Review of information governance in the Department of Health and Human Services (DHHS)

Review conducted and report prepared by PricewaterhouseCoopers

January 2017

Commissioner for Privacy and Data Protection

VICTORIA State Government

This page is intentionally left blank.

Review of information governance in the Department of Health and Human Services (DHHS)

Review conducted and report prepared by PricewaterhouseCoopers

January 2017

Published by the Commissioner for Privacy and Data Protection
PO Box 24014
Melbourne Victoria 3001

January 2017

Also published on:
http://www.cpdp.vic.gov.au

ISBN 978-0-9946370-5-5

DOCUMENT DETAILS	
Security Classification	UNCLASSIFIED
Dissemination Limiting Marker	Nil
Dissemination Instructions	For public release
Issue Date	January 2017
Document Status	Final
Authority	Office of the Commissioner for Privacy and Data Protection

This page is intentionally left blank.

Contents

This page is intentionally left blank.

Commissioner's Foreword

This information governance review of the Department of Health and Human Services (DHHS) was conceived as a response to an increase in privacy and data security complaints identified by our monitoring systems and a series of confronting media reports during 2016 that highlighted privacy and security deficits, in particular in foster care arrangements within DHHS.

DHHS has legal, policy and service delivery responsibilities that cover the delivery of some of Victoria's most complex and important services, often to its most vulnerable and disadvantaged citizens. These responsibilities include child protection, housing, disability services, family services and aged care. In order to ensure that these services are provided effectively and efficiently, DHHS relies on information systems. Often, these systems process highly sensitive personal information. The challenge for DHHS is to ensure that this data is shared responsibly to support its service delivery functions while at the same time protecting it from unauthorised disclosure. DHHS's information environment is the most complex of any of Victoria's government departments.

In order to manage this information complexity, DHHS needs systems, processes and procedures in place to oversee and manage it, to identify information risks and opportunities and to ensure that both service delivery and regulatory responsibilities are met, in particular privacy and security obligations under the *Privacy and Data Protection Act 2014*. Good information governance underpins the advancement of all of these objectives.

This review takes a diagnostic approach to DHHS's information governance. It highlights flaws in its information governance and makes recommendations about how these should be addressed. The recommendations constitute a blueprint for dealing with the underlying causes of the recent privacy and data security issues that have affected DHHS and its clients. None of the recommendations constitute a quick fix. Instead, they are designed to solve the underlying information governance problems within DHHS.

The review has been undertaken in an environment where there has been significant cooperation between the review team and DHHS staff. This has meant that, as the review has progressed, DHHS has taken the first steps towards improving its information governance.

I wish to extend my thanks to Mr Chris Braithwaite, who led the review project. I also thank the Secretary of DHHS, Ms Kym Peake and her staff for their cooperation.

1 Executive Summary

1.1 Introduction

The Department of Health and Human Services ('DHHS', 'the Department') is a Victorian government department, responsible for public health, mental health, alcohol and drug treatment, ambulance services, aged care, child protection, out-of-home care, youth affairs, public housing, disability, and sport policy, amongst other areas. In January 2015, the Victorian government merged the former Department of Health, Department of Human Services, and the Sports and Recreation function from the Department of Planning and Community Development (DPCD) and established DHHS. The Department has been established to develop and deliver policies, programs and services that support and enhance individual well-being, active living, socio-economic participation and safeguard the vulnerable.

DHHS works in close partnership with a number of Community Service Organisations (CSOs), as well as other health services organisations to deliver quality community, child, housing and various other services to the citizens of Victoria (i.e. 'clients'). These CSOs (also known as 'funded agencies') perform an extension of DHHS' various services and assist in the management of individual needs.

1.2 Background

Recently, DHHS has reported a rising number of breaches of personal information (PI) to the Victorian Commissioner for Privacy and Data Protection (CPDP), some of which originated from PI data exposure at the CSO level. CSOs must establish and maintain their own internal information governance, which includes the establishment of an accountability structure, frameworks and/or policies and procedures addressing information management legislative requirements and obligations (covering domains such as privacy, protective data security and data quality). DHHS is, however, accountable for setting out expectations and requirements when regulating and contracting with these CSOs. As such, it would be expected that these CSOs align with the information governance (as it relates to privacy, protective data security and quality) established by DHHS to guide their internal information governance practices.

Accordingly, CPDP elected to undertake a review of DHHS' overall information governance (as it relates to privacy, protective data security and data quality) processes that span across the Department. PwC undertook the review, under the appointment of CPDP in exercise of the CPDP's powers under s103(1)(d) of the *Privacy and Data Protection Act 2014* (PDPA 2014). Whilst PwC's review examined information governance (as it relates to privacy, protective data security and data quality) from a holistic department-wide view, focus was placed on two of DHHS' areas of operation that recently reported privacy breaches to the CPDP, home based care and family violence.

1.3 Rising information governance challenges

The volume and nature of information collected by organisations, including public sector organisations is growing exponentially. In addition, the shift to digital service delivery is necessitating the need for increased governance to oversee end-to-end management of information, while enabling information sharing to enhance existing internal processes. Research from leading organisations has foreshadowed the growing challenge information creates for organisations in the coming years:

- The amount of data in the digital universe is doubling every two years[1]

[1] International Data Corporation, EMC Digital Universe with Research and Analysis by IDC, The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things, April 2014

- Enterprise data volume will grow 50 times each year between 2014 and 2020[2]
- More than 90% of the data in the world today has been created in the last two years alone[3]
- The Internet of Things (IoT) will include 26 billion units by 2020[4]
- The percentage of mobile 'things' in the IoT will be over 75% by 2020, which will see public sector organisations preparing for the increased privacy requirements that the IoT will bring. This year, 40% of public sector respondents to PwC's 2017 Global State of Information Security Survey (GSISS) stated they are investing in IoT security, with 52% of public sector organisations indicating they have an IoT security strategy in place or are currently implementing one.[5]
- As consumers and third party partners become more concerned about how their sensitive data is gathered and shared, data privacy has become an increasingly critical requirement for the public sector. PwC's 2017 GSISS respondents from public sector say they plan to address several privacy initiatives over the next 12 months, with an emphasis on privacy training and awareness.[6].

1.4 Release of the Victorian Protective Data Security Standards

With the CPDP's recent issue of the finalised version of the Victorian Protective Data Security Standards (VPDSS) in July 2016, there is greater legislative emphasis on DHHS to implement the necessary information governance (as it relates to privacy, protective data security and data quality) programs to ensure the Department's adherence to section 88 of the PDPA 2014. Of the 18 standards included within the VPDSS, 12 relate to overall information security governance. As such, the scope of the PwC review of DHHS' information governance program was guided by the requirements set forth in the first 12 standards of the VPDSS and Information Privacy Principles (IPPs) established in the PDPA 2014. Refer to Appendix C: VPDSF Principles and VPDSS for further information on these principles and standards.

Whilst the VPDSS were formally issued by CPDP in July 2016, it should be noted that prior to that, a Whole of Victorian Government (WoVG) Information Security Management Framework (ISMF) was established in 2009, aligned to the Australian Government Protective Security Policy Framework (PSPF). The WoVG ISMF applied to 20 Victorian agencies, which included the Department of Health and Department of Human Services. As a result, though the VPDSS were only recently formally issued in July 2016, there is an expectation that a number of the VPDSS requirements should have already been implemented by DHHS as part of their compliance with the WoVG ISMF and annual reporting requirement to the Victorian Audit General's Office (VAGO).

As the 'owner' and often 'custodian' of data, DHHS will experience increasing pressure to embed and mature their information governance framework to support the way it administers and uses the PI it collects about Victorian citizens. As part of this framework, the Department will be expected to have a coherent set of standards, policies, guidelines and procedures that are implemented either manually or, where possible, automated through technology, to govern the overall information management of PI. These requirements also extend out to the extensive list of CSOs and commercial third party service providers, involved in the various elements of the Department's information management lifecycle, which are deemed as Contracted Service Providers (CSPs) under the PDPA 2014.

The results of our review have highlighted areas where DHHS is not yet fully aligned with the 12 standards set forth in the VPDSS (refer to section 1.6). CPDP have recognised that it is not the expectation that Victorian public sector organisations will be fully compliant with the VPDSS requirements by July 2018. Rather, the findings and recommendations outlined in this report, are intended to assist DHHS management in the timely completion of the Security Risk Profile Assessment (SRPA) and Protective Data Security Plan (PDSP), which are required to be submitted to CPDP by

[2] International Data Corporation, EMC Digital Universe with Research and Analysis by IDC, The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things, April 2014

[3] SINTEF, www.sciencedaily.com, Big Data, for better or worse: 90% of world's data generated over last two years, May 2013

[4] Gartner, www.gartner.com, Forecast: The Internet of Things Worldwide 2013, November 2013

[5] PwC, *The Global State of Information Security Survey 2017*

[6] PwC, *The Global State of Information Security Survey 2017*

July 2018 (as part of meeting their obligations as stated in Part Four of the PDPA 2014).

1.5 Scope and Approach

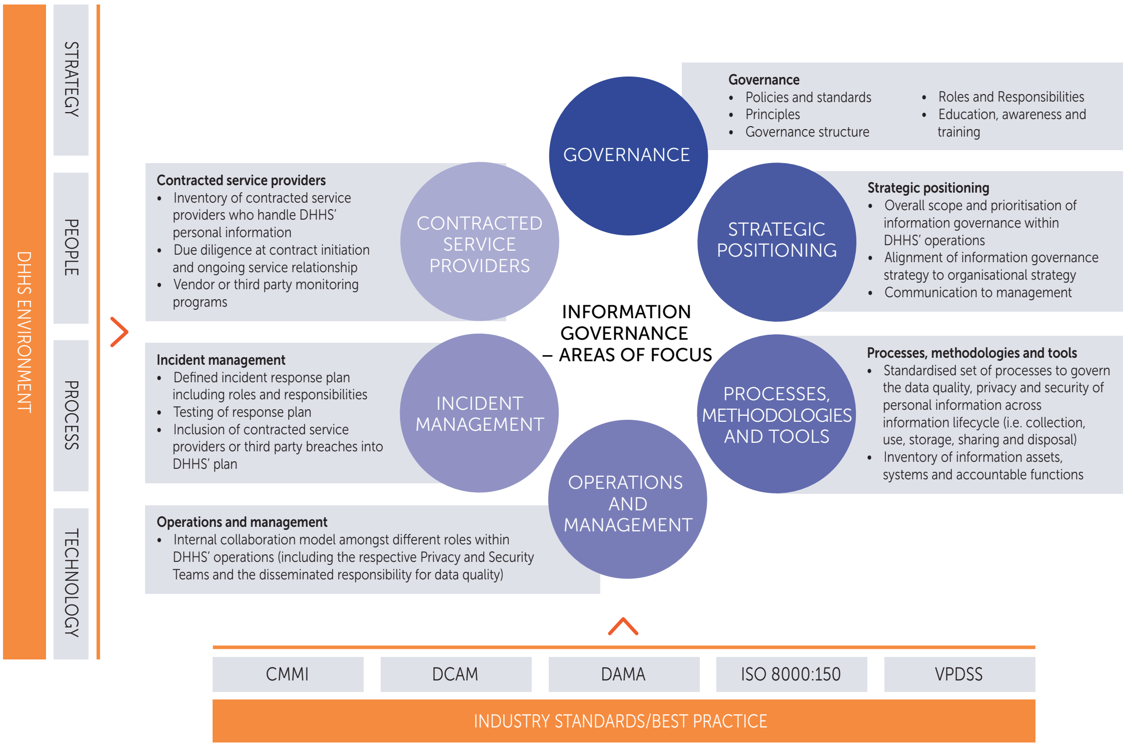
Whilst this review focused on information governance overall within DHHS, the scope of the review was not to determine the Department's compliance with the VPDSS or other relevant acts applicable to the Department (such as the Health Records Act; Public Records Act; Freedom of Information Act; Children, Youth and Families Act; etc.), but rather leveraged these legislative instruments as inputs to assess current information governance procedures against industry best practice.

In performing the information governance review (as it relates to privacy, protective data security and data quality) over DHHS and recommending appropriate pragmatic actions to uplift key capabilities, we have undertaken the following procedures:

- Reviewed existing documented strategies, frameworks, policies, procedures, and other relevant documentation that support DHHS' information governance programs
- Obtained and reviewed high level evidence to validate current capabilities, processes and controls that govern the quality, privacy and security of DHHS data across the Department's information lifecycle (i.e. collection, use, storage, sharing, and disposal)
- Conducted interviews and workshops with key stakeholders across the Department to obtain additional information to supplement our review of documentation and to understand how these documents are operationalised within the Department and extended to CSOs and CSPs
- Met with relevant CPDP and DHHS stakeholders prior to finalisation of findings and recommendations that were prioritised based on risk exposure.

We also recognise that there were a number of reviews of department activity related to the information management domains of governance, privacy, protective data security and data quality, which have also been included in the scope of our review. Appendix B (Audits and Reviews Considered) provides an outline of these reviews and related final reports we considered part of our scope. Several of the findings noted in these reviews were consistent and have informed this review.

The below diagram outlines the six key scope areas of our DHHS' information governance review (as it relates to privacy, protective data security and data quality), taking into account the environment and industry best practices under which DHHS operates:


DHHS ENVIRONMENT
STRATEGY
PEOPLE
PROCESS
TECHNOLOGY
INFORMATION GOVERNANCE – AREAS OF FOCUS
GOVERNANCE
CONTRACTED SERVICE PROVIDERS
STRATEGIC POSITIONING
INCIDENT MANAGEMENT
PROCESSES, METHODOLOGIES AND TOOLS
OPERATIONS AND MANAGEMENT
CMMI
DCAM
DAMA
ISO 8000:150
VPDSS
INDUSTRY STANDARDS/BEST PRACTICE

Governance
- Policies and standards
- Principles
- Governance structure
- Roles and Responsibilities
- Education, awareness and training

Contracted service providers
- Inventory of contracted service providers who handle DHHS' personal information
- Due diligence at contract initiation and ongoing service relationship
- Vendor or third party monitoring programs

Strategic positioning
- Overall scope and prioritisation of information governance within DHHS' operations
- Alignment of information governance strategy to organisational strategy
- Communication to management

Incident management
- Defined incident response plan including roles and responsibilities
- Testing of response plan
- Inclusion of contracted service providers or third party breaches into DHHS' plan

Processes, methodologies and tools
- Standardised set of processes to govern the data quality, privacy and security of personal information across information lifecycle (i.e. collection, use, storage, sharing and disposal)
- Inventory of information assets, systems and accountable functions

Operations and management
- Internal collaboration model amongst different roles within DHHS' operations (including the respective Privacy and Security Teams and the disseminated responsibility for data quality)

1.5.1 Summary of findings

Based on the procedures performed, stakeholders consulted and documents reviewed, we have identified a number of information governance risks in relation to DHHS' existing processes and procedures. A summary of findings identified has been provided below, with a detailed outline of findings provided in Section 3 of this report. While the purpose of this review was not to validate compliance against the VPDSF and VPDSS, we have provided linkage to the relevant VPDSF Principles and VPDSS requirements related to each finding to provide DHHS additional guidance on how the associated remediation efforts would work towards compiling and submitting their SRPA and PDSP. Refer to Appendix C: VPDSF Principles and VPDSS for further information on these principles and standards.

REF	SCOPE AREA	FINDING	PRIORITY RATING	ROOT CAUSE	VPDSF PRINCIPLE	VPDSS
1	Contracted Service Providers	Information management due-diligence and compliance procedures for contracted service providers (CSPs) should be enhanced	High	Procedure People	2, 6	9, 10, 12, 13, 14, 15

REF	SCOPE AREA	FINDING	PRIORITY RATING	ROOT CAUSE	VPDSF PRINCIPLE	VPDSS
2	Processes, Methodologies and Tools	A detailed information asset register has been established, and should be fully populated to document the Department's assets and the links to the system register	Medium	Procedure People	3	13, 14
3	Incident Management	Incident management procedures for regulator notification and data quality management should be enhanced	Medium	Procedure People	6	5, 7
4	Operations and Management	There should be a centralised view and monitoring of issues, recommendations and a status of actions taken to address findings from various external and internal reviews and audits around information management	Medium	Procedure People	1, 4	1, 2, 14
5	Governance Strategic Positioning	Scenario-based information management training should be developed and administered to relevant branches or local teams, based on their functional responsibilities	Medium	Procedure People	4	5, 6

REF	SCOPE AREA	FINDING	PRIORITY RATING	ROOT CAUSE	VPDSF PRINCIPLE	VPDSS
6	Processes, Methodologies and Tools	The overall management and maintenance of relevant information governance documentation and standard requirements should be strengthened	Medium	Procedure People	2, 5	1, 14

Risk rating categories

High	A significant weakness which could compromise the internal control environment and/or ability to meet legislative requirements and so requires priority management action.
Moderate	A control weakness which can undermine the system of internal control and/or ability to meet legislative requirements and should therefore be addressed by management in the short term.
Low	A weakness which does not seriously detract from the system of internal control and/or ability to meet legislative requirements but which should nevertheless be addressed by management.

Root cause categories

Procedure	Finding either requires a new procedure or a review of how the procedure applied.
People	Finding is specific to a person, human error, staff allocation or training requirement.
System	Technology is the main cause of the finding (e.g. system functionality).

2 General Observations

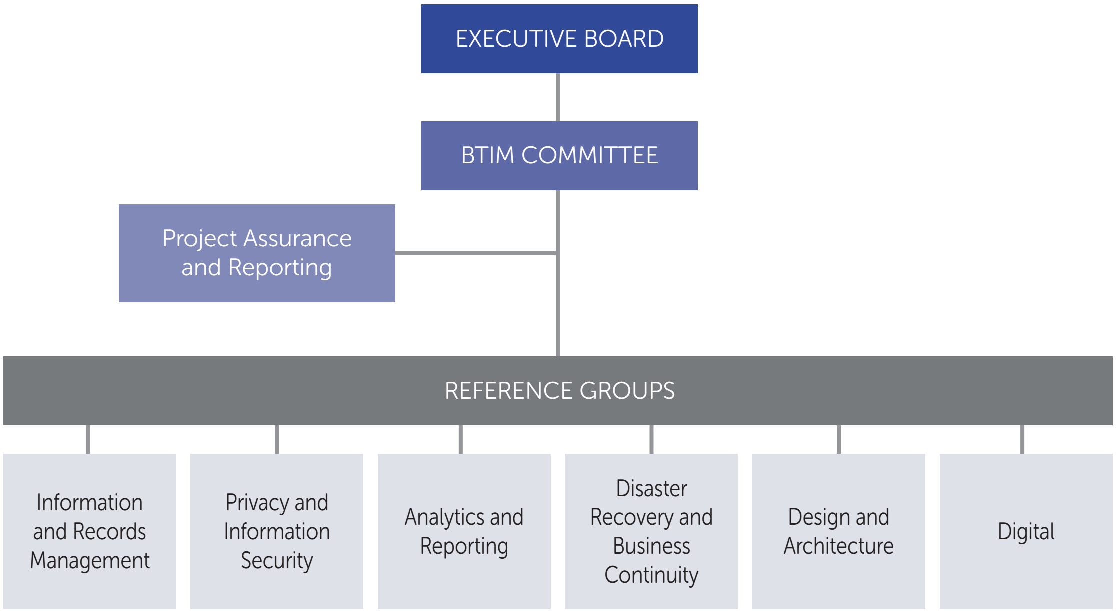
Governance and Strategic Positioning

DHHS has assigned organisational ownership and accountability for information management strategy and requirements to the Business Technology and Information Management (BTIM) branch of the department. The BTIM Committee represents the department's implementation of an Information Management Governance Committee, which departments are required to establish and maintain under the (WoVG) Agency Information Management Governance Standard (IM STD 02)[7].

The BTIM Committee is an executive sub-committee of the DHHS Executive Board, chaired by the Deputy Secretary, Corporate Services, made up of individuals from across various teams within DHHS. It governs the Department's IT and information management activities and reports up to the Board. BTIM oversees and directs the Department's coordinated, overarching BT and IM strategies and oversees seven (7) reference groups made up of senior level management from across the Department which, depending on their focus, will have differing input into the progression of information management maturity across the department.

Note: Project Assurance and Reporting acts a reference group providing advice to the BTIM Sub-committee on whether tools and methodologies available in the Department for the management of information are best practice and fit for purpose for the delivery of projects. A number of project steering committees and change control groups report to this reference group.

The governance structure for information governance, including relevant reference groups, is displayed below:


EXECUTIVE BOARD
BTIM COMMITTEE
Project Assurance and Reporting
REFERENCE GROUPS
Information and Records Management
Privacy and Information Security
Analytics and Reporting
Disaster Recovery and Business Continuity
Design and Architecture
Digital

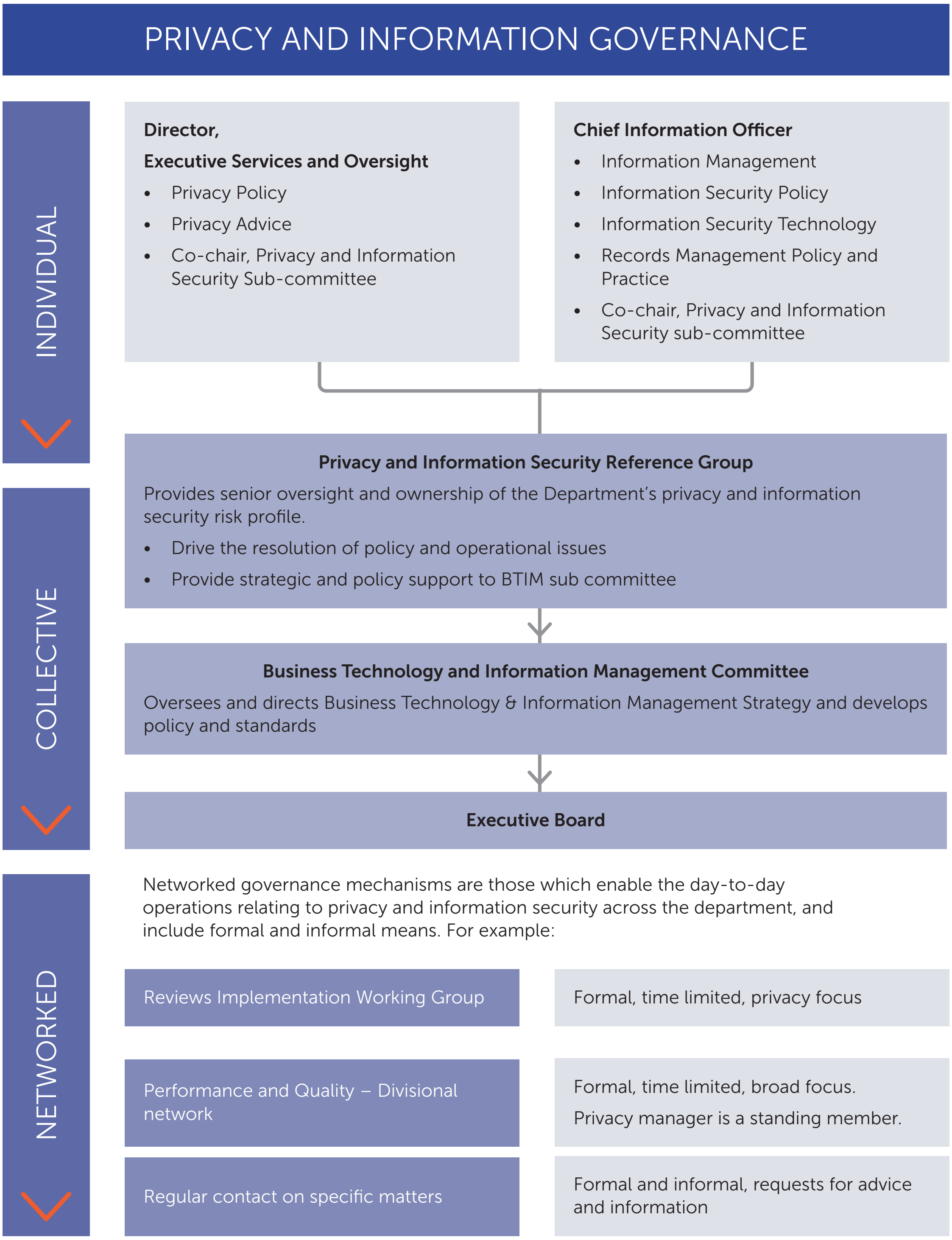
The department has implemented a privacy and information security governance framework that is multi layered to enable an appropriate distribution of strategic and operational responsibilities and comprises individual, collective and networked governance arrangements. In November 2016,

[7] https://www.enterprisesolutions.vic.gov.au/wp-content/uploads/2016/02/Agency-Information-Management-Governance-IM-STD-2.1.pdf

the BTIM Committee approved the repurposing of the Privacy and Information Security Reference Group (PISRG) to better assist the Department to manage its obligations under the *Privacy and Data Protection Act 2014* and enabling legislation such as the *Health Records Act 2001* and the *Children, Youth and Families Act*.

- Individual – Covers Senior executive officers with direct responsibility and accountabilities for the department's legislative obligations, regulatory compliance and policy design and implementation. This includes for Senior executive officers their responsibility and accountabilities for the information assets for which they are the documented Information Steward or Custodian.
- Collective – Collective governance is administered at three levels:
    - First tier: Privacy and Information Security Reference Group (PAISRG) – Director level body that coordinates oversight of risk, monitors performance and breaches, monitors implementation of responses to external and internal reviews
    - Second tier: Business Technology and Information Management (BTIM) committee – Director and Deputy Secretary level decision making body, develops and determines priorities, policies and standards
    - Third tier: Executive Board – Secretary and Deputy Secretary level body that provides leadership, sets the direction and vision for the department, and is responsible to the Ministers and Parliament.
- Networked – Networked governance facilitates day to day operations relating to privacy and information security and includes formal and informal mechanisms.

This multi-layered approach to privacy and information security governance is highlighted in the following:



PRIVACY AND INFORMATION GOVERNANCE

INDIVIDUAL

Director,
Executive Services and Oversight

- Privacy Policy
- Privacy Advice
- Co-chair, Privacy and Information Security Sub-committee

Chief Information Officer

- Information Management
- Information Security Policy
- Information Security Technology
- Records Management Policy and Practice
- Co-chair, Privacy and Information Security sub-committee

COLLECTIVE

Privacy and Information Security Reference Group

Provides senior oversight and ownership of the Department's privacy and information security risk profile.

- Drive the resolution of policy and operational issues
- Provide strategic and policy support to BTIM sub committee

Business Technology and Information Management Committee

Oversees and directs Business Technology & Information Management Strategy and develops policy and standards

Executive Board

NETWORKED

Networked governance mechanisms are those which enable the day-to-day operations relating to privacy and information security across the department, and include formal and informal means. For example:

Reviews Implementation Working Group	Formal, time limited, privacy focus
Performance and Quality – Divisional network	Formal, time limited, broad focus. Privacy manager is a standing member.
Regular contact on specific matters	Formal and informal, requests for advice and information

The Reference Groups have the support of the Centre for Learning and Organisation Development to develop and administer training over information governance and supporting the operational team to develop an awareness campaign for all staff, which has had specific focus on privacy and security. The awareness of requisite knowledge in privacy and security is facilitated through such activities as team talks, newsletters, inclusion in relevant practice manuals, intranet and Yammer content, and face-to-face sessions. The Department has already deployed eLearning modules for security and is in the process of developing a new eLearning module on information privacy that will supplement the other forms of training currently in practice.

As for Community Service Organisations (CSOs), which are obliged to uphold their information privacy and security obligations under the Service Agreement with DHHS, DHHS training on information management does not extend to these third parties. The CSOs are expected to have their own training and awareness programs for their staff to understand their information privacy and security obligations. This is further supported by the DHHS' periodic communication on the latest changes in the Department's policies and frameworks.

Through inquiry of relevant stakeholders and consideration of the findings outlined in the Leatherland report[8] and various Internal Audit reports, we recommend that scenario-based information management (as it relates to privacy, protective data security and data quality) training should be developed and administered to relevant branches or local teams, based on their functional responsibilities.

Refer to Finding #2 for more details on findings and recommendations for remediation.

The Department's *Information Management Strategy 2016-2020* has been recently defined and was presented for consideration and feedback to the BTIM Committee meeting in October 2016, with formal endorsement scheduled at the next meeting. Through inquiry of relevant stakeholders, it was noted that the *Information Management Strategy 2016-2020* has been aligned to the DHHS organisational strategy and Risk Management Strategy. Prior to the merger of departments, a 2014-2016 *Managing Information Strategy* was in place for the Department of Health.

Through review of the Department's Risk Management Strategy and Strategic Risk Register, it was noted that 'Breach of Privacy and Confidentiality' was highlighted as a corporate risk, beneath the strategic risk of 'Organisational Stewardship'. Numerous risk events were identified related to the 'Breach of Privacy and Confidentiality' and risk treatment plans and controls have been defined, including ownership for those controls. On a periodic basis, the effectiveness of each control and treatment plan is assessed and reported to ensure appropriate mitigation of risks.

Processes, Methodologies and Tools

DHHS has a number of initiatives to develop and enforce a standardised set of processes, methodologies and tools to govern the management of client's PI across the information lifecycle (i.e. collection, use, storage, sharing and disposal).

We identified some key processes, methodologies and tools that currently exist within DHHS to govern the overall management of information, outlined in numerous documents and training materials. These are outlined in Appendix A: (Information Governance Documentation Hierarchy).

These documents guide DHHS staff and Contracted Service Providers (CSPs), in their day-to-day management of DHHS information. Several department wide documents are in draft form or are working papers. It is understood that the delay in finalising these documents is at least due in part to the machinery of government changes that led to the creation of DHHS, consequential organisational and staff changes and forthcoming finalisation and endorsement of the Department's Information Management Strategy. Whilst we acknowledge that the documents that were provided for our review are considered to be valuable in terms of content, updating them to include any changes made as

[8] Leatherland, John, Review of Child Protection Privacy Incidents and Carer and Client Safety for Department of Health and Human Services, August 2016.

a result of this review (and other related reviews), and promulgating them as final documents with a review date will provide clarity and structure to DHHS' information governance framework. It is essential that all staff are made aware of all relevant documentation they must adhere to in their daily activities so DHHS is not relying on the existence of these documents on the intranet alone to provide this guidance to staff.

Refer to Finding #6 for more details on findings and recommendations for remediation.

One key tool that has been developed to support DHHS' information governance framework is the DHHS' Information Directory, otherwise known as 'Meta', which captures and manages:

- the Department's Information Asset Register (IAR)
- the Department's System Directory (to be remodelled into Application and Technology registers)
- national metadata standards (as captured in METeOR – the Australian Institute of Health and Welfare's online metadata solution)
- the Department's metadata standards
- the Department's metadata in data collections/information assets/indicator sets
- access to information management policies and associated artefacts including information governance, data quality, and data access and release, and
- links between all of the above mentioned.

Prior to a formal launch of the Information Directory, DHHS provided access to staff on an as-needs and on request basis in the interim, having demonstrated the tool to over 450 staff. At the time of the review the Department was undertaking a change management pilot to reveal any issues and determine the best approach to training and full population of the IAR. Population of the IAR has leveraged content from legacy registers from the former departments and will identify and assign ownership responsibilities (i.e. Roles that have been defined by DHHS relating to information governance include Information Owner, Information Steward, Information Custodian) to all DHHS information assets, in accordance with the DHHS Information Asset Governance Policy, as well as capture the links between the information assets and the system register, and which organisation types are contributing to the provision of different information assets. The IAR itself is an information asset recorded within the IAR in 'Meta' with appropriate ownership roles identified. Additionally, an extract of the IAR was made available to the public via the Department's webpage in December 2016, which did not include PI.

Use of the IAR allows for reporting on a number of key information attributes (i.e. numbers of assets with incomplete attributes, number of assets without an assigned owner, etc.). The IAR will also allow the Department to identify similar information assets to determine whether duplicates exist, and record the security classification of information assets based on the Department's classification scheme, which will need to be modelled against CPDP's security classification scheme. Currently, DHHS systems that hold and/or generate the information assets (where the assets are maintained electronically) are separately documented in 'Casewise'.

As the integrated Information Directory, Meta was configured to capture the Department's system register, which was previously held in the 'Casewise' system, and was to be migrated across. Since the first specification of Meta, a decision has been made to split the systems register component into application and technology registers, and extend the meta-model to include capabilities, objectives and strategy objects. At the time of this review, a Request for Tender had been released to progress this work (to include the configuration of the extended Meta-model), which is expected to commence in Q1 2017. In the interim, rather than migrating the full systems register into Meta, the system register was being used only a placeholder to capture the name of systems (applications) associated with information assets.

There are future plans to migrate the system architecture information from 'Casewise' to Meta (the new application and technology registers) in order to tie back information assets to relevant systems as part of the Department's associated data lineage both between information assets and information assets and applications (and capabilities). The Department continues on this effort as a means to further embed and mature their information and system governance framework, as a foundational component of aligning its information security controls with the VPDSF Information Security Guide: Chapter 2 – Protective Markings, WoVG Information Management Principles and the Public Record Office of Victoria (PROV) Standards and Policies.

We support the Department's efforts in this area, as the full roll-out of IAR as a foundational and instrumental building block for proper information management, which has previously been recognised in the VAGO 2015 report[9] that indicated that Agencies need to first understand and properly manage the PI they hold to achieve a fully mature IM environment. Whilst not a legislative requirement of the PDPA 2014, DHHS should continue to build upon the existing IAR to provide greater visibility into the management of its information assets in line with industry best practice.

Refer to Finding #2 for more details on findings and recommendations for remediation.

Operations & Management

The Governance and Strategic Positioning section above details the various internal teams and divisions involved in implementing the requirements outlined in the Department's information governance framework. Appendix A: (Information Governance Documentation Hierarchy) provides details related to the various documents that outline Departmental requirements around information management.

We noted that a number of reviews and audits that have been performed relating to information governance (inclusive of privacy, protective data security and data quality). These reviews and audits have been initiated internally by management, Internal Audit, or externally by bodies such as the VAGO. These reviews and audits have helped the Department determine their compliance with their internal requirements and legislative/regulatory obligations, their current level of maturity and their ability to manage key risks within these areas. Furthermore, there is an annual self-assessment performed by the Department to measure the current maturity of their information management (IM) practices using the IM3 tool developed by Public Record Office Victoria (PROV). The IM3 tool helps measure performance against the Victorian Government IM standards and assess an organisation's maturity against information management best practice. As a result of these various reviews and audits, a number of recommendations are provided to the Department to enhance their current programs of work and uplift relevant capabilities. We noted that currently there is no centralised system or mechanism in place to allow the Department to monitor issues, recommendations and status of actions taken to address findings from the various reviews and audits performed around information management.

Refer to Finding #4 for more details on findings and recommendations for remediation.

A key operation of the Department is the identification and continuous management of risks that pose threats to its ability to comply with legislative/regulatory obligations and/or internal requirements. Breach of privacy and confidentiality has been identified as a key risk in the category of 'Organisational Stewardship'. As a part of this risk identification and management process, a number of risk events related to breach of privacy and confidentiality have been identified, which range from inappropriate data classification to inappropriate incident management resolution and reporting procedures.

Key controls and treatment plans have been identified, documented and individuals assigned ownership for each risk event to ensure risks are appropriately mitigated. The Department has recently commenced reporting on the design and operating effectiveness of key controls and treatment plans and seek to continue reporting on its effectiveness on a quarterly basis.

The role of the Department Internal Audit function is to target and review areas of greatest importance or concern where the potential for improvement, or risks of failure are greatest. As part of the proposed Internal Audit Plan for 2016-17, the following reviews will be conducted and relate to certain

[9] Victorian Auditor General's Office (VAGO), Access to Public Information, December 2015

elements of the DHHS' information governance program: Data Integrity Framework, NIST Cyber Security Assessment, Freedom of Information, Integrated Client and Case Management System.

There are numerous procedures within the Department that define the management of data across the information life cycle (from collection to disposal), including personal information (PI), public sector information (PSI), master data, reference data and meta data.

Incident Management

Prior to the machinery of government changes, the Department of Human Services and the Department of Health maintained their own incident management procedures that extended out to their respective CSOs; the Critical Client Incident Management process. These incident procedures focus on physical, emotional and sexual harm to the Departments' clients, but have also highlighted a 'Breach of privacy confidentiality matters' as a major incident that may cause harm. The incident management processes have been replaced by a newly developed, centralised Client Incident Reporting Process that will utilise a centralised Client Incident Management System (CIMS) and corresponding procedures. Through inquiry of relevant stakeholders, it was noted that the new CIMS system will be accompanied by an associated policy, roles and responsibility guide, a high level communication plan and training of the new system for internal and external staff. We also understand that there is a goal to establish integration between the new CIMS system and a new privacy incident management system (that the Department is looking to implement) to allow for increased connectivity amongst the teams. Currently, privacy and security incidents are maintained within their own respective incident registers.

The department and CSOs are now required to manage privacy incidents through the Client Incident Reporting Process which is used where an incident or alleged incident that involves or impacts on clients during service delivery. The client incident reporting process is designed to ensure that the incidents are quickly identified, assessed and allocated for commensurate action. In relation to privacy incidents, the process is initiated by the completion of an incident report and the Privacy Breach Checklist.

Following completion of the Privacy Breach Checklist, the reporting officer undertakes an initial assessment of the incident in order to apply the appropriate category rating, although all privacy incidents are automatically allocated a 'category one' rating. The divisional privacy officer is usually notified at this stage or may be the reporting officer. Various divisions within the Department maintain a local divisional Privacy Officer that assists in the privacy incident assessment process, prior to reporting to 'central management', i.e. the Complaints and Privacy Unit. The divisional privacy officer provides the first line assessment of whether the incident noted by front-line staff is a breach versus an incident. As a part of their service agreement, CSOs are required to report all incidents to DHHS.

Incidents are then reported centrally to 'central management'. It was noted that currently there is no central electronic system in place to report/log privacy incidents, as these are currently facilitated through the completion of an offline Privacy Breach Checklist, which is either faxed, scanned and attached to an email or, in the case of the Child Protection division, sent via an attachment to 'central management' via the CRIS system.

The divisional privacy officer may contact the central Complaints and Privacy Unit to seek advice on issues including:

- whether CPDP and/or individuals whose privacy may be affected should be notified of the incident; and
- if further investigation is required and if so, if an external investigator should be appointed.

The escalation pathway for privacy incidents includes reporting on incidents constituting a breach of privacy to CPDP and/or affected individuals, which is determined on a case-by-case basis. DHHS currently does not have a defined or documented guidance and relevant criteria to help DHHS assess: (a) whether to notify affected individuals, and, if so; (b) consider when and how notification should occur, who should make the notification, and who should be notified; (c) consider what information should be included in the notification, and (d) consider who else (other than the affected individuals) should be notified (e.g. reporting to the CPDP). It was noted that privacy breaches, including resolution, are reported to the Board on a periodic basis, though again, this is not currently guided by defined notification and reporting requirement.

Currently there is no data quality specific incident management plan. However, the management of data quality incidents will be deemed the responsibility of the data custodian identified for the related information asset. The process for addressing quality issues with personal information is governed by the Freedom of Information Act 1982 (FOI Act) for most public sector agencies, including the department and CSPs by extension. The only redress available under the FOI Act is a notation added to the personal information and the applicant must be able to satisfy an agency that the information is incomplete, incorrect, out of date or misleading. The FOI Act requires the department to notify the individual of its decision within 30 days of receipt of the request.

There also is a Cyber Security Incident Management Plan (which covers more than just cyber security incidents; other types of security will be captured as well) managed by Information and Identity Security and supported by an Information Security Incident Management Policy. Privacy and security incidents identified both within the Department and by the Department's Community Service Organisations (CSOs) are generally logged leveraging the documented procedures outlined in the Privacy Breach Checklist and/or Cyber Security Incident Management Plan. The Department maintains an Incident Notification Group (ING) who are responsible for assessing the impact and scope of identified incidents, as well as an Incident Committee, made up of members across the Department, who help execute against the defined escalation and reporting procedures.

The Whole of Victorian Government (WoVG) Incident Management Committee provides funding, on an ad-hoc basis, for Victorian government agencies to test their security incident management plans. The last test performed by DHHS was April 2015, which led to improvements/refinements being made to the Department's Cyber Security Incident Management Plan and Information Security Incident Management Policy. However, it was noted that this test focused on cyber security as opposed to other related domain areas of personnel and physical security. However, we recognise that personnel and physical security controls are subject to the ISMF Self-Assessment Compliance, which is completed annually by the Security Manager and CIO, and submitted to the Department of Treasury and Finance. Whilst the privacy incident management procedures and processes are not subjected to planned and regular reviews, the recent high-profile privacy breaches that came under the Leatherland review has served to validate areas of strength and improvement opportunities to further strengthen the Department's privacy incident management process. The key recommendations arising from the Leatherland report[10] are currently part of the Department's program of work to improve their framework for managing privacy incidents.

Refer to Finding #3 for more details on findings and recommendations for remediation.

Contracted Service Providers

Currently, DHHS maintains thousands of active service agreements and contracts with various types of Contracted Service Providers (CSPs) throughout Victoria to deliver their services to the Victorian community, as well as support the Department. Essentially, CSPs are broken down into two categories:

- **Community Service Organisations** (CSOs) – DHHS provides funding to a number of organisations to provide services to the Victorian community on their behalf; often times referred to as funded organisations. These CSOs provide support to Victorian citizens (known as the Department's 'clients') as part of the Department's various programs. Examples of CSOs in the home based care program include: Anglicare Victoria, Berry Street, Family Life, and Connections UnitingCare.

[10] Leatherland, John, Review of Child Protection Privacy Incidents and Carer and Client Safety for Department of Health and Human Services, August 2016.

- Commercial Third Party Service Providers – DHHS maintains agreements with contracted service providers (i.e. commercial third party service providers who provide a service directly to the Department). An example of a commercial third party service provider is CenITex, which provides a range of ICT support, including system hosting services, to DHHS.

The primary mechanisms that DHHS uses for monitoring the compliance of their CSPs (both CSOs and commercial third party service providers) to their information management obligations (as it relates to privacy, protective data security and data quality) include:

- Agreements with CSPs (service agreements for CSOs and contractual agreements for commercial third party service providers) – These agreements (both service and contractual) directly highlight the need for the CSP to comply with regulatory (PDPA 2014, HRA 2001, *Freedom of Information Act* 1982, *Public Records Act* 1973, etc.) and internal DHHS requirements relating to information management obligations, as well as the right of DHHS to perform or request an independent third party to perform an audit or review of the third party's compliance with the service agreement.

We noted that all agreements with CSPs (service agreements for CSOs and contractual agreements for commercial third party service providers) maintain similar clauses in relation to their privacy, protective data security and information management requirements. Through review of a sample of recently completed service and contractual agreements, we noted the following general requirements that organisations must comply with, as outlined in clause 17 of the service agreement:

- Collect, hold, use, manage, disclose, transfer and dispose of data in accordance the IPPs, HPPs and other requirements laid out in the PDPA 2014 and HRA 2001
- Manage all records in accordance with standards under the *Public Records Act* (PRA) 1973, including storage, security and record keeping
- Provide access to records of the Department exercising rights under the Freedom of Information Act
- Dispose of records in accordance with the *PRA* 1973
- Maintain an Asset Register listing all details of each asset
- Provide Department with information about and report on services provided, including information management procedures
- Immediately notify the Department of a breach
- Make individuals aware that the Department may disclose their personal information in accordance with providing services through the utilisation of third party service providers and/or in accordance with the law

Specifically for the CSOs, the existing monitoring mechanisms with varying degrees of applicability to information management obligations (as it relates to privacy, protective data security and data quality) include:

- Funded Organisation Performance Monitoring Framework (FOPMF) – The FOPMF is used to assess CSOs' adherence to the service agreement requirements, which includes compliance with the PDPA 2014 and HRA 2001.
- Quality review against the Human Services Standards ('Standards') – A quality review is performed by an independent review body once every three years, which represent a single set of service quality standards for CSOs that cover Empowerment, Access and Engagement, Wellbeing, Participation, Governance and Management.
- Unannounced performance audits of home based care CSOs - These audits assess CSOs against all the service delivery standards, with a particular focus on client safety and wellbeing, as well as their compliance with program requirements.

In 2015, DHHS refreshed their FOPMF, a key department policy supporting service quality and sustainability for organisations funded under Service Agreements. The FOPMF provides an end-to-end process for monitoring CSOs to confirm each organisation's compliance with service agreement requirements, to risk assess identified issues, to monitor and respond to performance issues and to respond to identified risk.

The FOPMF requires organisations to complete a Service Agreement Compliance Certification (SACC) form to certify annually that they are compliant with the service agreement requirements, which includes compliance with the PDPA 2014 and HRA 2001. Submission of these annual attestations by the CSO, combined with information collected through ongoing monitoring of the CSO (via the SAMS system) and regular Departmental engagement are aimed at providing levels of assurance for DHHS. The chief executive officer (CEO) of each CSO signs the annual attestation and does so as the accountable representative from their organisation.

All service agreements for CSOs include provisions requiring the funded organisations to comply with Standards and performance targets, departmental policies and the legislated registration process, where required. CSOs must also agree to undertake a quality review against the Standards by an independent review body once every three years, and any additional performance reviews in relation to compliance with the Standards or accreditation. We recognise that the Standards represent a single set of service quality standards for CSOs that cover Empowerment, Access and Engagement, Wellbeing, Participation, Governance and Management, which are laid out in the Performance oversight and enforcement – residential care policy (released by DHHS on May 2016). Specifically, Standards 1.1, 1.2 and 3.5 outlines the specific requirements related to the privacy and confidentiality obligations of the CSOs. At the time of this review, it was noted that these set of requirements had not been updated to reflect the updated PDPA 2014, and still referenced the prior Information Privacy Act 2000. Furthermore, it was noted that a performance review of the CSOs against these specific Standards is only applied to a subset of CSOs utilised by DHHS. For those performed, the reviews may not be conducted by independent reviewers with an appropriate level of understanding and knowledge of the privacy, protective data security and data quality requirements outlined by the PDPA 2014 and VPDSS, as the primary focus of these reviews are on the quality of service being provided rather than compliance with privacy and security requirements.

A quality review is the routine monitoring of service delivery of CSOs by DHHS staff. If the quality review identifies an issue of sufficient magnitude, a service review may be undertaken. That is, the undertaking of a service review only occurs in response to a trigger event. At the time of this review, there was no recent examples of a CSO being subjected to a service review specific to the funded organisation’s information governance practices (as it relates to privacy, protective data security and data quality).

Unannounced audits of CSOs may also occur for out-of-home care. The CSOs that are chosen for an unannounced audit are prioritised through the risk-tiering process. The audits are conducted by staff from the DHHS’ Compliance and Quality Unit within the Performance and Reporting Branch. These audits assess CSOs against all the service delivery standards, with a particular focus on client safety and wellbeing, as well as their compliance with program requirements. The CSOs that are chosen for an audit are prioritised through the risk-tiering process. At the time of this review, there was no recent examples of a CSO being subjected to an unannounced audit specific to the funded organisation’s information governance practices (as it relates to privacy, protective data security and data quality).

There is a Service Agreement Management System (SAMS) in place that monitors all active service agreements with CSOs. SAMS is used to record risks that are identified within the CSO’s environment and actions taken to remediate such risks. DHHS staff utilise SAMS to actively monitor DHHS’ relationships with CSOs. While live monitoring is directed more towards the quality and delivery of services (and less towards privacy, protective data security and data quality) it is possible for information management issues to be identified and tracked within SAMS.

The Standards and Regulations Unit (SRU) is responsible for the oversight of third party certification audits that are required every three years along with the registration of particular services every three years. It was noted that the SRU also maintain two (2) separate registers for CSOs that are registered under the *Disability Act* and *Children, Youth and Families Act*. The organisations maintained in these registers would also be in the SAMS. It was noted that a subset of CSOs used by DHHS would be covered by the SRU third party certification requirements. For the CSOs that must comply with these Acts, they must undertake one full independent certification review against the Department’s Human Services Standards, subject to a set of requirements that will deem the CSO to be lower risk. The

Department has endorsed 10 independent review bodies to certify/accredit the CSOs against the Human Services Standards.

Monitoring the adherence of commercial third party service providers (who handle, process and store the Department's PI) against information governance practices (as it relates to privacy, protective data security and data quality) and legislative requirements set forth in the PDPA 2014 and VPDSS requirements does not follow the same approach that is defined for CSOs (as outlined above). We understand that DHHS has initiated a process to streamline and enhance its assessment capacity over commercial third party service providers, which will include a quarterly exercise to check new third party commercial contracts to validate its inclusion of the required clauses in relation to their information management requirement, and ongoing due diligence over privacy and security for outsourced IT data centres, which may include the receipt and review independent Service Organisation Control (SOC) Type II Report or other third party monitoring reports for the outsourced vendors. However, for DHHS's main commercial IT service provider (CenITex), there is a monthly Operation Security Report that is compiled and analysed by the Department's Security Manager and CIO; and is intended to provide visibility of risks, current threats, trends and an update of CenITex Security efforts for the month under review. This monitoring mechanism is well established for CenITex, but does not extend out to all commercial third party service providers.

Refer to Finding #1 for more details on findings and recommendations for remediation.

3 Detailed Findings

The following section outlines the detailed findings identified during the DHHS Information Governance Review that was completed over the September – November 2016 period, as well as the management actions required to address these issues.

1 Information management due-diligence and compliance procedures for contracted service providers (CSPs) should be enhanced

Priority – High

Root Cause – People, Procedure

VPDSF Principle – 2, 6

VPDSS – 9, 10, 12, 13, 14, 15

Finding and recommended actions

Under the PDPA 2014, whilst a contracted service provider (CSP) may process and store PI on behalf of an outsourcing party and be held responsible for their internal data security and management procedures, the ultimate accountability for the protection of PI remains with outsourcing party (i.e. DHHS).

The primary mechanisms DHHS uses for monitoring the compliance of their third party organisations to their information management obligations includes:

- **Service agreements with Community Service Organisations (CSOs)** and contractual agreements with commercial third party service providers – These agreements directly highlight the need for the CSP to comply with regulatory (PDPA 2014, HRA 2001, *Freedom of Information Act* 1982, *Public Records Act* 1973, etc.) and internal DHHS requirements relating to information management obligations, as well as the right of DHHS to perform or request an independent third party to perform an audit or review of the third party's compliance with the service agreement.

Specifically for the CSOs, the existing monitoring mechanisms with varying degrees of applicability to information management obligations (as it relates to privacy, protective data security and data quality) include:

CSOs

- **Funded Organisation Performance Monitoring Framework (FOPMF)** – The FOPMF is used to assess CSOs' adherence to the service agreement requirements, which includes compliance with the PDPA 2014 and HRA 2001.
- **Quality review against the Human Services Standards ('Standards')** – A quality review is performed by an independent review body once every three years, which represent a single set of service quality standards for CSOs that cover Empowerment, Access and Engagement, Wellbeing, Participation, Governance and Management.
- **Unannounced performance audits of CSOs** - These audits assess CSOs against all the service delivery standards, with a particular focus on client safety and wellbeing, as well as their compliance with program requirements.

Commercial third party service providers:

For DHHS's main commercial IT service provider (CenITex), there is a monthly Operation Security Report that is compiled and analysed by the Department's Security Manager and CIO; and is intended to provide visibility of risks, current threats, trends and an update of CenITex Security efforts for the month under review.

However, the following was noted in relation to these existing monitoring mechanisms:

- The Performance oversight and enforcement – residential care policy (released by DHHS on May 2016), which outlines the privacy and confidentiality obligations of the CSOs had not been updated to reflect the updated PDPA 2014, and still reference the *Information Privacy Act* 2000.
- It was noted that a quality review of the CSOs against the specific privacy and confidentiality obligations set forth in the Department's Human Services Standards is only applied to a subset of CSOs utilised by DHHS (i.e. residential care). Furthermore, for those performed, the reviews may not be conducted by independent reviewers with an appropriate level of understanding and knowledge of the privacy, protective data security and data quality requirements outlined by the PDPA 2014 and VPDSS.
- Unannounced performance audits of CSOs are conducted by staff from the DHHS' Compliance and Quality Unit within the Performance and Reporting Branch. Due to resource constraints, these audits may not be conducted by DHHS resources with an appropriate level of understanding and knowledge of the privacy, protective data security and data quality requirements outlined by the PDPA 2014 and VPDSS.
- The CSOs that are chosen for an unannounced performance audit are prioritised through the risk-tiering process. At the time of this review, there was no recent example of a CSO being subjected to an unannounced performance audit specific to the funded organisation's information governance practices (as it relates to privacy, protective data security and data quality), despite the rise in a number of PI breaches reported to the CPDP, some of which originated from PI data exposure at the CSOs.
- A similar framework for monitoring the adherence of commercial third party service providers against information governance practices (as it relates to privacy, protective data security and data quality) and legislative requirements set forth in the PDPA 2014 and VPDSS requirements does not follow the same approach that is defined for CSOs. Whilst we recognise that the Department may request and receive an independent Service Organisation Control (SOC) Type II Report or other monitoring reports (e.g. monthly CenITex Operations Security Report) for certain outsourced vendors, these third party monitoring reports are not always available, and supplemental monitoring activities are not well defined for the other commercial third party service providers that DHHS deals with.

Implication

By not performing an appropriate level of monitoring over CSPs and their adherence to the privacy and security requirements set forth in the service and contractual agreements, there is a risk that these CSPs do not adequately handle and secure clients' PI in accordance to DHHS requirements and legislative obligations set forth in the PDPA 2014, which may lead to further privacy incidents.

Recommendations

Recognising the limitations that exists for DHHS around resource staffing and Department funding, and the sheer volume of active CSPs that DHHS deals with (both CSOs and commercial third party service providers), it is recommended that DHHS:

1.1 Develop and establish a process to categorise new and existing CSPs according to risk, leveraging on the risk assessment model already in place for the Standards and Regulation Unit (SRU) and other areas of the Department.

[Implementation guidance: This approach could assist in risk identification and management (specifically in the domains of privacy and protective data security), using threshold and impact assessment guidance and forms. This risk model may be based on a variety of critical attributes that may include, but not limited to the following:

- nature of the programs delivered (specifically for CSPs)
- how much DHHS funds the CSOs and/or spends with the commercial third party service provider
- volume of data shared with the CSP
- Rrecent privacy and/or security incidents experienced within the CSP's environment
- sensitivity of the data shared (e.g. PI, PHI, and other sensitive data types)
- where the data is processed and how those local jurisdictional requirements align to DHHS expectations as an organisation bound by the PDPA 2014 and HRA 2001]

1.2 Based on the risk rating assigned to the CSOs, strengthen the existing monitoring mechanisms in place to assess the CSOs' adherence to specific privacy and security obligations.

[Implementation guidance: Monitoring activities could specifically address:

- updating the Performance oversight and enforcement – residential care policy (released by DHHS on May 2016) to reflect the updated PDPA 2014.
- providing additional training to the independent review bodies (who are involved in the quality reviews) and the DHHS' Compliance and Quality Unit (who are involved in the unannounced audits) to enhance their understanding and knowledge of the privacy, protective data security and data quality requirements outlined by the PDPA 2014 and VPDSS.
- for the unannounced performance audits of CSOs, confirming that CSOs have information governance policies (as it relates to privacy, protective data security and data quality) in place, and that instances of information governance breaches are added to the risk tiering calculation for that CSO.]

1.3 Based on the risk rating assigned to the commercial third party service providers, strengthen the existing monitoring mechanisms in place to assess the third party's adherence to specific privacy and security obligations.

[Implementation guidance: These monitoring mechanisms (listed by level of assurance from low to high) could include, but are not limited to: management attestations, self-assessment questionnaires, desktop reviews, site reviews, independent audit and reviews, review and receipt of SOC 2 reports.]

1.4 Communicate and train contract managers and other relevant stakeholders within DHHS for new / updated procedures for monitoring CSPs for their adherence to privacy and security requirements.

2 A detailed information asset register has been established, and should be fully populated to document the Department's assets and link to the systems register

Priority – Medium

Root Cause – People, Procedure

VPDSF Principle – 3

VPDSS – 13, 14

Finding and recommended actions

In order for organisations to take the reasonable steps to protect personal information from misuse, loss, unauthorised access, modification or disclosure (in accordance IPP 4 of the PDPA 2014), it is essential for organisations to be able to identify and understand their personal information holdings. This can be supported with the development and maintenance of an information asset register, which provides organisations a better understanding of the risks associated with certain information, required compliance with regulation and better management over information to support internal decisions and business initiatives.

DHHS is currently in the process of further populating their Information Asset Register (IAR), including documenting governance roles associated with the Department's information assets in accordance with the DHHS Information Asset Governance Policy, as well as track the location of all information assets and other relevant attributes. The IAR has used content from legacy information asset registers from the former Departments in the first instance, with content being verified and updated several times as the Department implements additional organisation restructure. However, there are still quite a large number of information assets yet to be fully documented within the current instance of the IAR.

Currently, Meta does not currently provide an integrated and holistic view of DHHS systems that hold and/or generate the information assets, as this is separately documented in 'Casewise' system register. We recognise that there are future plans to migrate the system architecture information from 'Casewise' to the equivalent registers in Meta in order to tie back information assets to relevant applications; which are subsequently linked to technology; (which is expected to commence in Q1 2017). In the interim, rather than migrating the full systems register into Meta, the system register in Meta was being used only as a placeholder to capture the name of systems (applications) associated with information assets.

It was further noted that the IAR does not currently capture data quality requirements or data quality metrics, however it does provide linkage to the data quality statement, which highlights data quality issues. However, data quality statements have not yet been defined for those information assets already recorded within the IAR.

Implication

The absence of a fully populated IAR and documented data lineage, both between information assets and information assets and systems (applications), may leave the Department susceptible to not maintaining a holistic view over all of its critical information assets across its lifecycle to ensure the appropriate level of controls are in place to protect the information and ensure appropriate usage from capture to destruction. It is important that robust mechanisms for maintaining the IAR is executed periodically as information assets is always changing.

Recommendations

Recognising that DHHS is involved in an on-going process to populate the IAR and integrate the Department's enterprise architecture, it is recommended that DHHS:

2.1. Leverage the existing IAR to provide greater visibility of the management of its information assets in line with best industry practice, which includes:

- outlining the DHHS systems that manage and/or generate the information assets
- populating the data quality requirements or data quality metrics associated with the information assets.

2.2 Develop and implement a communication strategy and plan to enhance DHHS stakeholders' understanding of the DHHS roles defined and implemented as it relates to information governance, including specific training to those DHHS staff members holding these information governance roles.

3 Incident management procedures for regulator notification and data quality management should be enhanced

Priority – Medium

Root Cause – People, Procedure

VPDSF Principle – 6

VPDSS – 5, 7

Finding and recommended actions

Whilst we recognise that DHHS has established and implemented procedures related to privacy and information security incident management, it was noted that the Department could further enhance its procedures in the following areas:

- external notification and reporting of incidents
- testing and review of defined incident management procedures
- established post-incident feedback mechanisms where lessons learned from noted incidents are considered and leads to enhanced internal communication and training and/or revisions to the documented incident management policies and procedures.

It was noted that DHHS currently does not have defined or documented guidance and relevant criteria to help DHHS assess: (a) whether to notify affected individuals, and, if so; (b) consider when and how notification should occur, who should make the notification, and who should be notified; (c) consider what information should be included in the notification, and (d) consider who else (other than the affected individuals) should be notified (e.g. reporting to the CPDP). It was noted that privacy breaches, including resolution, are reported to the Board on a periodic basis, though again, this is not currently guided by defined notification and reporting requirement. The incident management policies and plans reviewed make mention of consideration to communicate incidents to the CPDP and affected individuals, but do not provide a guidelines for triggering notification.

The Guide to effectively responding to privacy incidents states that 'the decision to inform affected individuals following the discovery of a privacy incident is not straightforward and cannot be reduced to a checklist exercise...', but further goes on to list a number of key factors and considerations in determining whether to notify an individual or not notify. These same factors have not been defined when it comes to determining whether notification to CPDP is required. There is also no defined process for what to do once CPDP has been notified of an incident, has provided recommendations and feedback mechanism for DHHS to communicate their implementation of recommendations to close the incident.

Additionally, we noted that the last incident management procedures test performed by DHHS was in April 2015, which led to improvements/refinements being made to the Department's Cyber Security Incident Management Plan and Information Security Incident Management Policy. Through review of the test, it was noted that the scope focused on cyber security and excluded other areas such as personnel security and physical security, though we do recognise that personnel and physical security controls are subject to the ISMF Self-Assessment Compliance, which is completed annually by the Security Manager and CIO, and submitted to the Department of Treasury and Finance. Additionally, the privacy incident management procedure has not been recently tested for effectiveness.

Implication

By not establishing and applying a set of approved criteria and requirements to trigger external notification and reporting, relevant incidents may not be reported to the appropriate parties, while irrelevant incidents are. A risk also arises when incident management plans are not reviewed and tested for effectiveness on a periodic basis to ensure the appropriate procedures have been implemented and embedded within the organisation.

Recommendations

Recognising that DHHS has made progress to develop and implement incident management procedures, it is recommended that DHHS:

3.1 Establish a set of factors for consideration when determining when to notify the Department's Board and CPDP of a privacy incident, similar to the factors that have been defined for notification to affected individuals.

3.2 Establish procedures to advise the status of CPDP recommendations to the Department's Board and to CPDP.

3.3 Establish the frequency in which the DHHS incident management plan, and privacy breach checklist and incident procedures should be tested to ensure the effectiveness of each plan.

[Implementation guidance: The results of the periodic testing could be considered and factored into enhancements to internal communication and training and/or revisions to the documented incident management policies and procedures.]

3.4 Develop a plan with timelimes for the implementation of a new information technology tool for the management of privacy incidents to provide end-to-end recording, investigation and resolution of all incidents.

[Implementation guidance: Such a tool could enhance the monitoring and oversight of performance and facilitate the identification of systematic issues that arise and leads to enhanced internal communication and training and/or revisions to the documented incident management policies and procedures.]

4 There should be a centralised view and monitoring of issues, recommendations and a status of actions taken to address findings from various reviews and audits performed around information management

Priority – Medium

Root Cause – People, Procedure

VPDSF Principle – 1, 4

VPDSS – 1, 2, 14

Finding and recommended actions

Over recent years, there have been a number of reviews and audits performed relating to information governance. These reviews and audits have been initiated internally by management and/or Internal Audit, or externally by regulatory bodies such as the Victorian Auditor General's Office (VAGO). Examples include:

Management-initiated:

- Security – External penetration testing every 2 months
- Targeted internal penetration testing of critical applications/systems such as HiiP, CRIS, Payroll, Finance, etc.
- Information Management Maturity Report– Self-assess maturity annually (June) utilising the PROV Information Management Maturity Measurement (IM3) tool
- ISMF Self-Assessment Compliance Report – completed annually
- Security assessment based on Australian Signals Directorate ISM framework and WoVG Security Policies and Standards
- Review of Child Protection Privacy Incidents and Carer and Client Safety (2016, completed by John Leatherland)

Internal Audit-initiated:

- Internal Penetration test (May 2016, completed by a professsional services firm, DHHS responsible stakeholder – Steve Hodgkinson)
- Information Security and Management (May 2015, completed by a professsional services firm, DHHS responsible stakeholder - General Counsel and Chief Legal Officer, Director of Statutory and Forensic Services.
- CRIS Review – ITGC review (2015, completed by a professsional services firm, DHHS responsible stakeholder – Director Service Implementation and Support Branch, IM&T Manager, Business Engagement Unit
- Application of Information Privacy Principles (July 2015, completed by a professsional services firm)

Externally-initiated:

- Annual VAGO security audit

Whilst we were able to discuss the status and resolution of the recommendations arising from these reviews and audits, there was no centralised view or monitoring of these recommendations by Executive Services and Oversight (ESO) until late 2016, where the recommendations and status were tracked through an Excel spreadsheet. It was noted that currently reviews performed by Internal Audit, VAGO, Victorian Ombudsman, Parliamentary Inquiry and Coronial requirements are tracked by ESO, while any other reviews are tracked by individual directors accountable for the scope of the review, through the use of Microsoft Excel spreadsheets and other offline mechanisms. We also recognise that while it is Internal Audit's remit to follow up on recommendations made in prior internal audit reports, this centralised monitoring process does not extend to those recommendations arising from management-initiated and externally-initiated reviews/audits. It was noted that the ESO will continue with the identification and implementation of a suitable centralised electronic tracking platform, noting that this platform will be made available to all branches. The ESO also intends to work with other teams to advocate usage of the platform department-wide to provide a centralised view of audit findings, corresponding recommendations and current remediation status to enable adequate management and governance of information risk within the Department as a whole.

Implication

Whilst the various reports and review actions may be owned and actively monitored by specific individuals or team across the various divisions of the Department, the siloed approach prevents the Department from achieving a holistic view of in-flight projects and remediation efforts that relate to information governance. As such, in the absence of centralised view of all related findings and recommendations, the Department may not be able to track recommendations that have been completed and those that have been delayed, and apply the necessary efforts to adequately manage and govern information risk within the Department as a whole.

Recommendations

It is recommended that DHHS (ESO):

4.1 Implement a suitable centralised electronic tracking platform.

[Implementation guidance: ESO could work with other teams to advocate usage of the platform department-wide to provide a centralised view of audit findings, corresponding recommendations and current remediation status to enable adequate management and governance of information risk within the Department as a whole. It is also recommended that the existence of this platform be made available to all branches.]

5 Scenario-based information management training should be developed and administered to relevant branches or local teams, based on their functional responsibilities

Priority – Medium

Root Cause – People, Procedure

VPDSF Principle – 4

VPDSS – 5, 6

Finding and recommended actions

The Department has progressed significantly in its development and implementation of Department-wide privacy and information security training. However, through review of the previous privacy training materials, it was noted that it is high level and aimed at providing general compliance requirements, rather than providing detailed guidance to DHHS employees on how to meet privacy and DHHS requirements for specific programs, branches and/or local teams.

We recognise that recommendations have already been made in regards to developing and enhancing scenario-based privacy training for Child Protection workers that focuses on the basic day-to-day 'do's and don'ts' of privacy, security and information sharing, for that specific job function. Additional discussions held with Child Protection workers during this review indicated that they would benefit from targeted privacy training and awareness that provided more guidance on acceptable procedures relating to their day-to-day activities. Specifically, there were requests for more targeted training to be provided around information sharing, leveraging on the established guidance outlined in the Department's Data Access and Release Policy, with further scenarios developed that were relevant for their roles/responsibilities within their respective program.

It was further noted during the course of our review that training does not currently exist for all domains of information management (specifically data quality) and upon approval of the Information Management Strategy, the Department will begin to roll out further training in relation to the other domains of information management.

Implication

The absence of scenario based training (whether eLearning, on-the-job and/or supervision based) may impact the level of understanding of DHHS employees (FTE, part-time, contractors) to handle PI appropriately in an open, transparent and protected way in alignment with DHHS requirements and legal obligations set forth in the PDPA 2014, HRA 2001, and other relevant acts.

Recommendations

Recognising the initiatives already underway to provide updated, targeted scenario-based training to some practitioners, DHHS should:

5.1 Further enhance and provide scenario-based, program specific privacy training for other functional areas within DHHS for which training has not been developed and which have heightened privacy risks associated with handling of clients' PI.

[Implementation guidance: This may include a deep-dive in certain areas that may include, but not limited to the Data Access and Release Policy, guidance on the appropriate sharing of information and the individual's rights to view information (from the standpoint of the client, caseworker, guardian/parent), data quality management, etc. Whilst we recognise the Department's staffing limitations, we suggest a risk-based approach be taken for prioritising the areas that require this training.]

5.2 Expand Department-wide training to cover the other domains of overall information management (including data quality management), and the related policies and procedures.

[Implementation guidance: We recognise this will be a key initiative following approval and execution of the DHHS Information Management Strategy. This Department-wide training may include, but not limited to:

- elements from the current documentation (e.g., Information Asset Governance Policy, Information Security Management Framework, and Data Access and Release Policy)
- further guidance on the roles established in relation to information governance (e.g., Information Owner, Information Steward, Information Custodian, Information Administrator, etc.) and the relationship of these roles to existing roles responsible for privacy and security
- further guidance on the population, usage and maintenance of the IAR, which is currently in the process of being populated fully across DHHS.]

6 The overall management and maintenance of relevant information governance documentation and standard requirements should be strengthened

Priority – Medium

Root Cause – People, Procedure

VPDSF Principle – 5, 5

VPDSS – 1, 14

Finding and recommended actions

Whilst we noted that numerous frameworks, policies, standards, guidelines and operating procedures relating to information governance (specifically privacy, protective data security and data quality) have been established to manage the handling of personal information by DHHS employees and may be shared with Community Service Organisations (CSOs) and commercial third party service providers for alignment with internal DHHS requirements, there is currently no documented link to guide coordination of the various documents that help put these practices into operation.

For example, in our desktop review of DHHS provided documentation and mapping exercise (refer to Appendix A) against an industry recognised documentation hierarchy, we noted the following:

- The current policies, standards and procedures that have been established for privacy do not currently link to an existing, overarching privacy framework and/or maturity model/privacy improvement plan. Whilst we recognise that the existing DHHS Privacy Policy has guided the development of the current privacy policies, standards and procedures, a Framework would provide a comprehensive view from privacy strategy through to privacy operations across DHHS and may include, but not be limited to the following sections or references: Privacy Strategy; Privacy Policy and Procedures; Privacy Operations; and Privacy Treatment Plans and Controls
- The DHHS Information Management Strategy 2016-2020 has recently been updated and has been presented for executive management consideration in October 2016. As such, there may be existing documents across the information management domains that will need to be reviewed/updated to ensure alignment with the updated strategy
- There are policies, standards and procedures that were developed prior to the merger of Department of Health and Department of Human Services across the information governance domains that will need to be reviewed/updated to ensure alignment with the updated DHHS environment. However, we noted that this has been largely progressed for key policy areas including the information asset governance, data access and release, data quality, identify access management and privacy
- The control sheet at the front section of the documents were not always updated to reflect the last review date for the document and/or whether the document was superseded by an updated version of the document
- Policies, standards and procedures that were developed prior to the recent issuance of the VPDSF (in June 2016) will need to be reviewed/updated to ensure alignment with the new VPDSF requirements. For example, when comparing the new classification formats outlined in the DHHS Information Security Classification Fact Sheet (issued in August 2016) to the information security classification guidelines outlined in the VPDSF Information Security Guide (issued in June 2016), there was a misalignment with the classifications (i.e. the DHHS guidelines currently is missing the 'Confidential'[11] classification). Whilst PwC acknowledges that the DHHS classification scheme has been developed to primarily align with the DHHS Risk Framework BILs and Federal Government Security classification framework, the information security classification guidelines should be updated to outline rationale for DHHS not deeming the top two VPDSF BIL levels relevant to

[11] The security classification of CONFIDENTIAL is used when compromise of the confidentiality of the information could be expected to cause significant harm/damage to government, operations, organisations and individuals.

measuring risk within the DHHS risk context and that their usage will be handled on a case by case basis.

Moreover, it was noted that not all e-learning modules are currently managed on the Learning Management System (LMS), as such there are limits to the procedures in place to ensure and validate that all relevant employees within DHHS have been made aware of pertinent documentation and understand how to apply those to their daily activities, absent of face-to-face training.

As noted by a past Internal Audit review, there was inconsistency on implementing program specific privacy guidelines for all programs, where it would not be included in respective Practice Manuals.

Implication

Outdated, missing and/or unlinked documents may result in DHHS employees and CSOs not being able to adequately meet their regulatory and client expectations for handling PI in an open, transparent and protected way. Additionally, a document hierarchy would be valuable for policy and procedural owners in ensuring a consistent approach to the creation and update of frameworks, procedures and guidelines, which will help in the delivery of training.

Recommendations

Recognising that the machinery of government changes and recent issuance of the VPDSF has resulted in continuous pressures for DHHS to manage and maintain their governance documentation and standard requirements, it is recommended that DHHS:

6.1 Establish a plan to review existing documentation to align with the new measures and requirements established in the DHHS Information Management Strategy 2016-2020, VPDSF and other key changes in DHHS organisational requirements.

[Implementation guidance: This could include a communication plan to raise awareness of revised and/or newly developed documentation to the relevant DHHS employees and CSOs, where shared with them, which could be facilitated through the additional scenario-based training.]

6.2 Ensure that the control sheet at the front section of the documents reflect the last review date for the document and/or whether the document was superseded by an updated version of the document.

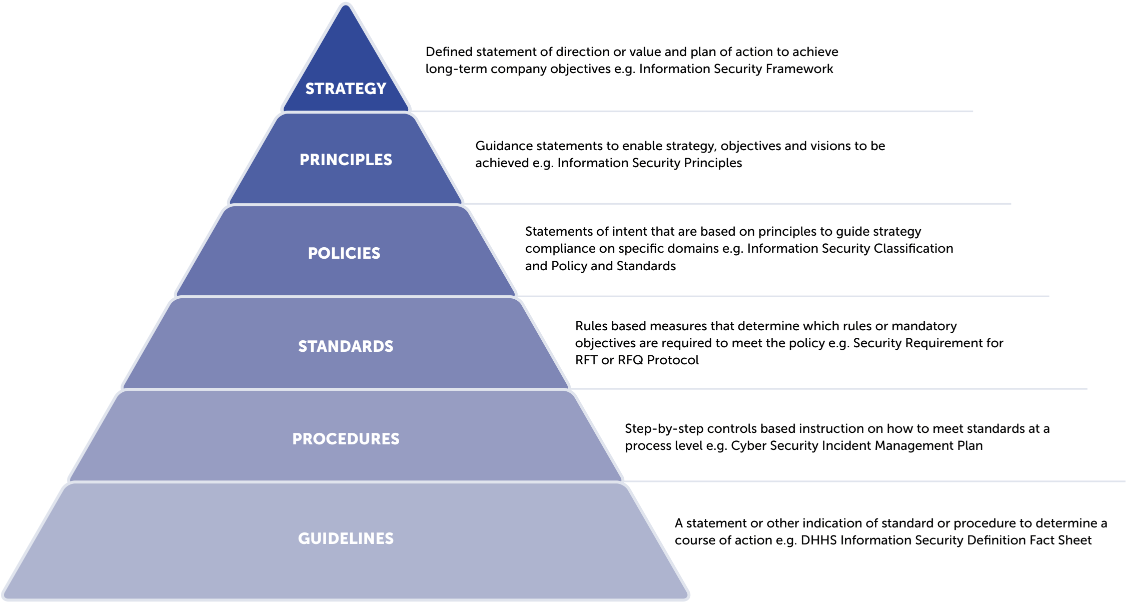
6.3 List and develop a plan to produce key documentation that is deemed to be important but is currently missing.

[Implementation guidance: An example is a Privacy Framework that could provide a comprehensive view from Privacy Strategy through to Privacy Operations across DHHS].

Appendices

Appendix A – Information Governance Documentation Hierarchy

The following diagram outlines an industry recognised documentation hierarchy that was referenced in our desktop review of the DHHS provided documentation and mapping exercise:



Defined statement of direction or value and plan of action to achieve long-term company objectives e.g. Information Security Framework

Guidance statements to enable strategy, objectives and visions to be achieved e.g. Information Security Principles

Statements of intent that are based on principles to guide strategy compliance on specific domains e.g. Information Security Classification and Policy and Standards

Rules based measures that determine which rules or mandatory objectives are required to meet the policy e.g. Security Requirement for RFT or RFQ Protocol

Step-by-step controls based instruction on how to meet standards at a process level e.g. Cyber Security Incident Management Plan

A statement or other indication of standard or procedure to determine a course of action e.g. DHHS Information Security Definition Fact Sheet

	STRATEGY / FRAMEWORK	PRINCIPLES	POLICY / STATEMENT	STANDARDS	PROCEDURES	GUIDELINES / FACT SHEET
INFORMATION MANAGEMENT	DHHS Information Management Strategy 2016 - 2020 DHHS Information Management Strategy 2016 - 2020 Appendices DHHS Records Management Strategy 2015-2018 Risk Management Policy and Framework 2015 - 16	DHHS Information Management Principles Information Usage Agreement for the Risk Assessment and Management Panel Program	DHHS Information Asset Governance Policy DHHS Records Management Policy	Meta-data Standards	Information Sharing Protocol between Commonwealth and Child protection Agencies Protocol for the transfer of Care and protection Orders and proceedings and Interstate Assistance	DHHS Personal Information Fact Sheet Guidelines for populating DHHS Information Asset Register Information Sharing CP CF and Family Service Client Incident Management System Summary Guide Responding to subpoenas (2221) Preparing the court report (2224) DHHS Information Asset Definition Factsheet DHHS Information areas - Key Contact details

	STRATEGY / FRAMEWORK	PRINCIPLES	POLICY / STATEMENT	STANDARDS	PROCEDURES	GUIDELINES / FACT SHEET
PRIVACY	DHS Privacy Framework	DHHS Service Agreement (Sec 17) Child protection and Integrated Family Services Statewide Agreement	DHHS Privacy Policy FERIS Privacy Statement Child Protection - Privacy Statements and Operating Manual Privacy Statement for members of Child Protection High Risk Panels (3066)		Undertaking a national police history check (1502) CSOs undertaking a national police history check (1505) Privacy-Breach-Checklist Breaches of Privacy (3063) DHHS Threshold Privacy Assessment Template	Client Relationship Information System (CRIS) Privacy Guidelines Privacy in Child Protection: Legislation and implications for practice DHHS Factsheet Appropriate Access to Personal Information DHHS Factsheet Collecting and Managing Employee Information DHHS Privacy Impact Assessment Guide DHHS Privacy factsheet - Executive officers DHHS Guide to effectively responding to privacy incidents DHHS team talk: effectively managing Privacy and Information Sharing Privacy training slides Factsheet: Developing a Privacy Collection Statement Use of Private information in Court Reports (2225) Freedom of Information (FOI) (3064) Information Sharing (3061) Information sharing in OOHC (3065) Factsheet on deeds of confidentiality Factsheet on disclosing health information Service Agreement Information Kit for Funded Organisations - Privacy and Data Protection

	STRATEGY / FRAMEWORK	PRINCIPLES	POLICY / STATEMENT	STANDARDS	PROCEDURES	GUIDELINES / FACT SHEET
SECURITY	Information Security Framework Information Security Management Framework ICCMS - Security Access Framework Identity and Access Management Framework Information Security Risk Management Framework 3rd Party Information Security Framework Portable Storage Framework HiiP Security Access Framework	Information Security Principles (within Information Security Management Framework)	Information Security Classification and Policy and Standards Information Security Maintenance Policy Information Security Management Policy Mobile Communications and Portable Storage Device Policy Information Security Incident Management Policy Acceptable use of departments technology	Security Requirements for RFT or RFQ Protected Information Security Incident Management Standard	CRIS, CRISSP, FERIS, HiiP Security Access Criteria - Process Map CenITex Operations Security Report Cyber Security Incident Management Plan Information security (3062) Access by External Auditors Identity and Access Management Implementation Plan Security Requirements for RFT or RFQ	Information Security Classification Factsheet Information Security Event and Incident Management (ISEIM) Process and Guidelines Cyber Security Guidelines - Sec Op Proc. Incident response Child Protection and your personal information for professionals Client Incident Report - How to Complete Client Incident Management System - Summary Guide

	STRATEGY / FRAMEWORK	PRINCIPLES	POLICY / STATEMENT	STANDARDS	PROCEDURES	GUIDELINES / FACT SHEET
DATA QUALITY	DHHS Data Quality Framework		Data Quality Policy Data Quality Statement		Data Quality Standard Operating Procedures (in progress)	Data Quality Assessment Tool
DATA ACCESS AND RELEASE			Data Access and Release Policy		Data Access and Release Standard Operating Procedures	Data Access and Release Guidelines
RISK	DHHS Risk Management Policy and Framework Funded Organisation Performance Monitoring Framework (FOPMF) Strategic Risk Profile			DHS Risk Register - Final version	Risk Treatment Plan	Client Incident Management Instruction Guide and Roles and Responsibilities Divisional Common Risks Client Incident Management (CIMs) Internal Roles and Responsibilities Guide Service Agreement Checklist Guidelines Guidelines for the Service Agreement Compliance certification (SACC) Form Service Agreement Information Kit for Funded Organisations

Appendix B – Audits and Reviews Considered

	REPORT CITATION
1	Leatherland, John, Review of Child Protection Privacy Incidents and Carer and Client Safety for Department of Health and Human Services, August 2016.
2	A professional services firm, Review of Kinship Care Model – Department of Health and Human Services Final Report, June 2016.
3	A professional services firm, Department of Health and Human Services – Internal Audit Report – Information Security and Management, April 2015.
4	A professional services firm, Department of Health and Human Services – Internal Audit Report – CRIS Review, February 2015.
5	A professional services firm, Department of Health and Human Services – Internal Audit Report – Application of Information Privacy Principles, July 2015.
6	Victorian Auditor General's Office (VAGO), Follow up of Residential Care Services for Children, June 2016
7	Victorian Auditor General's Office (VAGO), Early Intervention Services for Vulnerable Children and Families, May 2015
8	Ombudsman Victoria, Own motion Investigation into the Department of Human Services Child protection Program, November 2009
9	Ombudsman Victoria, Own Investigation into Child Protection – out of home care, November 2010
10	Victorian Auditor General's Office (VAGO), Access to Public Information, December 2015
11	Victorian Auditor General's Office (VAGO), WoVG Information Security Management Framework, November 2013
12	Victorian Auditor General's Office (VAGO), Residential Care Services for Children, March 2014
13	KPMG, Internal Penetration Test Department of Health and Human Services, May 2016

Appendix C – VPDSF Principles and VPDSS

The Victorian Protective Data Security Framework (VPDSF) Principles outline the underlying concepts that support the general themes of the VPDSF. These Principles of the framework are intended to enable Victorian government entities to evaluate its current and prospective security practices:

VICTORIAN PROTECTIVE DATA SECURITY FRAMEWORK (VPDSF) PRINCIPLES	
Principle 1: Governance	Strong governance arrangements ensure the protective data security requirements of the business are reflected in organisational planning.
Principle 2: Risk Management	Risk management empowers organisations to make informed decisions and prioritise security efforts.
Principle 3: Information Value	Understanding information value informs an organisation's application of security measures to protect public sector data.
Principle 4: Security Culture	A positive security culture with clear personal accountability and a mature understanding of managing risk, responsibility and reputation allows an organisation to function effectively and support the delivery of government services.
Principle 5: Continuous Improvement	A continuous improvement lifecycle model enables an organisation to systematically identify opportunities to mature their protective data security practices.
Principle 6: Business Objectives	Sound protective data security practices enable an organisation to achieve its business objectives in an efficient, effective and economic manner.

The Victorian Protective Data Security Standards (VPDSS) form part of the Victorian Protective Data Security Framework (VPDSF) and establish 18 mandatory requirements to protect data security across the Victorian public sector. The purpose of the VPDSS is to provide a set of criteria for the consistent application of risk-managed security practices across Victorian government information. The 18 standards are presented across governance and the four security domains, and feature core messages of what needs to be to be achieved. The VPDSS includes the following:

VICTORIAN PROTECTIVE DATA SECURITY STANDARDS (VPDSS)		
Security Governance Executive sponsorship of and investment in security management, utilising a risk based approach	Standard 1 – Security Management Framework	To ensure security governance arrangements are clearly established, articulated, supported and promoted across the organisation and to enable the management of security risks to public sector data.
	Standard 2 – Security Risk Management	To ensure public sector data is protected through the identification and effective management of security risks across the core security domains.
	Standard 3 – Security Policy and Procedures	To set clear strategic direction for the protection of public sector data.
	Standard 4 – Information Access	To ensure access to public sector data is authorised and controlled across the core security domains.
	Standard 5 – Security Obligations	To ensure all persons with access to public sector data understand their security obligations.
	Standard 6 – Security Training and Awareness	To create and maintain a strong security culture that ensures that all persons understand the importance of security across the core security domains and their obligations to protect public sector data.
	Standard 7 – Security Incident Management	To ensure a consistent approach to the management of security incidents, allowing timely corrective action to be taken for the protection of public sector data.
	Standard 8 – Business Continuity Management	To enhance an organisation's capability to prevent, prepare, respond, manage and recover from any event that affects the confidentiality, integrity and availability of public sector data.
	Standard 9 – Contracted Service Providers	To ensure the protection of public sector data across the core security domains, through the appropriate inclusion of the VPDSS in any contracted service provider arrangements.
	Standard 10 – Government Services	To provide assurance that the organisation's public sector data is protected when they receive a government service from another organisation.
	Standard 11 – Security Plans	To ensure that an organisation treats identified risks through informed business decisions, while applying cost-effective security controls to protect public sector data.

VICTORIAN PROTECTIVE DATA SECURITY STANDARDS (VPDSS)		
	Standard 12 – Compliance	To promote the organisation’s security capability and ensure adequate tracking of its compliance with the VPDSS.
Information Security Protection of information, regardless of media or format (hard and soft copy material), across the information lifecycle from when it is created to when it is disposed	Standard 13 – Information Value	To ensure an organisation uses consistent valuation criteria to assess public sector data that informs the appropriate controls for the protection of this information, across the core security domains.
	Standard 14 – Information Management	To ensure the organisation’s public sector data is protected across all stages of its lifecycle
	Standard 15 – Information Sharing	To prevent unauthorised access of the organisation’s public sector data, through the application of secure information sharing practices.
Personnel Security Engagement and employment of eligible and suitable people to access information	Standard 16 – Personal Lifecycle	To ensure a secure environment by actively managing all persons continued suitability and eligibility to access the organisation’s public sector data.
ICT Security Secure communications and technology systems processing or storing information	Standard 17 – Information Communications Technology (ICT) Lifecycle	To ensure the organisation’s public sector data is protected through the use of ICT security controls.
Physical Security Secure physical environment (i.e. facilities, equipment and services) and the application of physical security measures to protect information	Standard 18 – Physical Lifecycle	To maintain a secure environment where the organisation’s public sector data is protected through physical security measures (facilities, equipment and services).

Appendix D – Stakeholders Engaged

ROLE/POSITION	TEAM
Director	Executive Services and Oversight
Assistant Director	Executive Services and Oversight
Chief Information Officer	Business Technology & Information Management
Assistant Director, Strategy and Design	Business Technology & Information Management
Assistant Director Service Delivery	Business Technology & Information Management
Director, Budget, Strategy and Corporate Planning	Corporate Services
Assistant Director, Safeguarding and disability Supports	Safeguarding and Community Services
Director	Procurement and Contract Management
Assistant Director	Centre for Learning and Development
Director Client Outcomes and Service Improvement	Operations
Director Health and Human Services Regulation and Review	Operations

This page is intentionally left blank.

Commissioner
for Privacy and
Data Protection

VICTORIA
State
Government