framework that government schools operate in. This unique operating context introduces information security risks.

Whilst this audit operated as a backdrop, OVIC held additional concerns regarding the lack of nuanced insight into information security risks and practices of these different operating environments and worked with the Department of Education (**DE**) on a revised reporting model to address this.

OVIC has worked closely with DE as a regulated organisation, having historically submitted 2 multi-organisation PDSPs to OVIC:

- DE 'Corporate', representing the Department and over 1,500 school environments and equivalent subsidiary entities
- DE school councils, representing over 1,500 school councils.

In 2023, OVIC and DE entered into a revised reporting model that is set to conclude in 2028. Under this model, DE will provide an annual PDSP to OVIC that will provide improved visibility and insight into school information security practices.

In 2024, 102 schools (and school councils) were integrated into this model, reflecting the information security program of nominated schools and school councils, as well as broader DE corporate reporting. A further 105 (totalling 207) are due to report in 2025.

Class B Cemetery Trusts

In 2020 the ISU drafted bespoke requirements to reflect the unique operating and governance arrangements of the then 483 Class B Cemetery Trusts (**Class Bs**). The ISU worked closely with representatives from the sector in framing the requirements in the Class B PDSP reporting template.

Tailored products for this sector included contextualised language to suit the stakeholder base and reduced reporting requirements for Class Bs. At the time, the ISU consulted with key stakeholders from select Class B cemeteries, the Cemeteries and Crematoria Association of Victoria (**CCAV**) and the Department of Health (**DH**). Each stakeholder group offered helpful feedback and informed the development of the product.

The ISU will continue to work with the DH Cemetery Sector Governance Support Unit when refreshing Class B requirements and reporting material.

Committees of Management

The Department of Energy, Environment and Climate Action (**DEECA**) oversees approximately 1,500 Crown land reserves in Victoria, managed by roughly 978 Voluntary Committees of Management (**CoMs**) confirmed as in scope for Part 4 PDP Act. These CoMs are public entities under the *Public Administration Act 2004* (Vic) and as such have been captured by Part 4 of the PDP Act.

In November 2024, OVIC met with DEECA who oversee the operation of these CoMs to gain an updated insight into the numbers and extent of these entities. OVIC appreciates the help DEECA has provided the ISU to date in helping inform a deeper appreciation of how these entities operate and the tensions that arise with a volunteer cohort. This includes challenges around their understanding of legislative obligations including PDSP reporting.

OVIC understands that this stakeholder base may require tailored resources and additional support much like Class B Cemetery Trusts. OVIC and DEECA are continuing to work together to clearly articulate CoMs' future legislative and reporting obligations.

Clarified roles and responsibilities

As referenced in the VAGO 2019 Security of Government buildings report, auditors noted there was 'no clear, strategic leader for policy, oversight and coordination of the 3 domains of protective security across government agencies. This precludes the better integration and coordination of protective security arrangements.'[83]

Whilst responsible organisations have made efforts to address this since 2019, there is still a lack of clarity around information security roles and responsibilities. Further work is needed in this space to offer clarity to VPS stakeholders on who they should turn to for direction, guidance, and support.

In addition to this, OVIC is interested in collaborating with other oversight bodies to reduce the administrative and reporting burden of VPS organisations. This extends to key Commonwealth agencies and bodies that influence the operation and reporting outcomes for certain VPS organisations.

[83] To read the report, please visit: https://www.audit.vic.gov.au/report/security-government-buildings?section=#page-anchor

Annexure

Report sources, scope and approach

Part 4 of the PDP Act sets out public sector agencies, special bodies,[84] and other bodies as regulated organisations with information security obligations. Currently 3387 organisations are deemed to be captured under Part 4 of the Act. [85]

Sources of insights

In writing this report, OVIC has considered analysis of, and reflection on:

- Protective Data Security Plan (**PDSP**) submissions of reporting organisations across 2022 and 2024
- information security incident notifications to OVIC
- audits, reviews, investigations conducted by OVIC
- audits, reviews and publications of other Victorian government integrity and oversight bodies
- business engagement and outreach activities undertaken by OVIC's Information Security Unit (**ISU**).

In addition to this, areas of this report draw on monitoring and assurance activities beyond the 2-year window and at times reflect on information security practices of organisations that are not directly regulated by Part 4 of the PDP Act, but opt to participate in reporting programs and schemes.

These are known as 'reporting organisations.'

Protective Data Security Plans

This report utilises data directly drawn from PDSPs submitted to OVIC by reporting organisations between 2022 and 2024.

Regulated organisations are required to submit a PDSP to OVIC, however, OVIC also receives voluntary PDSP submissions to OVIC by other Victorian organisations to support best practice. These are included in this report.

Information Security Incidents

This report presents statistics drawn from information security incident notifications submitted to OVIC across this same timeframe (2022 – 2024). In total, OVIC received 1428 incident notifications.

Of these, 56 incidents were reported by organisations that were not regulated by Parts 4 or 5 of the PDP Act.

3 incidents were reported by organisations that did not submit a PDSP to OVIC in 2024.

Audits

To date, OVIC has conducted 3 audits relating to the VPDSS, considering the information security activities of 4 organisations per audit.

[84] *Public Administration Act 2004* (Vic).
[85] Number as of April 2025, subject to change.

Scope of PDSP analysis

Number of organisations included in the analysis

The PDSP statistics in this document draw from

- the 360 organisations that submitted a PDSP to OVIC before 31 October 2024,[86] and
- 316 organisations that submitted a PDSP to OVIC in both 2024 and 2022.[87]

This includes organisations that submitted via a single organisation or multi-organisation PDSP, as either the primary or the subsidiary organisation.

PDSP multi-organisational reporting model

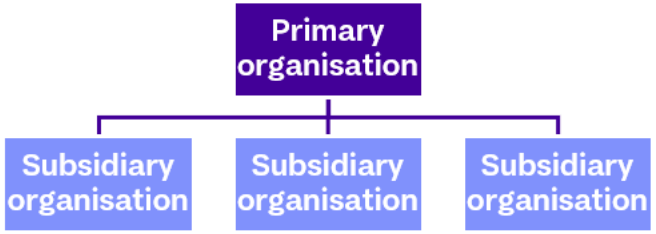
The multi-organisation reporting model was designed to support scenarios where subsidiary organisations have equivalent risk profiles (including appetite and tolerance), risk references, control environments, implementation statuses, completion dates for the elements, and maturity levels to those of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

Following analysis of the 2018, 2020 and 2022 multi-organisation PDSP submissions, OVIC identified concerns around the unique conditions of subsidiary organisations to that of their primary organisation.

In some cases, these differences were not catered for in multi-organisation PDSPs, highlighting concerns around the identification and management of the information security risks of the subsidiary and primary organisations.

To address these issues, OVIC further strengthened the multi-organisation reporting model in 2024. This model required all organisations (primary and subsidiaries) seeking to use the model to meet certain reporting criteria before proceeding.

In the 2024 reporting cycle, this strengthened reporting model continued, and relevant data is incorporated in this report.[88]



PDSP data excluded from this report

This report excludes PDSP data from:

- any PDSPs received after 31 October 2024 from organisations (12)
- Class B Cemetery Trusts (465) submitting a PDSP using an alternative reporting template and material
- Schools / School Councils (1571) operating under the Department of Education's central service model and associated reporting program
- some Committees of Management (971)
- one Local Government Authority (1).

PDSP reporting data from these entities cannot currently be standardised and as such, comparisons cannot be made against other reporting organisations.

[86] 2024 PDSP statistics represent data across 360 organisations drawing from 94 reportable VPDSS elements, excluding 4 elements under Standard 9. This figure represents single organisation, and multi-organisation submissions.

[87] 2022 and 2024 PDSP statistics represent data across 316 organisations drawing from 91 reportable VPDSS elements, excluding elements under Standard 9 and elements relating to IACS.

[88] 67 organisations submitted to OVIC under their primary organisations via the multi-organisation reporting model.

Comparisons drawn from 2024 and 2022 PDSP submissions

OVIC analysed 360 organisations that reported in 2024.

316 of those organisations also reported in 2022. Any comparative analysis across these 2 reporting cycles (2022 and 2024) was based on 316 organisations.

Additional comparative analysis exclusions include:

Standard 9

- In 2024, OVIC amended the PDSP form, whereby the public sector body Head attestation in Part C confirms the organisation's implementation of all 4 elements under Standard 9.

Subsidiary organisation data (multi-organisation reporting model)

- The 2022 dataset did not include subsidiary PDSP data and therefore is excluded from any comparative analysis in this report.

IACS Data

- Comparative analysis was also limited by the introduction of 3 new IACS elements (E1.120, E1.130 and E2.100) in the 2024 reporting cycle. Because these elements were not present in 2022 reporting, there is no data for comparison in 2024.

Generative Artificial Intelligence Data

With the rise in the use of Generative Artificial Intelligence, OVIC introduced questions in the 2024 reporting cycle which sought to understand how the VPS was using this technology. As such, no data was available to contrast against 2022 PDSP reporting cycles.

[89] 2024 PDSP statistics represent data across 360 organisations drawing from 94 reportable VPDSS elements, excluding 4 elements under Standard 9. This figure represents single organisation, and multi-organisation submissions.

Approach

PDSP analysis techniques / methods

The PDSP statistics in this document represent quantitative data from reporting organisations, supported by qualitative insights compiled by the ISU. In summary, the graphs in this document represent either:

- 360 organisations that submitted a PDSP before 31 October 2024[89]
- 316 organisations that submitted a PDSP in both 2024 and 2022 and therefore make up the comparative cycle-to-cycle insights.[90]

The ISU's qualitative analysis considered data from a sample of 50 organisations, representative of the fuller 360 reporting organisations in 2024.

Sectors

The 360 organisations that submitted a PDSP in 2024 have been nominally broken into 11 separate sectors. In forming these sectors, the ISU has considered the Victorian Public Sector Commission's existing industry and sub-sector categories, as well as organisations' current departmental portfolios and functions. Sector-based data is displayed in various graphs and insights throughout the report.

Data quality

The data and insights presented in this report are primarily based on self-assessments provided by reporting organisations via their PDSPs and organisations participating in the Scheme. As such, the accuracy and completeness of the information relies on the respondent's own understanding and disclosure. While efforts have been made to interpret the data objectively, the inherent challenges/limitations of self-reported information should be considered when reviewing the insights.

OVIC did note, however, that some organisations failed to understand the inputs needed for PDSP fields relating to risk references, control libraries and IACS elements. These gaps, anomalies and discrepancies are discussed throughout the report.

[90] 2022 and 2024 PDSP statistics represent data across 316 organisations drawing from 91 VPDSS elements, excluding 4 elements under Standard 9 and 3 elements relating to IACS.

OVIC's information security monitoring and assurance

The PDP Act requires OVIC to research, promote, monitor and assure information security of regulated VPS organisations. These activities are designed to help maintain the confidentiality, integrity and availability of Victorian public sector information and systems. OVIC identifies trends, themes and issues through a variety of channels. The channels include:

- PDSP submissions
- incident notifications as a result of VPDSS E9.010
- reports or complaints from the public
- media reports
- monitoring and assurance activities as outlined in our Regulatory Action Policy[91]
- referrals from other regulators
- insights from OVIC's outreach and engagement activities.

Protective Data Security Plans

In 2018, VPS organisations submitted their first PDSPs and attestations to OVIC. These submissions provided OVIC with high-level insight into the state of information security across the VPS. In subsequent years, PDSP reporting continues to deliver important insights into the evolving information security work programs of organisations, as well as an effective way to highlight the challenges they may be facing.

Education, guidance and research

OVIC provides a range of online guidance, tools, templates and other supporting resources. These include videos, FAQs and specific information sheets and guidelines on information security topics. OVIC also undertakes research on information security and law enforcement data security matters.

Preliminary inquiries

When OVIC becomes aware of an information security issue, the office may make preliminary inquiries for further information. Public sector body Heads are required to provide assistance and direct their staff to constructively and transparently assist OVIC.[92]

OVIC works with organisations at the preliminary inquiry stage to try to resolve any information security issues. OVIC may offer non-binding suggestions to improve practices or suggest actions to address non-compliance with the VPDSS. Preliminary inquiries also allow the Information Commissioner to decide whether to conduct further regulatory activity.

Walkthroughs

As part of its Regulatory Action Policy, OVIC has the ability to undertake walkthroughs. Walkthroughs enable OVIC to gain a firsthand appreciation of an organisation's information security program. Walkthroughs may include, but are not limited to, onsite in-person observation of an organisation's facilities, interviews with organisational representatives, documentation or system review, and specific control reviews.

A walkthrough provides OVIC with the opportunity to discuss its observations with the organisation and put forward its findings.

Audits

OVIC conducts audits of organisations to ensure adherence with the VPDSS and compliance with the PDP Act. Audits can be used:

- to investigate non-compliance with the VPDSS or PDP Act
- as a proactive, periodic assurance tool
- to inform research activities
- to target a particular information security issue.

Ministerial reviews

At the request of the Minister, the Information Commissioner must undertake reviews of information security matters and report to the Minister. On receipt of a report, the Minister may table a copy of the report before each House of Parliament.

[91] To read more about OVIC's monitoring and assurance powers and functions, review the 2022 - 2025 Regulatory Action Policy available here - https://ovic.vic.gov.au/regulatory-action/regulatory-action-policy/

[92] *Privacy and Data Protection Act 2014* (Vic), section 110.

Supplementary Insights and Resources

OVIC resources

For more information regarding the OVIC materials and guidance, please visit the ISU Resource Page.

Organisational specific insights – Quantitative statistics

If you require assistance in interpreting this report or would like to discuss your organisation's own PDSP or sector allocation, please reach out directly to the ISU so that we may discuss with your team further.

Email security@ovic.vic.gov.au with an outline of your request.

www.ovic.vic.gov.au