

Victorian Public Sector Insights – Information Security Monitoring and Assurance Report

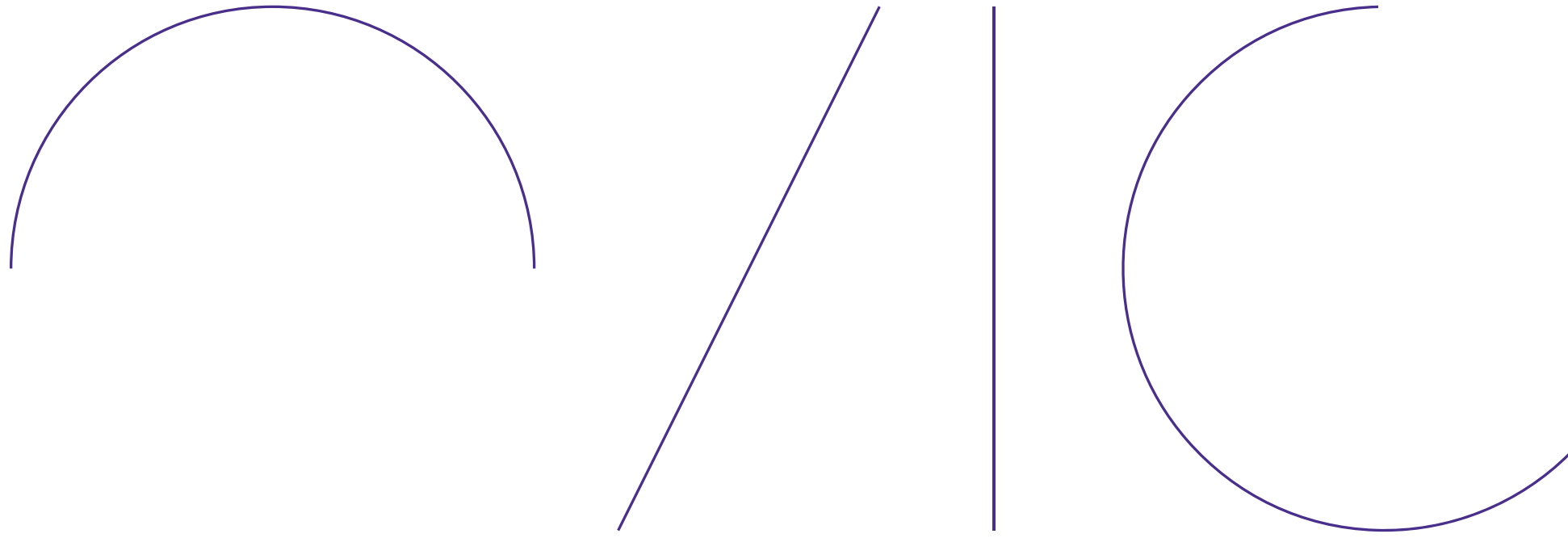
2025

Victorian Information Security Network (**VISN**)

August 2025



A reminder – Today's session
is being recorded.



Acknowledgment of Country

Anthony Corso

Assistant Commissioner –
Information Security

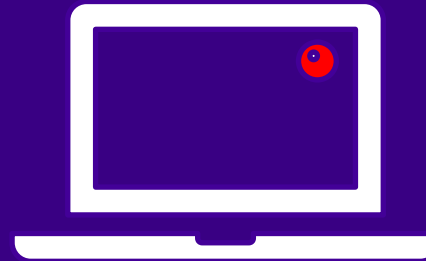
We acknowledge the Wurundjeri people of the Kulin Nation as the Traditional Owners of the land from which we are presenting today.

We pay our respects to their Elders, past and present, and Aboriginal Elders of other communities who may be with us today.

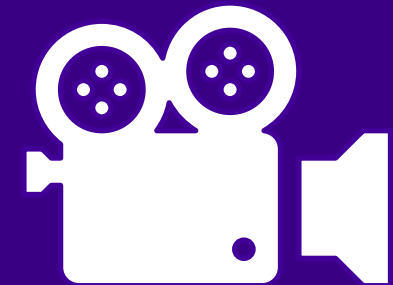
Housekeeping - What to be aware of



Cameras and mics have been **muted** for attendees.

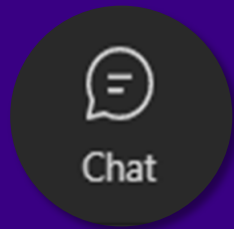


Today's session is **being recorded**.

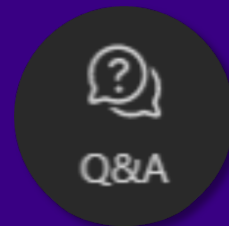


A copy of OVIC's **slides** and the **recording** will be made available in the coming days on our website.

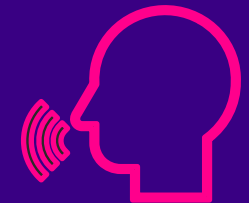
Housekeeping – How to engage



Regular **chat functionality** in Teams is **enabled** in this forum. Your name will be displayed against any questions you post.

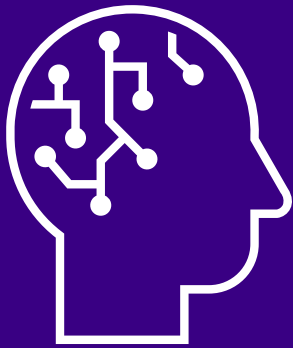


If you want to ask an **anonymous question**, type your question into the **Teams Q&A channel**.



Each speaker will answer questions following the presentation. If you prefer to ask your question verbally, **raise your hand and come off mute when called upon**.

Housekeeping – Use of AI tools



Slides and a recording of this session will be made available in the coming days.

As such, we ask for that no Generative AI tools are used to take notes or record this event. We will remove users/tools who do so.

OVIC's position on the use of generative AI in meetings with OVIC

A PDF document of this information is available to view and download [here](#).

This article outlines the Office of the Victorian Information Commissioner's (**OVIC**) position on the use of generative AI tools including AI notetakers, in meetings between OVIC's staff and OVIC's stakeholders.

OVIC's stakeholders may include Victorian public sector organisations, local councils, contracted service providers, consultants, Members of Parliament, interstate and international colleagues, and members of the public.

OVIC's staff includes OVIC employees and statutory office holders.

<https://go.vic.gov.au/4fM3O3t>

Sean Morrison
Information Commissioner

Information Commissioner's reflection – Data Protection (Information Security)

2014

The PDP Act

On 3 September 2014 the PDP Act came into operation.

2016 - 2018

First high level PDSP submissions

Regulated organisations were required to submit a high level PDSP to address 18 Standards that were issued in 2016.

2020 - 2024

Move to VPDSS 2.0

Following an independent review and active stakeholder engagement, VPDSS 2.0 was issued. This reflects our commitment to continuous improvement and responsiveness to stakeholders.

Now > Future

Intelligence led monitoring and assurance

We've been listening and we want to ensure the future of the VPDSS is fit for purpose. OVIC is looking to continue to refine our products as well as our monitoring and assurance approach.



Victorian Public Sector Insights – Information Security Monitoring & Assurance Report

This report presents insights derived from information security assurance activities of regulated VPS organisations.



Futures

November 2024 OVIC signalled the commencement of a review of the VPDSS designed to ensure currency and to uplift the fuller product suite.

Today's agenda

What we'll explore today



Introduction of the VPS Insights – Information Security Monitoring and Assurance Insights report



General observations drawn from the report



Implementation of the Standards



Incident Insights



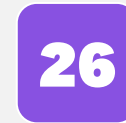
Audits, Investigations and Reviews



Engagement



Futures



What to expect for 2026 PDSP reporting



Questions

Victorian Public Sector Insights – Information Security Monitoring And Assurance - 2025 Report

Setting the tone

Part 4 of the *Privacy and Data Protection Act* requires VPS organisations to:

- adhere to the Victorian Protective Data Security Standards (VPDSS or the Standards)
- undertake a Security Risk Profile Assessment (SRPA)
- develop, implement, and maintain a Protective Data Security Plan (PDSP)
- submit a current copy of its PDSP to OVIC
- provide OVIC free and full access to public sector information and information systems, when requested, including participating in any monitoring and assurance activities conducted by OVIC
- ensure that a contracted service provider of a VPS organisation, does not do an act or engage in a practice that contravenes the Standards, regarding public sector information collected, held, used, managed, disclosed, or transferred by the provider for the VPS organisation



Increasing reach, strengthening oversight in 2024

3,300
organisations

approximately **captured** by
Part 4 of the *Privacy and
Data Protection Act 2014*
(Vic)

Authorised Version No. 027	
Privacy and Data Protection Act 2014	
No. 60 of 2014	
Authorised Version incorporating amendments as at 26 April 2021	
TABLE OF PROVISIONS	
Section	Page
Part 1—Preliminary	1
1 Purposes	1
2 Commencement	1
3 Definitions	2
4 Interpretation	12
5 Objects	13
6 Relationship of this Act to other laws	14
7 Rights and liabilities	14
8 Act binds the Crown	14
Part 1A—Functions, powers of Information Commissioner and appointment of Privacy and Data Protection Deputy Commissioner	15
Division 1—Performance of functions	15
8A Functions of Information Commissioner	15
8B Functions of Privacy and Data Protection Deputy Commissioner	16
8C Information privacy functions	17
8D Protective data security and law enforcement data security functions	19
Privacy and Data Protection Act 2014	20
No. 60 of 2014	20
Part 4—Protective data security	22
Part 4—Protective data security	22
Division 1—Application of Part	22
84 Application of Part	23
(1) Subject to subsection (2), this Part applies to—	
(a) a public sector agency; and	
(b) a body that is a special body, within the meaning of section 6 of the Public Administration Act 2004 ; and	
(c) a body declared under subsection (3) to be a body to which this Part applies.	

84%

of PDSP submissions
received **on time** in 2024

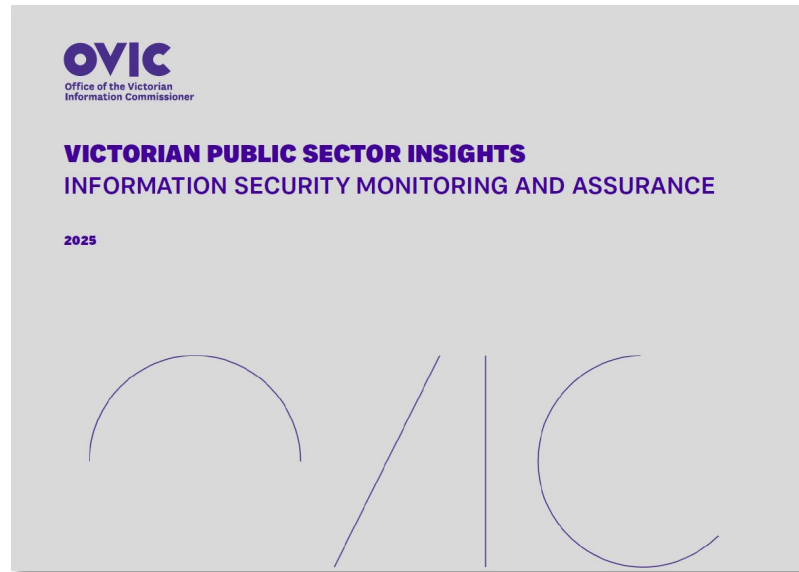
On time submissions
increased by

+6%
from 2022

1.8%

of organisations did not
submit a PDSP in 2024 and
are considered **non-
compliant**

Insights from 2024 PDSP submissions



The report was published in August and is available on the OVIC website.

<https://go.vic.gov.au/4mtDSMr>

Overview of the Report

Contents

1. PDSP Insights

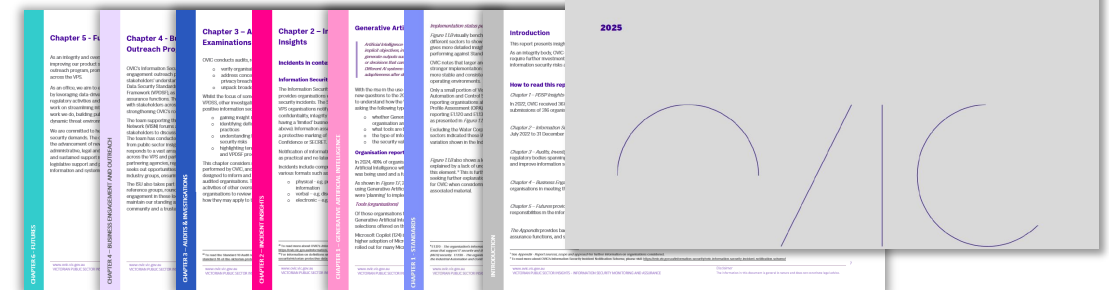
- Standards
- Generative AI Insights

2. Incident Insights

3. Audits, Investigations, Examinations and Reviews

4. Business Engagement

5. Futures



The basis of our insights from 2024 submissions

Quantitative Review

360
organisations

were **quantitatively analysed** from 2024 PDSP submissions

The 360 organisations have been **split** into

11
sectors

316
organisations

submitted a PDSP in both 2022 and 2024, enabling **comparative analysis**

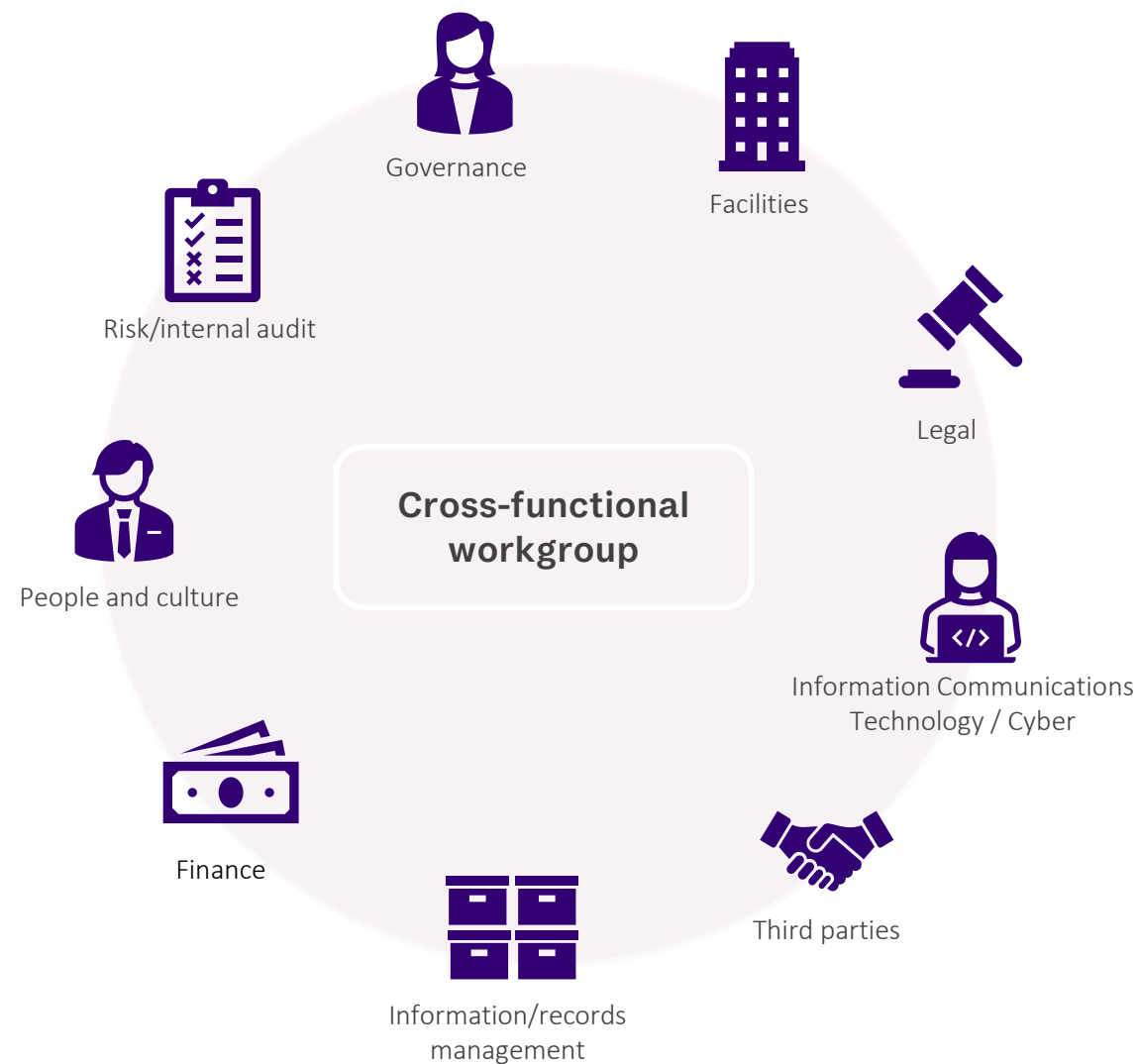
Qualitative Review

50
PDSPs

from 2024 were selected for **qualitative analysis**

*General observations drawn
from the report*

Information security: an organisation wide responsibility



Security is recognised as a shared business priority



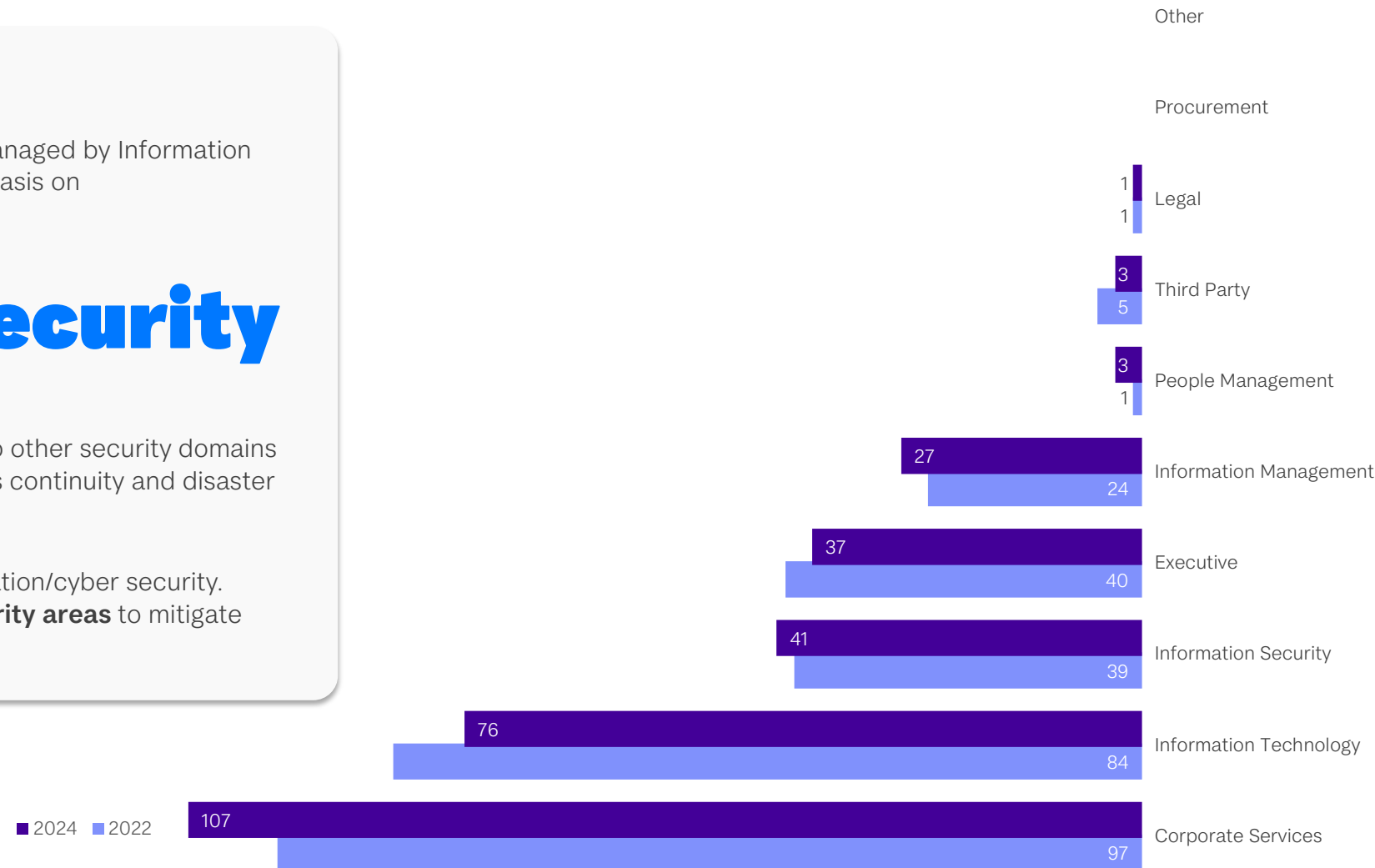
Qualitative Analysis finding

Often OVIC saw organisations whose program was managed by Information Technology or Corporate Services had a strong emphasis on

ICT or Cyber Security

This bias may indicate less consideration was given to other security domains such as personnel, governance, physical and business continuity and disaster recovery.

ICT controls alone will not holistically address information/cyber security. Organisations need to consider **all information security areas** to mitigate security risks.



Turning challenges into actionable insights

Qualitative Analysis findings

Many organisations reported as being impacted by a machinery of government in January 2023 leading to a rise in the selection of **significant changes** and **machinery of government**.

Government budgets have tightened across the VPS leading to more organisations selecting **financial** as a challenge or barrier.

As organisations' have become more familiar with the Standards there has been a clear decrease in the selection of **lack of clarity around roles and responsibilities**, **capability** and **lack of understanding of the Standards**.

2022 2024



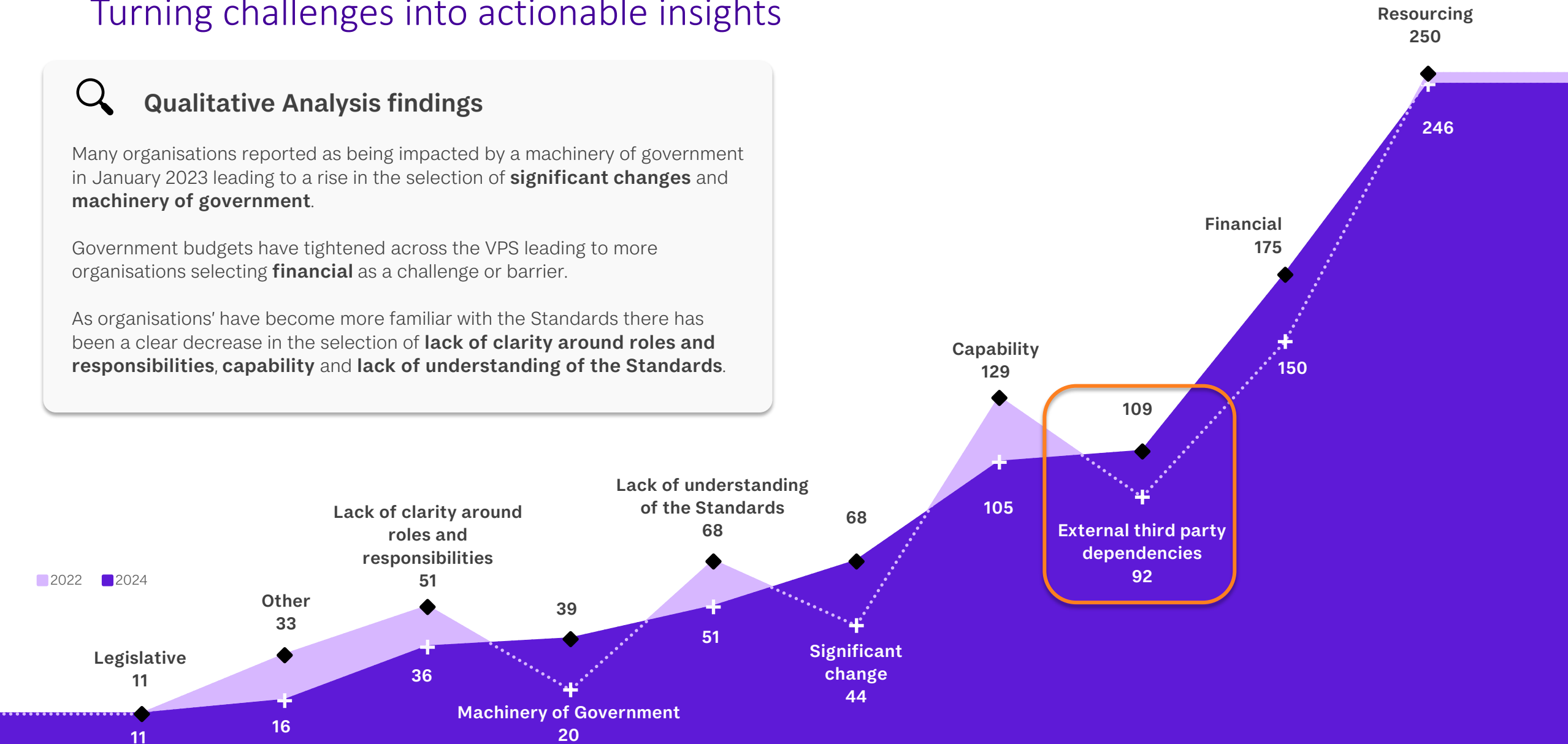
Turning challenges into actionable insights

Qualitative Analysis findings

Many organisations reported as being impacted by a machinery of government in January 2023 leading to a rise in the selection of **significant changes** and **machinery of government**.

Government budgets have tightened across the VPS leading to more organisations selecting **financial** as a challenge or barrier.

As organisations' have become more familiar with the Standards there has been a clear decrease in the selection of **lack of clarity around roles and responsibilities**, **capability** and **lack of understanding of the Standards**.



Turning challenges into actionable insights

Qualitative Analysis findings

Many organisations reported as being impacted by a machinery of government in January 2023 leading to a rise in the selection of **significant changes** and **machinery of government**.

Government budgets have tightened across the VPS leading to more organisations selecting **financial** as a challenge or barrier.

As organisations' have become more familiar with the Standards there has been a clear decrease in the selection of **lack of clarity around roles and responsibilities**, **capability** and **lack of understanding of the Standards**.

2022 2024

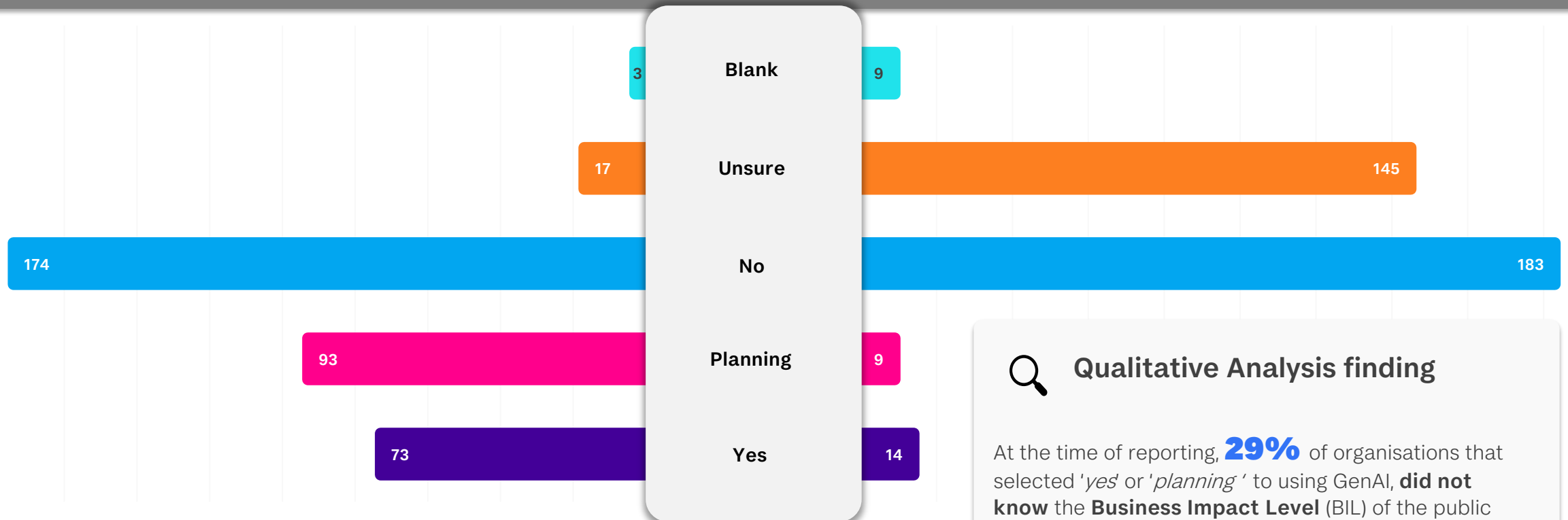


Early days of Generative AI adoption

Organisations'
adoption of Gen AI



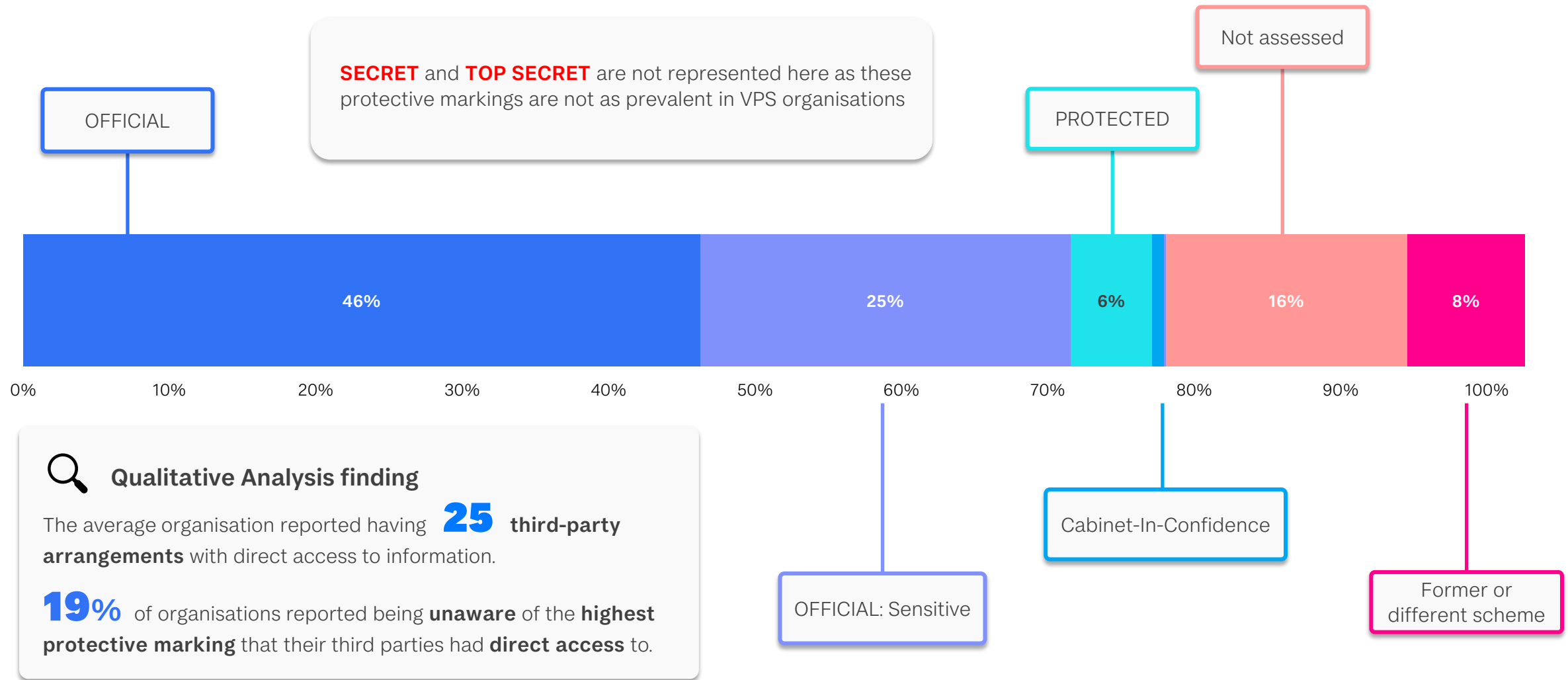
Contracted service providers'
adoption of Gen AI



Qualitative Analysis finding

At the time of reporting, **29%** of organisations that selected 'yes' or 'planning' to using GenAI, **did not know** the **Business Impact Level (BIL)** of the public sector information being used as an input into Large Language Models (LLMs).

You can't protect what you don't know



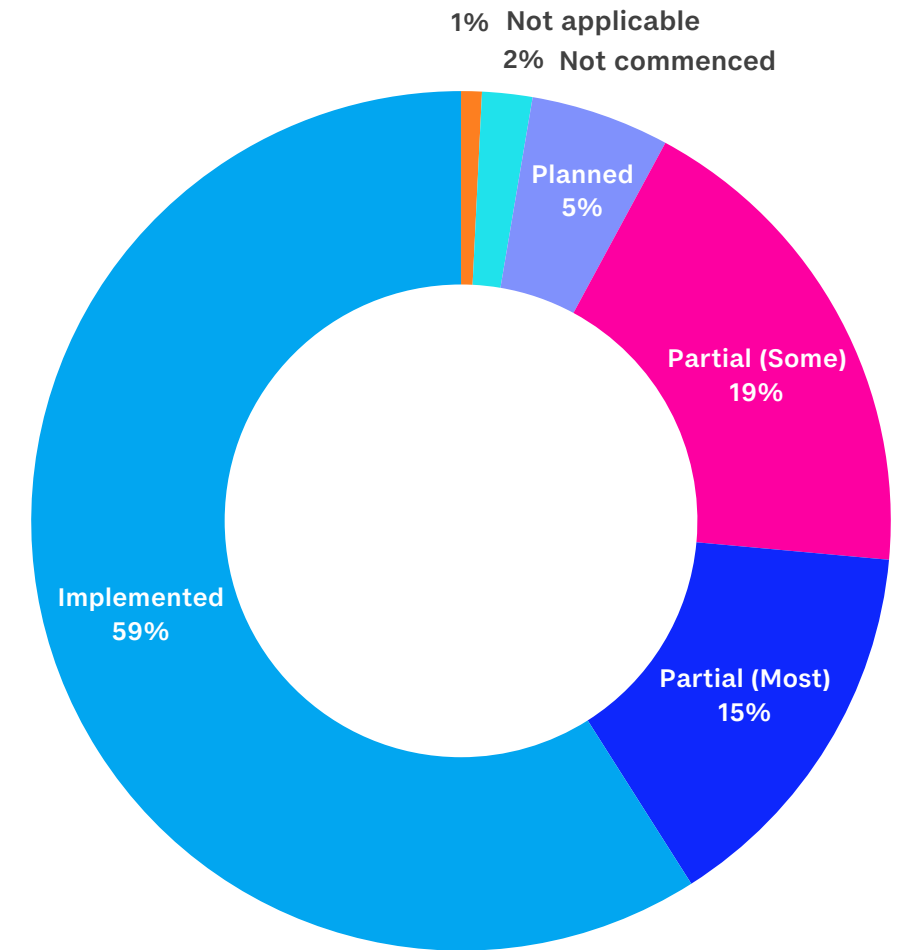
Are you risk informed, or do you focus on compliance? Perhaps it's a bit of both?

Standard 3

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

Benefits of adopting a risk informed approach

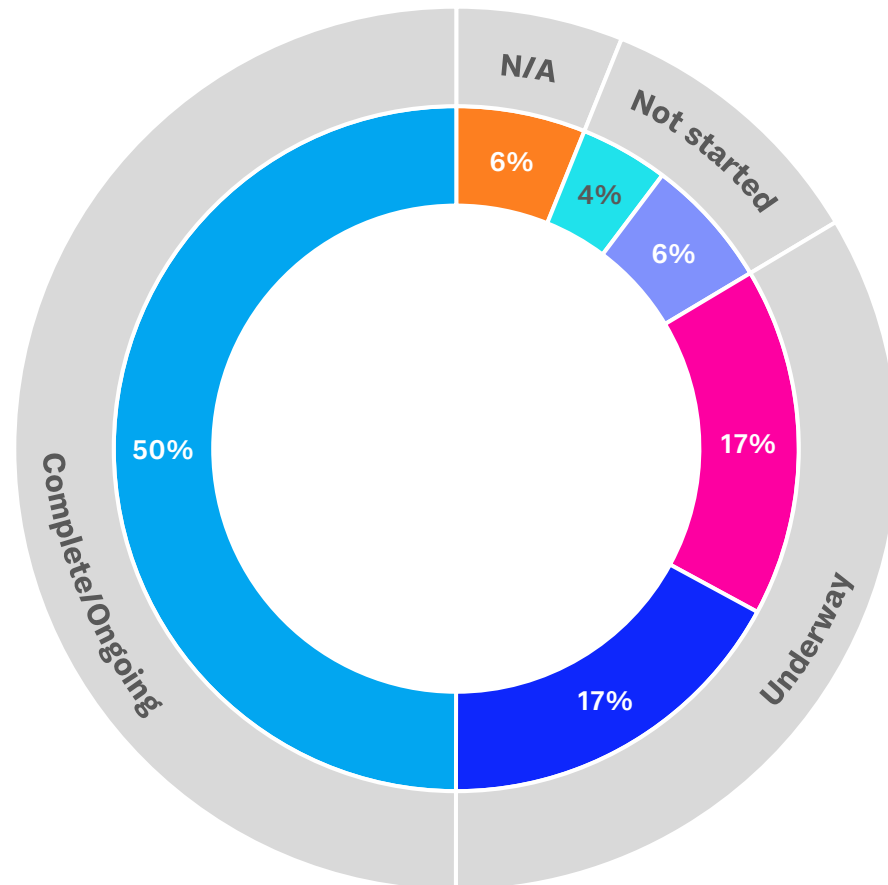
- Risk informed organisations make smarter more balanced security decisions
- Compliance alone may meet requirements but may overlook real risk exposures
- Bringing compliance and risk together delivers stronger, more sustainable security



Chapter 1

Implementation of the Standards

From plans to practice: implementation in motion



Not Applicable

Status: Not applicable

6%

There is no related information security risk that needs to be managed.

Not started

Status: Not commenced

4%

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

Planned status

6%

The organisation has a program of work in place that includes work to meet the requirement; and the program is appropriately planned and resourced.

Underway

Status: Partial (some)

17%

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

Status: Partial (most)

17%

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

Complete/Ongoing

Status: Implemented

50%

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

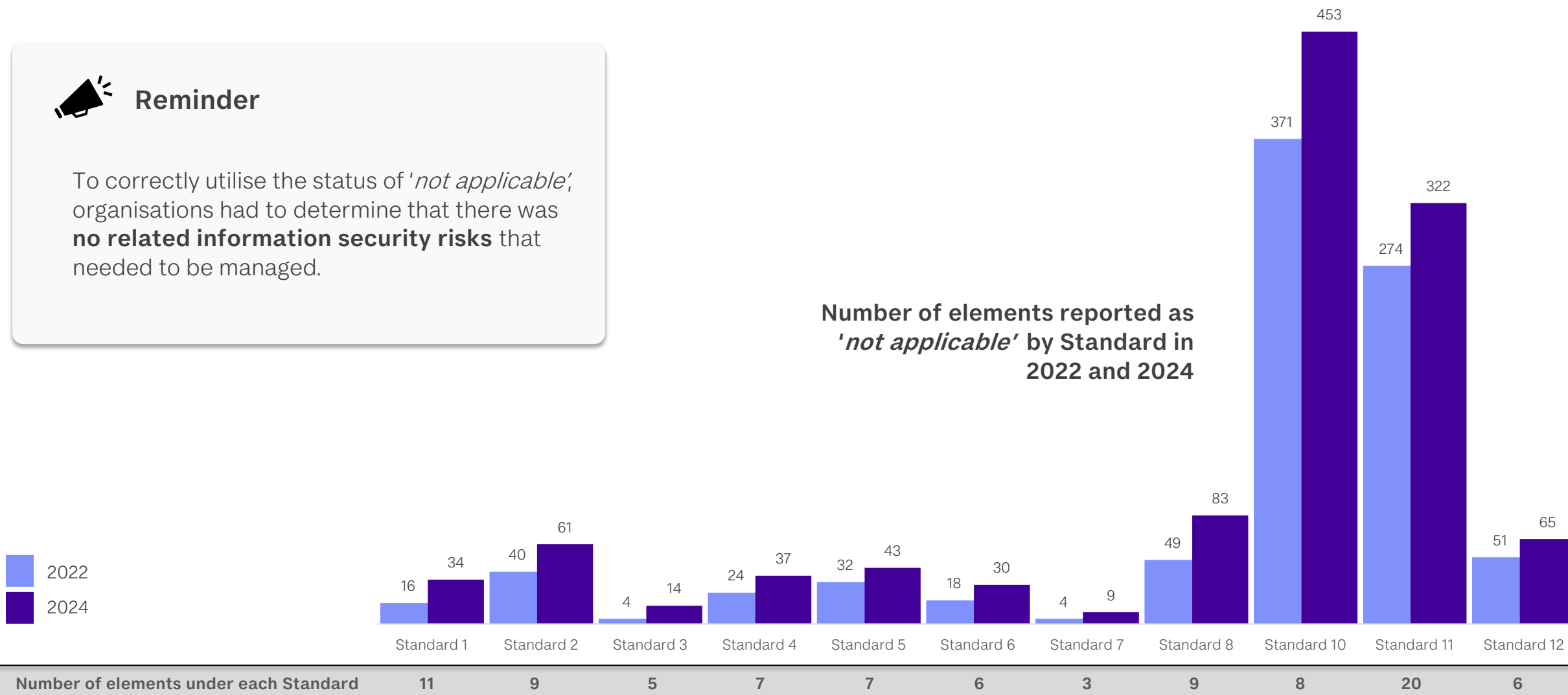
Exercising awareness of uncertainties



Reminder

To correctly utilise the status of *'not applicable'*, organisations had to determine that there was **no related information security risks** that needed to be managed.

Number of elements reported as *'not applicable'* by Standard in 2022 and 2024



Revisiting your organisation's risks

Standard 2

These elements require organisations to consistently identify and assess the value of its information. As a foundational Standard, OVIC would encourage organisations to revisit this if they selected of *'not applicable'*.

Standard 8

There was a big increase on the selection of *'not applicable'* for this Standard. **18%** of organisations that reported *'not applicable'* for these elements also provided conflicting responses in other sections of their PDSP.

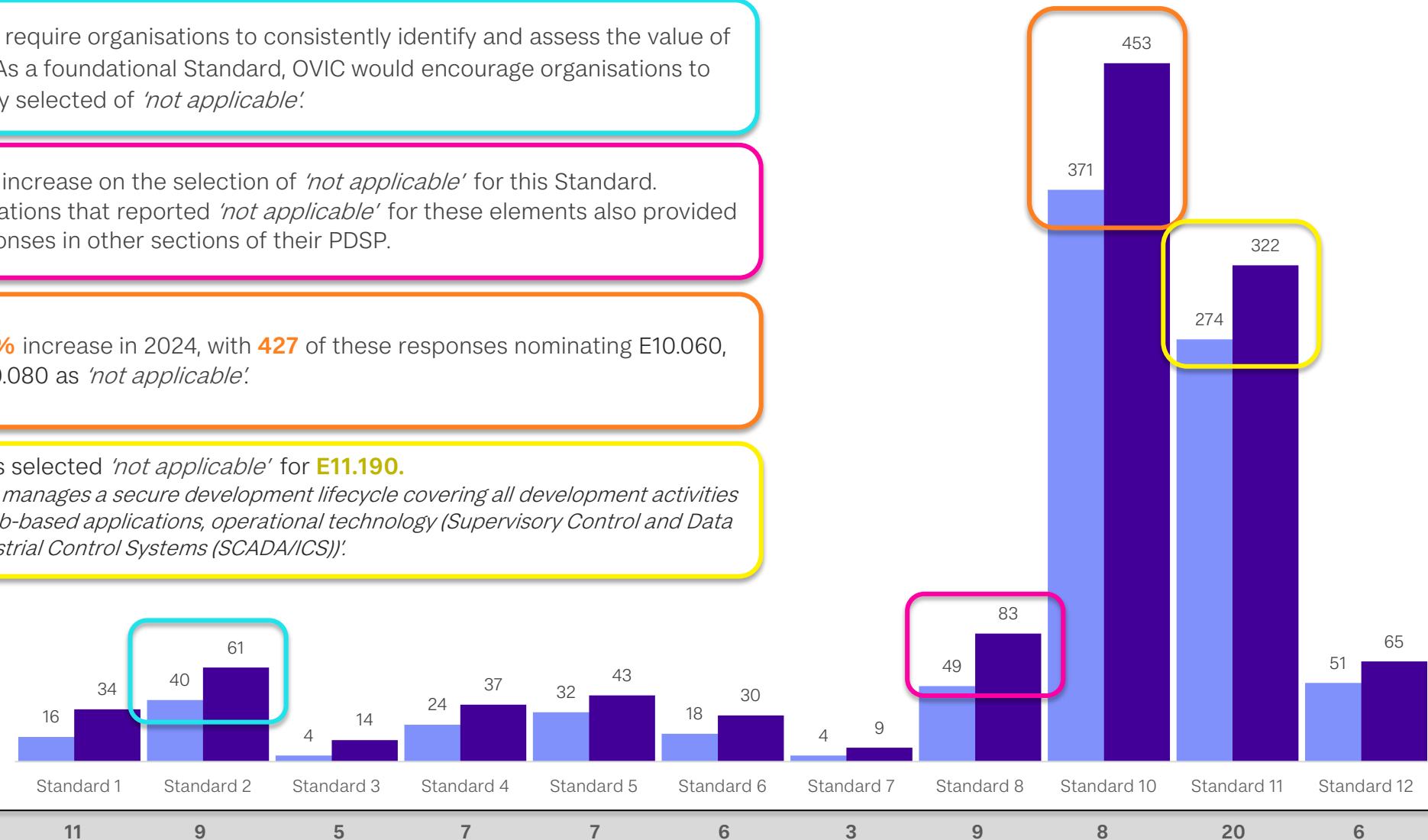
Standard 10

There was a **22%** increase in 2024, with **427** of these responses nominating E10.060, E10.070 and E10.080 as *'not applicable'*.

Standard 11

76 organisations selected *'not applicable'* for **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))'.

Number of elements reported as *'not applicable'* by Standard in 2022 and 2024



Implementation rates continued to increase

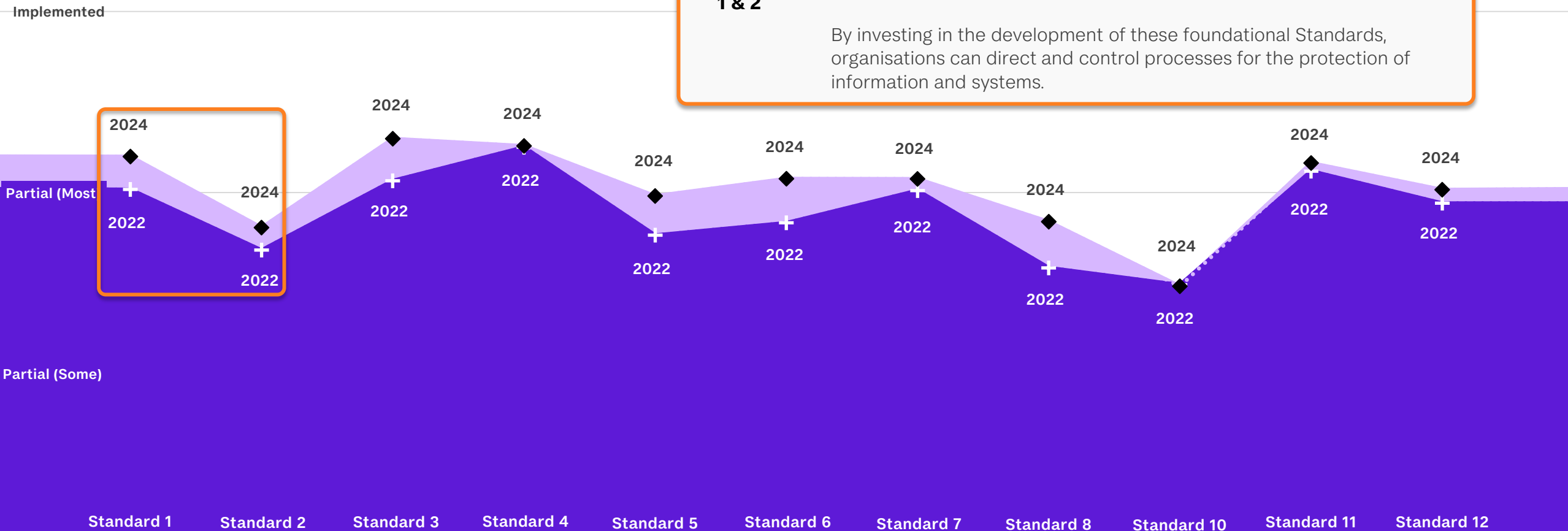
Strong foundations

Standards 1 & 2

Good news, organisations have reported they are working towards implementation of the foundational Standards!

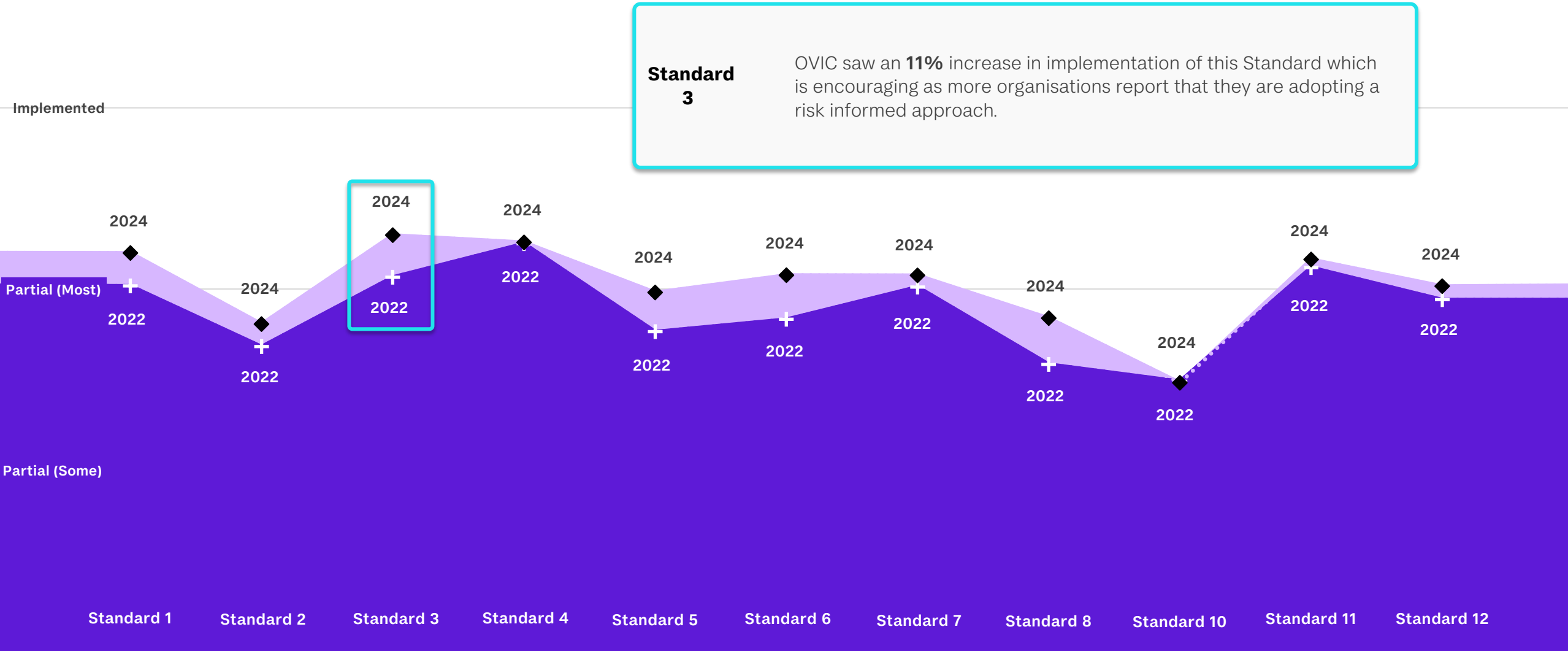
2024 reporting has shown an increase in implementation for both Standard 1 and 2.

By investing in the development of these foundational Standards, organisations can direct and control processes for the protection of information and systems.



Implementation rates continued to increase

Governance matters, building resilience through risk management



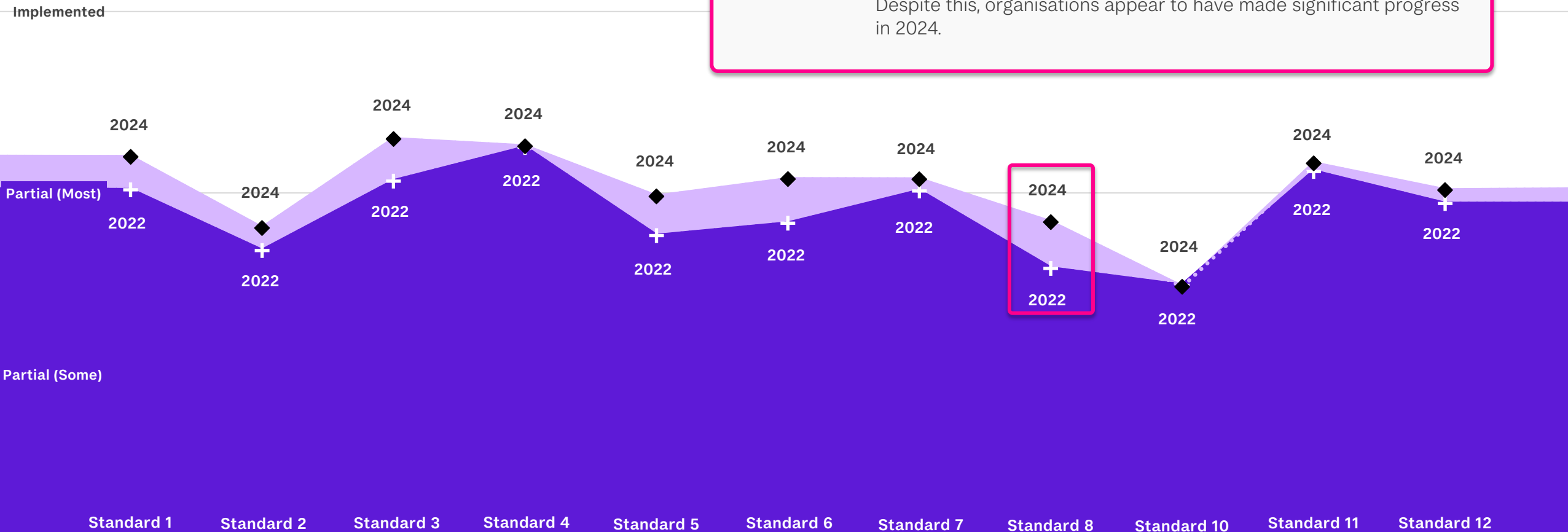
Implementation rates continued to increase

Managing the supply chain risks

Standard 8

In 2022, this Standard had one of the lowest reported implementation rates.

Despite this, organisations appear to have made significant progress in 2024.



Where is your organisation placed?

Justice, Community and Emergency Services (23)

Arts, Sport and Recreation (28)

Departments (10)

Environment and Land Management (32)

Finance, Legal, and Administrative (38)

Health and Human Services (45)

Industry and Transport (25)

Local Government (76)

Regulatory and Integrity Bodies (31)

Education (25)

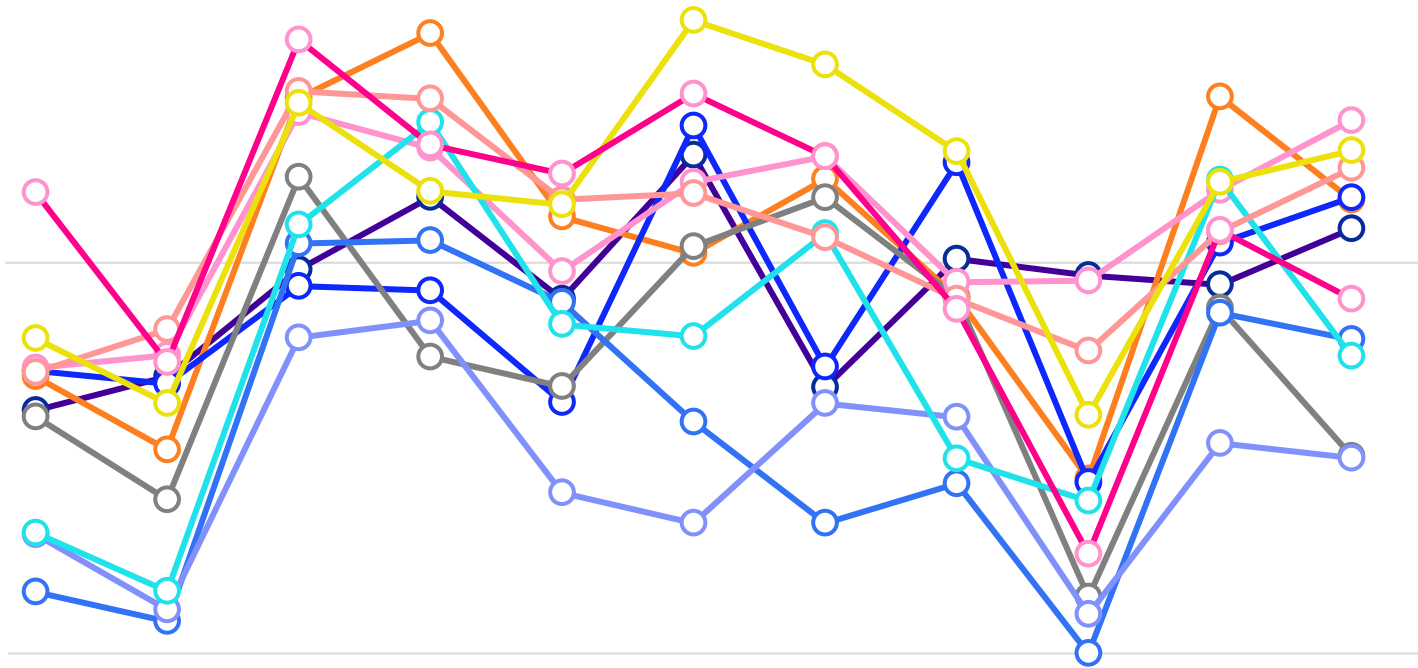
Water Corporations and Catchments (27)

Implemented

Partial (Most)

Partial (Some)

Standard 1 Standard 2 Standard 3 Standard 4 Standard 5 Standard 6 Standard 7 Standard 8 Standard 10 Standard 11 Standard 12



Chapter 2

Incident insights

Standard 6 – Reported vs. reality



Qualitative Analysis finding

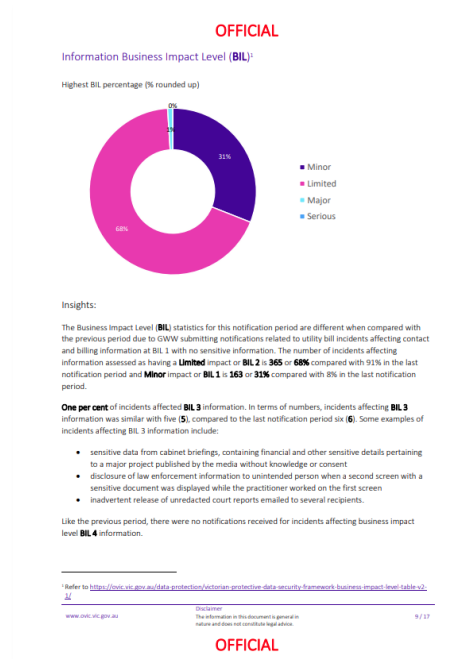
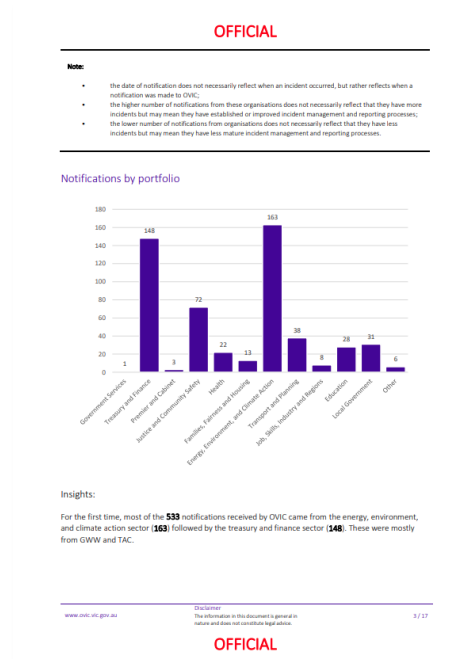
Standard 6 has one of the **highest implementation rates** of all the Standards in 2024.

69% of organisations reported that they record their information security incidents in a register.

However **over half** of these organisations also reported that they had experienced **ZERO incidents** for the **24-month period** captured by the 2024 PDSP.

Turn every incident into a learning opportunity

OVIC publishes **Incident Insights Reports** that provide an overview and analysis of incident notifications received by OVIC under the information security incident notification scheme.



Organisations are encouraged to use the insights within these reports to inform their own information security risk assessments.

Please note: the incident insight report references organisations in portfolios, not sectors

Chapter 3

Audits and investigations

Learning through audits, investigations and examinations

- Gain valuable insights on how security is working in your organisation
- Highlight strengths and opportunities for improvement
- Ensure stakeholders voices are heard and reflected in audit outcomes
- Provide an avenue for consultation and continuous improvement
- Turn findings into practicable lessons
- Testing whether the controls operating effectively

Audits

OVIC has regulatory powers to monitor and assure compliance with the Victorian Protective Data Security Framework.

Audit of Standard 10 of the Victorian Protective Data Security Standards

This audit focused on four Victorian public sector organisations' adherence to Standard 10 of the Victorian Protective Data Security Standards.

Audit of Standard 2 of the Victorian Protective Data Security Standards

This audit focused on four Victorian public sector organisations' adherence to Standard 2 of the Victorian Protective Data Security Standards.

Audit of Standard 8 of the Victorian Protective Data Security Standards

This audit focused on four Victorian public sector organisations' adherence to Standard 8 of the Victorian Protective Data Security Standards.

Investigations

OVIC has regulatory powers to undertake investigations and issue a Compliance Notice if there is a serious breach of legislation.

Investigation into the use of surveillance by the University of Melbourne

OVIC conducted this investigation following the tracking of tracking of students involved in a sit-in protest.

Report on the privacy impacts of Greater Western Water's migration to a new billing and payment system

OVIC conducted this investigation following privacy concerns relating to personal information being disclosed to unauthorised third parties by the new billing and payment system at GWW.

Investigation into the use of ChatGPT by a Child Protection worker

OVIC conducted an investigation in response to a privacy incident reported by the Department of Families, Fairness and Housing regarding a Child Protection worker who had used ChatGPT when drafting a Protection Application Report.

Examinations

OVIC has regulatory powers to undertake examinations to investigate a potential breach, or as a proactive assurance tool.

Examination into 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 Information Privacy Principle 4.1.

Examination of Victorian universities' privacy and security policies

OVIC conducted an examination into the protection of personal information in Victorian universities to ensure compliance with the Information Privacy Principles.

Examination into the use of apps and web-based learning tools in Victorian government primary schools

OVIC conducted an examination into the use of digital learning tools in Victorian government primary schools and how privacy issues are managed.

Our Regulatory Approach

Regulatory approach

OVIC's regulatory approach is independent, collaborative, targeted and proportional, transparent and consistent.

Regulatory Action Policy

Our Regulatory Action Policy explains how we use our powers when taking regulatory action.

Witness Welfare Management Policy

This policy describes how OVIC supports the welfare of witnesses and other people involved in OVIC regulatory action.



To find out more visit:
<https://ovic.vic.gov.au/regulatory-action/>

Chapter 4

Engagement

Engagement at Scale: What works best?

Scope

3,300+
organisations

Cohorts

Wide array of cohorts with varied **capabilities** and different stages of **maturity**

Enquiries

3,067
enquiries received by the team
in **2023/2024**

Our team

Coverage shaped by a small team of subject matter experts

Current engagement approach

- Host Victorian Information Security Network (VISN) events
- Publish online resources and guides
- Meet with organisations one on one where possible
- Publish newsletters
- Participating in existing channels to reach broad stakeholder groups efficiently (e.g., ISAG, IMG, Sector SIGs, Local government, Home Affairs, Standards committees)

Your turn: What could work best for you?

- Where do you see the biggest opportunities?
- What approaches work best?
- How can we balance scale and depth with limited resources?
- What support or tools would make engagement easier?
- Which engagement methods would you like us to try?

Email us at security@ovic.vic.gov.au for an ideas or opportunities for us to consider.

Chapter 5

Futures

Moving forward together

Seek **legislative reform** of the PDP Act

Review the **Victorian Protective Data Security Framework** and **Standards**

Develop enhanced **reporting models** and **methods**

Provide **intelligence formed insights** to the VPS

Engage with government organisations to **clarify roles and responsibilities**

Work together to **review existing strategies** for certain cohorts

OVIC
Office of the Victorian
Information Commissioner

For organisations and agencies

Victorian public sector stakeholders

Reporting 2025

In 2025, Victorian public sector (**VPS**) organisations are normally required to submit an Attestation signed by the public sector body Head.

Following significant deliberation and review by members of OVIC, VPS organisations now have deferred 2025 Attestation reporting obligations under the Victorian Protective Data Security Framework (**'the Framework'**) and Standards (**'VPDSS' or 'the Standards'**). All other reporting obligations to OVIC remain unchanged.

This deferral supports OVIC's intention to review and uplift the VPDSS product suite, following feedback from stakeholders and responses from the 2024 Protective Data Security Plans (**PDSPs**). This project will focus on maintaining currency of the Standards and offering clarity to users and delivering efficiencies in this space.

OVIC will undertake formal consultation on the revised VPDSS, with more information on these engagements to come.

Authorised Version No. 027 Privacy and Data Protection Act 2014 No. 60 of 2014

Authorised Version incorporating amendments as at
26 April 2021

TABLE OF PROVISIONS

Section	Page
Part 1—Preliminary	1
1 Purposes	1
2 Commencement	1
3 Definitions	2
4 Interpretation	12
5 Objects	13
6 Relationship of this Act to other laws	14
7 Rights and liabilities	14
8 Act binds the Crown	14

Part 1A—Functions, powers of Information Commissioner and appointment of Privacy and Data Protection Deputy Commissioner

Division 1—Performance of functions	15
8A Functions of Information Commissioner	15
8B Functions of Privacy and Data Protection Deputy Commissioner	16
8C Information privacy functions	17
8D Protective data security and law enforcement data security functions	19
8E Performance of concurrent functions	20
8F Int	
8G Gt	
8H An	

Privacy and Data Protection Act 2014
No. 60 of 2014
Part 4—Protective data security

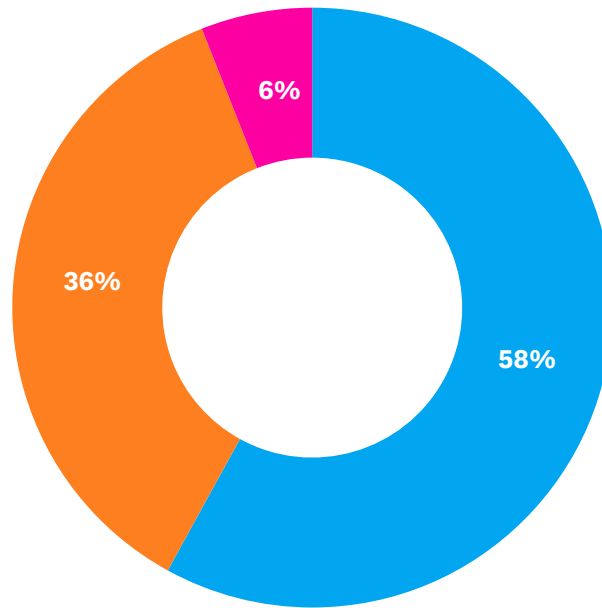
Part 4—Protective data security

Division 1—Application of Part

84 Application of Part

- (1) Subject to subsection (2), this Part applies to—
- (a) a public sector agency; and
 - (b) a body that is a special body, within the meaning of section 6 of the **Public Administration Act 2004**; and
 - (c) a body declared under subsection (3) to be a body to which this Part applies.

Strengthening security through collaboration (VPDSS 3.0)



Organisations' overall understanding of the Standards

- Consistent, proficient or practical understanding
- Basic understanding
- Not understood

Attestation Deferral

Organisations were not required to attest in 2025 which allowed our office to commence a review of the VPDSS.

Initial Review

A draft VPDSS 3.0 was developed, that represented an ambitious evolution in the Standards' development.

Given the remaining timeframe, we felt it was best to pause and take stock before broader stakeholder engagement, ensuring future Standards reflect your input and are practical, well supported and sustainable.

Decision

Retain the current Standards and continue to report against these in the 2026 reporting cycle. This will ensure continuity and stability of organisations' existing information security programs.

Next Steps

Develop an approach for broader stakeholder engagement.

Rest assured, we will provide ample time to adopt any updated Standards.

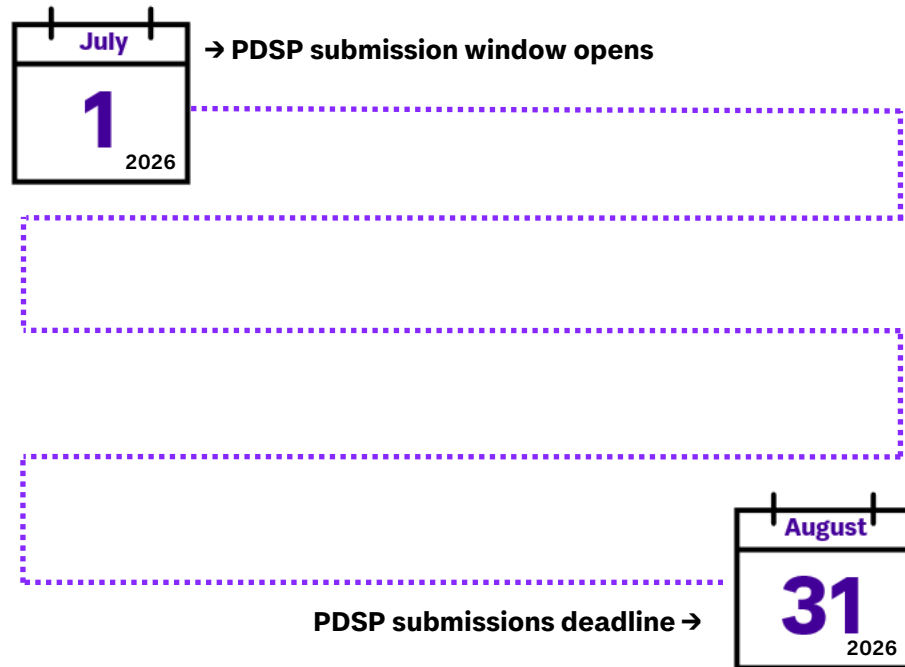
2026 reporting

Protective Data Security Plans

2026 Protective Data Security Plans

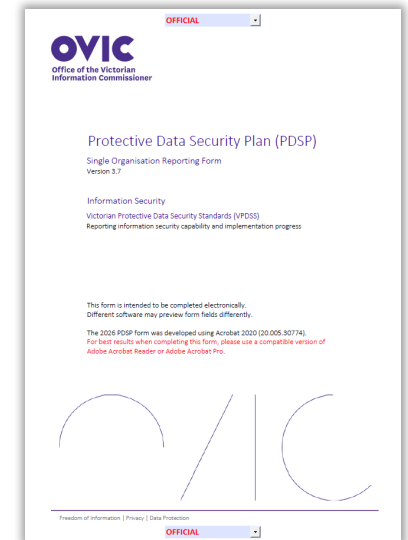
Reminder that 2026 reporting requires all agencies and bodies captured by Part 4 of the *PDP Act* to submit a PDSP.

More information and reporting templates will be made available in early 2026.



6 tips for PDSP preparedness

1. Review your 2024 PDSP to see how the organisation is tracking towards the proposed implementation of Standards and associated elements
2. Undertake an updated Security Risk Profile Assessment (including consideration of any information security incidents that have occurred)
3. Ensure you have executive buy-in
4. Leverage off a cross-functional workgroup and arrange regular check-ins
5. Notify OVIC of any changes to key contacts within the organisation (Information Security Lead and agency Head)
6. If applicable, start considering your multi-organisation PDSP list



The screenshot shows the cover page of the "Protective Data Security Plan (PDSP) Single Organisation Reporting Form, Version 3.7". It includes the OVIC logo, the title "Protective Data Security Plan (PDSP)", and the subtitle "Single Organisation Reporting Form, Version 3.7". Below this, it states "Information Security Victorian Protective Data Security Standards (VPDSS) Reporting information security capability and implementation progress". A note mentions that the form is intended to be completed electronically and that the 2025 PDSP form was developed using Acrobat 2020 (20.005.30714). At the bottom, there is a large stylized "OVIC" logo and a footer with "Freedom of Information | Privacy | Data Protection" and "OFFICIAL".

Questions



Have your say on this VISN event -
<https://forms.office.com/r/MRFVMnG5Bc>

Find out more

Visit the OVIC website to view the **Victorian Public Sector Insights Information Security Monitoring & Assurance 2025 Report** or to download any of our guidance material

ovic.vic.gov.au

Contact the Information Security Unit

security@ovic.vic.gov.au



Have your say on this VISN event -
<https://forms.office.com/r/MRFVMnG5Bc>


Office of the Victorian
Information Commissioner

For organisations and agencies

Home / Information security / Information Security Resources / Monitoring and Assurance Insights

Download



Victorian-Public-Sector-Insights---
Information-Security-Monitoring-and-
Assurance-Report-2025.pdf
Size 3.52 MB

Download

Contents

- **OVIC's approach**
- 2025 – Victorian Public Sector Insights – Information Security Monitoring and Assurance report
- 2023 – Organisation-specific PDSP Insight Reports
- + 2021 – Organisation-specific PDSP Insight Reports

Monitoring and Assurance Insights

These reports seek to highlight the information security achievements of organisations, whilst reflecting on areas of organisations' information security programs that require further investment and focus. The reports provide organisations with insights into OVIC's analysis of their information security programs informed by various intelligence sources.

OVIC encourages organisations to consider the insights offered and where needed, review their information security risks and recalibrate future work programs based on the material offered.



www.ovic.vic.gov.au