# Top Questions for the Audit and Risk Committee

## A sense check guide to how the agency's VPDSF program is progressing

This document aims to provide Audit and Risk Committee (ARC) members with suggested questions to identify how the Victorian Protective Data Security Framework (VPDSF) uplift program is progressing and how commitments documented in the Protective Data Security Plan (PDSP) will be achieved.

## Top Questions

### 1. "Have we developed a detailed project charter/work plan endorsed by the executive?"

Identify if the public sector organisation has developed and resourced an appropriate project/work plan to enable the systematic uplift of controls as per their PDSP. Determine if an appropriate level of project governance exists to ensure the project is meeting its objectives within budget and timelines.

### 2. "Is our progression against the work plan improving our information security maturity?"

Identify at a standards and controls level, where the public sector organisation has seen an uplift in maturity and by how much. How would this be demonstrated?

### 3. "If OVIC were to assess us today, how would we demonstrate our adherence to the VPDSF?"

Determine if the appropriate steps have been taken to understand the current state and develop an uplift plan (which should have been captured in the public sector organisation's detailed PDSP). These steps would have included:

- developing an Information Asset Register and populating with relevant information assets and their associated value
- identifying and assessing risks relevant to these assets into the Security Risk Profile Assessment
- developing a risk-based uplift in the Protective Data Security Plan, and
- undertaking the self-assessment against the Victorian Protective Data Security Standards

### 4. "Do we have a detailed internal control library and how aligned is it to the Victorian Protective Data Security Standards (VPDSS)?"

Determine if the organisation has identified and documented controls which demonstrate alignment to the VPDSS.

### 5. “Now that we have our information assets in a register, how much validation of these assets have we performed?”

Determine if a process exists to keep the Information Asset Register (IAR) up to date and any associated forward work plan to maintain the currency of the register. Determine if any further work has taken place to ensure the IAR identifies all information that is stored, used and transferred within and outside of the organisation. Determine how much technical validation (in addition to interviews / workshops) of the IAR has occurred.

### 6. “What level of risk reduction have we observed so far, and across which risk areas?”

Identify the progress of controls uplift in alignment to priority risk areas. Identify which controls were implemented as a priority, which risks they relate to and how much reduction has been achieved so far. Determine if the agency is on target to reduce risk levels in alignment with risk appetite.

### 7. “How are we assessing ongoing effectiveness of controls?”

Identify how the effectiveness of controls is currently being assessed and reported, and whether there is adequate oversight from the various lines of defence (e.g. management, risk and internal audit). Determine whether there is a systematic approach for controls testing to ensure key controls are assessed more frequently and/or to a greater level of rigour. This includes coverage of relevant third parties and entities that you are reporting on behalf of.

## Contact Us

**t:** 1300 00 6842
**e:** enquiries@ovic.vic.gov.au
**w:** ovic.vic.gov.au

## Disclaimer