ibac independent broad-based anti-corruption commission
Victoria

Unauthorised access and disclosure of information held by the Victorian public sector

An analysis of corruption risks and prevention opportunities

February 2020

Authorised and published by the
Independent Broad-based Anti-corruption Commission,
Level 1, 459 Collins Street, Melbourne.

February 2020

If you need this information in an accessible format,
please call 1300 735 135 or email
communications@ibac.vic.gov.au.

This document may also be found in formats on our
website www.ibac.vic.gov.au

ISBN 978-1-922349-02-6 (print)

ISBN 978-1-922349-02-6 (online)

Contents

Definitions

Terms	Explanation/Expanded abbreviation
CMS	Case management system
CPDP	The Commissioner for Privacy and Data Protection. In 2017, amendments made to the *Privacy and Data Protection Act 2014* merged the Offices of CPDP and the Freedom of Information Commissioner into the Office of the Victorian Information Commissioner.
DHHS	Department of Health and Human Services
DJR	The Department of Justice and Regulation. After machinery of government changes, it was renamed the Department of Justice and Community Safety in January 2019.
DPC	Department of Premier and Cabinet
DTF	Department of Treasury and Finance
IPP	Information Privacy Principles
IT	Information technology
MoU	Memorandum of understanding
NSW ICAC	New South Wales Independent Commission Against Corruption
OCG	Organised crime group
Official information	Any information (including personal information) obtained, generated, received or held by or for a Victorian public sector organisation for an official purpose or supporting official activities. This includes both hard and soft copy information, regardless of media or format.
OVIC	Office of the Victorian Information Commissioner
PDP	Privacy and Data Protection (OVIC)
PROV	Public Record Office Victoria
Public sector agencies	All organisations that comprise the Victorian public sector (including both the public service and public entities)
QLD CCC	Queensland Crime and Corruption Commission
SLEDS	Standards of Law Enforcement Data Security
VAGO	Victorian Auditor-General's Office
Victorian public sector (public sector)	All public bodies, including state government agencies and local councils
VO	Victorian Ombudsman
VPDSF	Victorian Protective Data Security Framework
VPDSS	Victorian Protective Data Security Standards
VPS	Victorian public service

1 Overview

Public sector agencies manage a wide range of information. This includes personal health records and contact details as well as sensitive political and economic information and financial data. The appropriate handling and security of this information is imperative. Unauthorised access and disclosure of data and information undermines the credibility of the public sector and jeopardises trust in government agencies to responsibly manage public information and ensure personal information is managed carefully and securely.

This report provides an overview of the key risks associated with unauthorised access and disclosure of information by Victorian public sector employees. It explores the drivers of these risks, as well as potential prevention, reporting and detection measures. This report is one of three, outlining the key risks of unauthorised access and disclosure of information applicable across the public sector in Victoria. The other two reports focus on risks specific to local government and Victoria Police.

This report discusses how the misuse of information or material by public officers, acquired in the course of the performance of their duties, may constitute corrupt conduct.

Accountability, trust and transparency in how public sector agencies protect and manage information, in particular official information, is essential for good governance and for the effective working of the public sector. Any incident, or series of incidents, which undermine the public's confidence in the public sector's ability to secure official information is likely to have flow-on effects to the willingness of the public to provide information that assists public sector agencies in fulfilling their purpose.

Information held by public sector agencies can be misused intentionally or unintentionally. The consequences of unauthorised use of data can include serious threats to the safety of individual citizens and the broader community. It may also lead to government funded projects and contracts costing more due to corrupted procurement processes, reducing public funds available for other public services. It may also cause the community to be less willing to share information with the public sector, in turn impacting research and the delivery of services.

IBAC works to inform the public sector and community about the risks and impacts of corruption, and how it can be prevented. IBAC's intelligence and research reports assist public sector agencies to identify corruption, and to expose and prevent it.

This report was informed by an analysis of IBAC findings from investigations and research, consultation with public sector agencies, Victoria Police, interstate and Commonwealth integrity bodies, and key agencies responsible for information management and privacy in Victoria.

The unauthorised access and disclosure of information is a consistent theme across investigations of corruption in Australia. IBAC's previous strategic assessments and public reports have identified it remains a key issue for public sector agencies in Victoria holding security classified or sensitive information such as Corrections Victoria[1] and Victoria Police[2]. Police, custody and correctional officers have access to official information, often of a personal or confidential nature, so it is not surprising a large proportion of investigations and assessments undertaken by IBAC and partner agencies focuses on these sectors.

Although the policing and corrections sectors face heightened risks, information misuse is a corruption risk across the entire Victorian public sector, especially in sectors that have employees with high levels of access to information (such as system administrators or IT specialists) or in sectors with high financial benefits to be gained from corruption (such as planning or major projects).

Public sector agencies may also be at higher risk of information misuse due to the large size of their information holdings. An example of this is public hospitals where employees may have access to a range of personal health records as well as personal financial and insurance information. Employees could be targeted for access to this information which could then be used to commit fraud.

An increased reliance on technology by public sector agencies and by the community has introduced different risks for how data is secured. The public sector has increasingly moved to storing information electronically, communicating via email, capturing evidence via photographs as well as using data analytics to help decide how resources are used.

This increased reliance upon technology for work and personal use has resulted in increased efficiency but has also raised the risk of public sector employees easily copying or replicating data for circulation. While technology has benefited the work of the public sector overall, it has also made it 'very easy to disclose information – in terms of time, quantity and sensitivity – and difficult, if not impossible, to retrieve it'[3] once disclosed.

The risks of physical and verbal information security breaches should not be underestimated by public sector agencies, with incidents identified by IBAC (and partner agencies) often resulting from a failure of a range of information security and corruption controls.

IBAC's complaint data and intelligence suggest information misuse is still widely misunderstood by both the public sector and the community. It is therefore likely it is often not detected or reported when it does occur. More education is needed across the Victorian public sector about how information misuse may constitute corrupt conduct as well as related corruption risks, and prevention and detection strategies.

[1] IBAC, *Corruption risks associated with the corrections sector*, November 2017.

[2] IBAC, *Special report concerning police oversight*, August 2015.

[3] Commissioner for Law Enforcement Data and Security, *Social Media and Law Enforcement*, July 2013, p 44.

1.1 Key findings

- Unauthorised access and disclosure of information are key enablers of other corrupt behaviour and are often rated as low risk by agencies. This is evident in lower than expected numbers of reports to IBAC and in the behaviours uncovered in investigations undertaken by IBAC and other public sector agencies. The increased understanding of information misuse as an enabler of corruption will help the detection and investigation efforts by public sector agencies.
- IBAC intelligence suggests information misuse is under-reported across the entire public sector. This may be due to a lack of detection, an under-appreciation for information security and privacy rights of complainants, or a lack of awareness that information misuse and disclosure may constitute an offence in itself.
- IBAC and Victorian public sector agencies often do not detect information misuse until they are investigating other misconduct or corrupt actions. This is partly due to information security systems which have not been fully developed, and a lack of processes to either detect unauthorised information access in isolation or flag that it has occurred.
- Unauthorised disclosures to the media is a risk across public sector agencies. These incidents are difficult to substantiate due to the source of the information leaks often being challenging to identify.
- Sharing information with approved third parties also presents corruption risks. This is partly driven by the confusion created by the complex legislative, administrative and regulatory environment governing information sharing. Although policies may be in place to control information access and disclosure by third parties, the proactive detection and enforcement of information misuse by agencies owning the information is difficult.
- Increased use of personal devices and smartphones in the workplace has made unauthorised disclosure of information much easier. The level of maturity in how public sector agencies deal with this increased risk is extremely varied.
- Unauthorised information access and disclosure is a key risk in procurement. Greater awareness and implementation of best practice, and reporting procurement suspected to be corrupted due to information misuse to IBAC, could mitigate this risk.
- Customised auditing of information access is under-used and its benefits are under-appreciated across the Victorian public sector. A program of proactive, extensive and repeated auditing could be used to identify and deter unauthorised access of information.
- The introduction in 2016 of the Victorian Protective Data Security Framework (VPSDF) across the public sector is expected to reduce the incidents of unauthorised information access and disclosure over the longer term. However, it is initially expected that as awareness of information security increases, so will the number of the reports of information security incidents. The strength of the influence by the Victorian Protective Data Security Standards (VPDSS) on longer term cultural change will depend on how successfully public sector agencies implement the framework and align their practices.

1.2 Methodology

1.2.1 Scope

This report considered corruption risks related to information misuse across IBAC's jurisdiction of the Victorian public sector.

Under the *Independent Broad-based Anti-corruption Commission Act 2011* (the IBAC Act), IBAC may investigate and take complaints about corruption across the public sector, local councils, police, parliament and the judiciary in Victoria.

This report does not consider the unintentional misuse of information, as this is unlikely to engage IBAC's jurisdiction and amount to corrupt conduct.

IS UNAUTHORISED ACCESS AND DISCLOSURE OF INFORMATION AND DATA CORRUPT?

The IBAC Act defines corrupt conduct (among other things) as conduct of a public officer that involves the misuse of information or material acquired in the course of the performance of their functions, being conduct that would constitute a 'relevant offence'.[4]

Unauthorised access and disclosure of information by employees of public sector agencies can be considered corrupt conduct under the IBAC Act definition of corrupt conduct, depending on the circumstances and details of access or disclosure.

CAN YOU MAKE AN UNAUTHORISED DISCLOSURE OF INFORMATION WHEN REPORTING SUSPECTED CORRUPTION TO IBAC?

Under the *Public Interest Disclosure Act 2012*, a person may make information disclosures to IBAC, an investigating entity or the public sector agency in question about employees of that entity if the information shows or tends to show the subject officer is engaging, has engaged, or is proposing to engage in improper conduct or detrimental action.[5]

The Office of the Victorian Information Commissioner (OVIC) defines information management as the way in which an organisation plans, identifies, creates, receives, collects, organises, governs, secures, uses, controls, disseminates, exchanges, maintains, preserves, and disposes of its information.[6] Good information management promotes good information security and assists in deterring unauthorised access and disclosure of information. This report also looks to other stages of the information management cycle where it is relevant to unauthorised access and disclosure of information held by public sector agencies in Victoria.

Information misuse by private organisations or public sector employees outside Victoria is excluded from this report. However, case studies from other Australian jurisdictions are highlighted to provide examples of key vulnerabilities and risks which may be relevant to Victoria.

This report acknowledges employees are allowed to disclose information without permission in certain circumstances, particularly when reporting police misconduct or corrupt conduct to IBAC, Victoria Police or another investigating entity. These public interest disclosures (sometimes referred to as whistleblowing) are assessable for protections under the *Public Interest Disclosure Act 2012.*

[4] IBAC Act section 4(1) (d). Relevant offence means an indictable offence against an Act or the common law offences committed in Victoria for: attempt to pervert the course of justice; bribery of a public official; perverting the course of justice; or misconduct in public office.

[5] Detrimental action refers to actions or incitements causing injury; intimidation; or adversely treating an individual in relation to their career in reprisal for making a disclosure or cooperating with an investigation in relation to a disclosure under the *Public Interest Disclosure Act 2012*.

[6] Commissioner for Privacy and Data Protection, *Glossary of Protective Data Security Terms'*, 2016.

1.2.2 Terminology

IBAC receives complaints from the public and notifications from public sector agencies. A complaint or notification may include multiple allegations, all of which are individually assessed. This report includes summaries of allegations received by IBAC as a means to illustrate some key points.

IBAC notes there are limitations with the use of these examples, including:

- allegations are unsubstantiated at the time of receipt
- allegations can be incomplete, lack detail, from an anonymous source or may not individually name the subject of the allegation
- allegation data is not a comprehensive or a reliable indicator of the actual prevalence of particular activities, or the risk mitigation practices and compliance activities already in place.

Despite these limitations, the analysis of allegations can assist in identifying trends or patterns and provide practical examples of identified trends.

This report also refers to a number of terms that are defined in the *Privacy and Data Protection Act 2014*, including 'personal information', 'sensitive information' and 'law enforcement data'. For clarity, these terms are used within the report in their ordinary sense, unless otherwise stated.

This report often refers to unauthorised access and disclosure of information as 'misuse of information'.

2 Context

The unauthorised access or disclosure of information held by public sector agencies can have wide ranging and long lasting adverse effects on the agency targeted, and on its employees. It can also affect the privacy and safety of citizens and therefore the community confidence in the security of information held by the public sector.

Accountability, trust and transparency in how public sector agencies protect and manage information, in particular official information, is essential for good governance and for the effective working of the public sector. Any incident, or series of incidents, which undermine the public's confidence in the public sector's ability to secure official information is likely to have flow-on effects to the willingness of the public to provide information that assists public sector agencies in fulfilling their purpose.

Different legislative requirements impose different information management and information security conditions, based both on the type of information held or accessed, and the way that it is used. This adds to the complexity within which the public sector is expected to interact with and protect official information.

Information misuse can have negative financial consequences for public sector agencies and the broader Victorian community. This includes information leaks to suppliers during procurement, which can lead to less competition in future procurement processes. In an IBAC survey of suppliers to state and local government in Victoria, approximately one-third of respondents stated they were discouraged from tendering for work due to concerns about corruption.[7] This may be influenced by a perception the tender has been won before the process has been completed.

In 2017/18, the public sector spent a total of $3.011 billion on procurement contracts for purchasing goods and services from the private sector.[8] This amount increases when government investment in major projects, infrastructure, and procurement related to construction and health related goods and services are included.[9] Given the value of the procurement undertaken by the public sector, information misuse during the tender process could have serious financial consequences for the public sector and the community.

Information misuse can assist organised crime and encourage further offending. The Australian Criminal Intelligence Commission has highlighted public sector corruption, including information misuse, as a key enabler for organised crime.[10] IBAC has previously explored the issue of public sector employees providing information to organised crime entities.[11] Information leaks by public sector employees to organised crime groups is serious and warrants ongoing scrutiny, including continual auditing, training and guidance for employees.

IBAC's investigations have consistently identified information misuse as a key element in corruption, even when unauthorised information access or disclosure was not initially reported or suspected. An analysis of IBAC's investigations across the public sector in Victoria showed approximately 60 per cent of all investigations have included information misuse issues, although this may have not been the original allegation investigated.

[7] IBAC conducted a survey of Victorian suppliers to state and local government in 2015–16, which found 38 per cent of respondents believed it was typical or very typical for public sector officials to give suppliers unequal access to tender information. IBAC, *Perceptions of corruption: Survey of Victorian Government suppliers*, 2016, p 2.

[8] Victorian Government Purchasing Board, *Annual Report 2017–18*, p 17.

[9] Victorian Government Purchasing Board, *Suppliers*, 6 February 2019.

[10] Australian Criminal Intelligence Commission, *Organised Crime in Australia 2017*, August 2017.

[11] IBAC, *Organised crime cultivation of public sector employees*, September 2015.

2.1 The legislative framework for information management in the Victorian public sector

Information management for the public sector and its employees in Victoria is complex, and depending on the type and context of information held, can be difficult to navigate.

Victoria has a large legislative framework and governance around information management within the public sector in Victoria. This framework covers legislation including, but not limited to the:

- standards for responsible management of information, as outlined in the *Privacy and Data Protection Act 2014*, from capture and creation of information through to disposal
- standards of keeping records in the *Public Records Act 1973*
- right to privacy in the *Charter of Human Rights and Responsibilities Act 2006*.

Most employees of the Victorian public service (VPS) are employed under the *Public Administration Act 2004*, which defines misconduct, among other things, as 'an employee making improper use of information acquired by him or her by virtue of his or her position to gain personally or for anyone else financial or other benefits or to cause detriment to the public service or public sector'. In addition, legislation exists related to information management by specific public sector agencies, making the issue complex and likely difficult for some public sector employees to navigate.

OVIC is an independent regulator with combined oversight of information access, information privacy, and data protection. OVIC administers the Victorian Protective Data Security Framework (VPDSF)[12], which applies to the majority of agencies and bodies across the Victorian public sector. OVIC is also responsible for:

- monitoring and ensuring compliance with the Information Privacy Principles (IPP), which set out minimum standards for how Victorian public sector bodies should handle personal information
- providing an alternative dispute resolution service for individual privacy complaints, which may be referred to the Victorian Civil and Administrative Tribunal for determination
- investigating, reviewing and auditing compliance with the VPDSF and IPP.[13]

Other avenues for reporting misuse of information include Victoria Police, IBAC, the Victorian Ombudsman, or reporting directly to the agency which held the information thought to have been misused.

The Public Record Office Victoria (PROV) is responsible for issuing information management standards, and assisting agencies in being compliant with the *Public Records Act 1973*. Strong frameworks for management of information, including governance, life cycle, business systems and processes, are essential to good information management processes;[14] however, they may not fully prevent information misuse from occurring.

As well as the references to information misuse in the IBAC Act, the unauthorised access and disclosure of information is referred to in other legislation in Victoria. *The Crimes Act 1958* lists relevant summary offences under section 247G regarding unauthorised access to or modification of restricted data. Public sector agencies must also manage specific types of information as required by legislation (for example, the *Health Records Act 2001* or enabling legislation specific to the public sector agency which owns the information).

[12] The VPDSF is the overall scheme for managing protective data security risks in Victoria's public sector. The previous Standards for Law Enforcement Data Security (SLEDS) were incorporated in the Victorian Protective Data Security Standards (VPDSS) which is part of the VPDSF. For more information, visit www.ovic.gov.au

[13] Office of the Victorian Information Commissioner, *Short guide to the Information Privacy Principles*, 2018.

[14] Public Record Office Victoria, *Recordkeeping for government: Getting started*, updated 27 June 2018.

2.2 Previous reviews of information management

In 2015/16, PROV reviewed the level of maturity in information management across the public sector and found the auditing of, and compliance with information management was the key weakness experienced by all departments and agencies. Five of the then seven departments participated, along with four key government agencies, and the review was based on a self-assessment conducted by the agencies.[15] Weaknesses in information management systems and practices almost certainly increase the number of information security incidents, including those involving corrupt conduct not being detected and reported to the relevant departments, integrity bodies and the police.

The Victorian Auditor-General's Office (VAGO) completed an audit, *Managing Public Records*, in early 2017. This audit examined both the information technology systems and the supporting processes and practices of PROV, the Department of Education and Training (DET) and the Department of Health and Human Services (DHHS). It found further reform of information management and agency tools is needed 'as longstanding weaknesses in Victoria's regulatory framework remain. These weaknesses – in particular the absence of system-wide compliance monitoring and reporting and out-dated legislation – heighten the risk of key public sector records being lost, inaccessible, inappropriately accessed or unlawfully altered or destroyed.'[16]

VAGO found the two agencies examined in the audit lacked controls on third-party information access, and had insufficient compliance monitoring processes. It is possible other departments and public sector agencies have similar weaknesses, resulting in increased risks for unauthorised information access and disclosure.

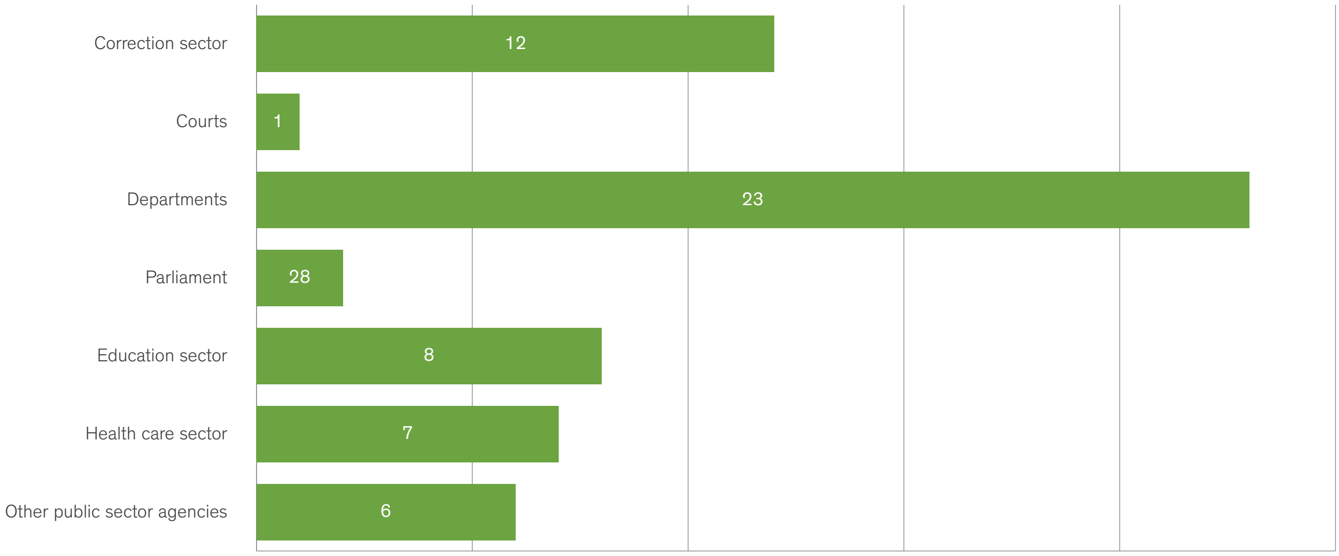
2.3 Allegation trends

The analysis of IBAC's complaints and notifications data found complainants often do not allege unauthorised access and release of information, even where this activity enabled probable misconduct or corruption to occur. This highlights a significant under-reporting of information misuse, and that while allegations provide an insight into reporting, IBAC's data is unlikely to reflect the actual level of information misuse that is occurring. Training and education is needed to raise awareness around the identification, detection, prevention and reporting of information misuse.

[15] Public Record Office Victoria, *Information Management Maturity Current State Assessment 2015–16*, 16 November 2016.

[16] Victorian Auditor-General's Office, *Managing Public Sector Records*, 8 March 2017, p xi.

FIGURE 1 – ALLEGATIONS TO IBAC OF UNAUTHORISED INFORMATION ACCESS AND DISCLOSURE (1 JUNE 2013 TO 30 JUNE 2018)[17]



The allegations data in Figure 1 shows IBAC has received a very low number of allegations regarding information misuse against Victorian public sector agencies. Due to the low number of allegations, it is difficult to identify trends or patterns in the allegations.

Of note, Figure 1 does not include instances of information misuse by Victoria Police employees, as this is considerably higher than the rest of the public sector. There are several potential contributing factors – in particular, the fact that Victoria Police makes a high number of mandatory notifications to IBAC regarding information misuse indicates it has a strong information security framework that recognises when a breach occurs. Another reason is the greater awareness, both within the community and Victoria Police, of the large amount of personal, criminal and sensitive information the agency holds.

The public sector and the community often find it difficult to recognise information misuse and therefore report it as corrupt behaviour, especially when this behaviour has enabled other alleged offending – such as bribery, fraud or collusion. Increased education on how information misuse may constitute corrupt conduct, enable further corruption and how it impacts citizens' privacy, as well as the efficiency and functioning of the public sector, could strengthen reporting of information misuse.

Under-reporting of information misuse is also likely the result of both members of the public and public sector agencies being unaware of when their information has been misused or shared. For instance, unauthorised information access may not be detected, and unauthorised disclosures may not become public or be reported to the individuals or the agencies affected.

[17] The sectors do not include complaints about the portfolio department – these are included in allegations against the category of 'Departments'. Other public sector agencies range from statutory authorities, regulators, public boards etc. This graph does not include allegations against Victoria Police, local government organisations or their employees, which are published in separate reports.

3 Corruption risks for unauthorised information access and disclosure

Investigations by IBAC, policing and partner agencies indicate that the misuse of official information is often an enabling crime for further misconduct or corrupt conduct. Through consultations with partner integrity agencies, IBAC found information security to be a consistent misconduct and corruption issue for public sector agencies, with some agencies highlighting concerns regarding how to best identify and manage corruption risks associated with the information they hold.

3.1 Information released to benefit associates

Unauthorised information disclosure to associates is a common theme across IBAC investigations and is often an enabler of corrupt conduct. As highlighted in Case Studies 1 and 2, many public employees have access to large databases of information which can easily be used inappropriately. In IBAC investigations, bribery and kickbacks do not appear to be a motivation for unauthorised information release – rather it is more commonly seen to occur as either a favour or an act of goodwill.

CASE STUDY 1 – IBAC OPERATION BARRON
LOOKING UP PEOPLE ON THE SYSTEM TO HELP OUT AN ASSOCIATE

In 2016, IBAC received intelligence to suggest a VicRoads employee was unlawfully accessing and altering registration and licensing details of numerous members of the community, and disclosing this information to associates. IBAC commenced Operation Barron to investigate these allegations.

The investigation focused on the actions of the Team Leader of the Registration and Licensing Support Team (the team leader). The team leader had worked at VicRoads since 2009 performing various customer service roles before transferring to the team leader role in 2014. In this role, the team leader had no direct interaction with members of the public, and instead supervised a team that was responsible for resolving customer enquiries referred from other VicRoads business areas, or public enquiries received by email or post. The team leader had full access and capability to edit data held within the VicRoads registration and licensing systems.

The investigation found evidence the team leader had misused the VicRoads systems; however, the number of exact occasions this occurred was unable to be determined due to their high use of the system over a considerable period of time. For example, one audit of their access showed they had accessed VicRoads records on approximately 18,000 occasions within a two-year period. Of note, the team leader's father had strong links to people involved in organised crime. One of these associates used private VicRoads registration and licensing information obtained through the team leader to locate a person that consequently reported to police instances of criminal damage to their property and threats from organised crime group (OCG) members.

VicRoads cooperated with the IBAC investigation and the team leader was suspended from their position in early 2017, and resigned from VicRoads while under investigation. The team leader confirmed known examples of their unauthorised access, alteration and disclosure of VicRoads registration and licensing information.

In addition, the team leader made admissions to sharing their systems access password and provided additional examples of occasions when they had used their VicRoads system access for unauthorised purposes.

IBAC charged the team leader with the following criminal offences:

- three counts of misconduct in public office for wilfully accessing and disclosing VicRoads information without authorisation
- one count of misconduct in public office for wilfully accessing and modifying VicRoads data without authorisation associated with the roadworthiness of a vehicle
- one count of corrupt modification of data to cause impairment, associated with the roadworthiness of a vehicle contrary to Section 247C of the *Crimes Act 1958*
- one count of corrupt access to restricted data, associated with the roadworthiness of a vehicle contrary to Section 247G of the *Crimes Act 1958*.

The team leader pleaded guilty to four separate charges of misconduct in public office, and the two summary offences of corrupt access to restricted data were withdrawn. The team leader was convicted and sentenced to a two-year community corrections order requiring them to complete 200 hours of unpaid community work.

IBAC found no evidence the team leader acted for personal financial gain; however, some of their checks benefited friends by saving them time and money by not following proper processes. Additionally, certain unauthorised checks benefited a close associate who was able to be seen as doing favours for others.

In response to Operation Barron, VicRoads reviewed and updated its information systems as well as the associated education and training to further strengthen the organisation against the corruption vulnerabilities identified.

CASE STUDY 2 – IBAC OPERATION CAPARRA
A CORRECTIONS VICTORIA EMPLOYEE LOOKING UP PRISONER DETAILS

In March 2018, the former Department of Justice and Regulation (DJR) informed IBAC of allegations against a Corrections Victoria employee. The allegations included that the employee had failed to disclose declarable associations with current and former inmates of facilities managed by Corrections Victoria. It was also alleged this employee had accessed information on eight individuals via the Department's prisoner database without a valid reason. After this behaviour was identified, the employee was suspended from duty.

IBAC commenced an investigation into the allegations in April 2018.

The employee had commenced their role as a Justice Property Officer with Corrections Victoria in December 2017, and in being appointed to the role they declared they were not related to or associated with anyone currently or previously held in correctional facilities in Australia.

IBAC's investigation determined the employee:

- failed to declare associations with current and former inmates in Victorian correctional facilities and their connections to criminal entities
- accessed restricted information on numerous occasions, outside the scope of their official duties, for at least 13 individuals known to them or their partner, using two different computer systems.

The employee admitted to these actions, stating to IBAC they did not fully understand their obligations under Corrections Victoria policies at the time they were working as a property officer.

IBAC found the employee's mobile phone number was already listed in Corrections Victoria systems on phone lists for two prisoners.

IBAC referred the information detailing the extent of the employee's identified misconduct back to Corrections Victoria for appropriate disciplinary action.

IBAC understands Corrections Victoria has since expanded its pre-employment probity checks.

IBAC has received a number of complaints and information from the public with similar circumstances to the original allegations described in Case Studies 1 and 2. This includes a report made to IBAC that alleged a private sector employee frequently asked a family member employed in a public sector agency to access official information on their behalf – namely phone numbers or addresses of people they '[needed] to find'. Requests of this nature might occur over a long period of time before they are detected. This is especially the case if the public sector employee is in a role that requires frequent data access. These examples also highlight how easy it can be for public sector employees to inappropriately become a regular source of official information for friends and family.

The Department of Health and Human Services (DHHS) experienced a number of information breaches in child protection cases throughout 2015 and 2016, which were well publicised. These include cases where the location of children living in care were accidentally disclosed. These cases led to DHHS commissioning an independent review of the specific incidents, as well as carer and client safety.[18] The review focused on 61 incidents over five years, with 58 of these substantiated as information breaches. All but one of these incidents were due to human error, including failures to redact personal identifying information and addresses from documents being filed in the Children's Court. The review noted 40 of the incidents were where information became available to third parties that could have been expected to place children or their caregivers at direct risk of harm. This warranted both a change in information security practices by employees and in child protection information management systems.

DHHS accepted the recommendations of the review, including the development of mandatory privacy training to increase employee awareness of privacy and confidentiality obligations, as well as a review of privacy issues detailed in employee manuals and policies. A further review of information governance and security was also conducted by the former Commissioner for Privacy and Data Protection in 2017.[19]

IBAC assesses information access and misuse within child protection settings as an area of high risk due to there being high incentives for members of the public being affected by a child protection case to seek unauthorised access to information.

Public sector departments and agencies that have lower levels of interaction with the public and also hold less personal information of the community (such as the Department of Treasury and Finance (DTF) and the Department of Premier and Cabinet (DPC)) still have corruption risks related to information holdings. These agencies may manage highly valuable information such as sensitive political, policy or economic information. Unauthorised information access and disclosure incidents in these areas may have significant political and financial consequences. DPC in particular has been previously found by VAGO to have gaps in information management; however, VAGO has noted DPC is improving its information security.[20]

[18] Leatherland, John, *Review of Child Protection Privacy Incidents and Carer and Client Safety for Department of Health and Human Services*, 'Final Report', 26 August 2016.

[19] Commissioner for Privacy and Data Protection, *Review of information governance in the Department of Health and Human Services*, 'Review conducted and report prepared by Pricewaterhouse Coopers', January 2017.

[20] Victorian Auditor-General's Office, *Managing Public Sector Records*, 8 March 2017.

3.2 Organised crime groups targeting public sector employees for information

It is well established that public sector corruption can be an enabler of organised crime, and the corrupt use of official information is one of the key ways this can occur. IBAC highlighted these risks in its 2015 intelligence report, *Organised crime group cultivation of public sector employees*, which found most public sector bodies hold information or commodities that are attractive to organised crime groups, and there was a general lack of awareness of this threat across the public sector.[21]

Internationally, there has been an increase in organised crime groups (OCGs) targeting health records of patients, as well as using health sector employees to leak official information. A global data breach report, which included case studies and data from Australia, found OCGs in possession of this data may use it for identity theft or to access online banking.[22] In one extreme case, an OCG was also able to use employees to corrupt systems and lock down files and then demand a ransom for the files to be released.[23]

IBAC's Operation Barron, discussed in Case Study 1, also highlights the pervasive nature of OCGs, and the way groups can infiltrate the public sector through a range of strong and weak associations. This is further illustrated in Case Study 3.

CASE STUDY 3 – IBAC OPERATION TOUCAN[24]

LOOKING UP INFORMATION AND POTENTIALLY PASSING IT ON TO ORGANISED CRIME

In early 2013, IBAC received information several Victorian public sector employees, working at different statutory bodies based in Shepparton, were providing official information to members of an OCG. While IBAC was unable to establish direct evidence of employees passing information to OCG members, IBAC was able to establish one employee's:

- proven links to one or more OCG members
- proven unauthorised or otherwise inappropriate access to some agency-held information
- failure to disclose declarable associations
- suspicious conduct regarding other issues in connection with the person's employment.

A newspaper article detailing a connected police investigation was released during Operation Toucan. After this article was published, IBAC noted the persons of interest changed their behaviour, suggesting the media reporting likely compromised this investigation by putting the persons of interest on alert.

[21] IBAC, *Organised crime group cultivation of public sector employees*, September 2015.

[22] Verizon Enterprise Solutions, *Verizon's 2017 Data Breach Investigations Report*, April 2017.

[23] Dunlevy, Sue, *Herald Sun*, "Pay up or we destroy your patients' health records': Cyber criminals hit hospitals', 27 April 2017.

[24] Previously published in IBAC, *Organised crime group cultivation of public sector employees*, September 2015.

3.3 Motivated release of information

In consultation with IBAC, public sector agencies have indicated a perceived increase in unauthorised information release motivated by individual beliefs. Significant political or social issues can create powerful motivators for employees to disclose information without authority. This is made more difficult to investigate when this information is leaked to the media and reaches the public arena, especially if the information disclosed was known to many employees. Official information can be easily disclosed to interested parties or political groups via social media, and this can assist in protecting the identity of the person disclosing the information.

Although not proven to be politically or ideologically motivated, Case Study 4 demonstrates the ease with which public sector employees can misuse information for a perceived cause. Motivated release of information is also particularly assisted by personal devices including smartphones, which make the photographing or copying of official information relatively easy to do, and more difficult to detect.

CASE STUDY 4 – AUSTRALIAN DEPARTMENT OF DEFENCE EMPLOYEE LEAKING INFORMATION ONLINE[25]

In 2012, a graduate recruit with the Department of Defence (who held a high-level security clearance – Negative Vetting Level 1) leaked security classified government information online. Approximately eight months into their employment, they downloaded a document classified SECRET, saved it to a compact disc, and took it home before posting two pages of material to an online forum.

The material posted on the forum by the recruit highlighted possible motivations for the offending; 'Julian Assange is my hero' and 'I release what I feel should be in the media: bombings, civilian deaths, actions of the 'terrorists' that just aren't reported in the media'. However in sentencing, the court accepted there had been no political, ideological or financial motive for the offending.[26]

The recruit's actions were discovered by a former Department of Defence employee who reported it, and the Australian Federal Police were able to track the internet protocol (IP) address of the original forum post by the offender. The police searched the premises, seized the personal computer and the broken disc which contained the security classified material that was found in the rubbish bin. Forensic analysis showed the recruit had used the computer to leak the material and had also searched for ways to hide their actions.

The recruit was sentenced to one year in prison.

[25] Knaus, Christopher and Michael Inman, *Canberra Times*, 'A junior Defence staffer allegedly took home an intelligence report and posted it online', 5 August 2015.

[26] Inman, Michael, *Canberra Times*, 'Canberra APS worker jailed for leaking 'top secret' documents', 6 November 2015.

3.4 Sharing of system login credentials

Unauthorised access of information also occurs when an employee uses another employee's login details to access information. IBAC intelligence suggests this is occurring more frequently in offices where desk sharing takes place, most commonly in regional areas or in offices undertaking field work. While the consequences of such action may be less serious, especially if the employee already has access to the same systems and information, it leaves public sector bodies vulnerable to being unable to detect and prosecute information misuse when it does occur.

IBAC intelligence suggests there is a fairly prevalent practice across the public sector of support staff, particularly executive assistants, using systems under executives' login details and passwords. This presents a number of risks, and creates difficulties in detecting unauthorised access or disclosure should it occur. An example of this is highlighted in Case Study 5.

CASE STUDY 5 – COMPROMISED AUTHORISATION PROCESSES

IBAC received an allegation from an executive assistant (the EA) at a metropolitan university. It was alleged a senior executive officer (the EO) had instructed the EA to perform authorisations by logging into the EO's account to approve workflow requests, financial transactions, travel requests, purchase orders and employee leave requests which only the EO had authority to approve. To do this, the EA had to use the EO's login and password.

The complaint alleged this was common practice at the university among senior executives and their EAs.

This case was referred to the university's vice-chancellor for investigation.

4 Drivers of corruption risks related to information access and disclosure

Public sector agencies manage many different types of information. Due to this, corruption risks vary across the different working environments of public sector agencies, and these risks have different drivers. By way of example, both Corrections Victoria and DHHS are more likely to handle sensitive personal information while the Department of Environment, Land, Water and Planning is more likely to handle sensitive planning information affecting business. IBAC believes public sector agencies are best placed to manage their own unique corruption drivers and risks.

Public sector agencies should regularly review their information assets and perform assessments to determine how to appropriately protect the information they hold. This would put the agencies in a position to critically consider how to manage information based on their size, resources and risks. OVIC designed the VPDSF Five Step Action Plan[27] to assist agencies in undertaking this.

4.1 High-level access by managers and information technology administrators

Compared to other employees, managers and supervisors often require a higher level of access to information systems to fulfil their management responsibilities. This can include access to confidential personal details in human resource, payroll and financial systems, as well as those more specific to their agency. This high-level access can drive unauthorised access to information, and as shown in Case Study 6, can lead to personal benefits.

CASE STUDY 6 – COMPLAINT TO IBAC OF MISUSE OF THE SHERIFF'S OFFICE DATABASE

In mid-2015, IBAC received an anonymous complaint alleging a supervisor within the Sherriff's Office was misusing their position. The allegations stated the supervisor and their domestic partner were the subject of numerous Sheriff's warrants, including through a company which had the supervisor listed as the Company Director. It was alleged the supervisor had accessed the Sheriff's Office database to check on the warrants and upon discovering their name listed against the warrant, removed themselves as the Company Director.

The anonymous complainant further alleged when the supervisor was confronted about their misuse of the database they denied it, and a complaint was made to the Regional Director, however no action had been taken against the supervisor.

IBAC referred the complaint to the former Department of Justice and Regulation (DJR). DJR responded to IBAC explaining the supervisor had been put on a performance management plan following the internal complaint to the Regional Director and the supervisor had later resigned.

Noting the corruption risks highlighted by this case, DJR rewrote their operations manual to minimise the risk of such offences occurring in future, and was committed to strengthening its audit capability and enforcement of policies and procedures.

[27] Office of the Victorian Information Commissioner, *Overview of the Framework and Five Step Action Plan*, 'Victorian Protective Data Security Framework', October 2018.

Employees working in information technology with high levels of access present higher risks related to information misuse. These employees often bring new skills and innovation to the public sector, and often work with a high level of autonomy and little oversight, and possess skills that could be used to cover up misconduct.

The number of IT employees with high levels of access is expected to increase as a part of DPC's *Cyber Security Strategy 2016–2020*, a workplace plan to attract, develop and retain skilled cyber security public sector workers.[28] It is possible the proposed increase in the number of information technology specialists and administrators across the VPS could raise awareness of information security across the public sector, and eventually lead to a reduction in unauthorised access and disclosure of information. However, the increase in the number of employees with high-level access to information also creates a key risk where these skills might be used to evade detection, potentially increasing the likelihood of information misuse occurring. This risk needs to be acknowledged and addressed by public sector agencies when developing corruption and prevention strategies, and these should be tailored for each agency, depending on the types of information it manages and its associated value. IBAC notes this risk is also mitigated by the controls that agencies are required to implement as part of the VPDSS.

Due to the public sector often competing with the private sector for information technology specialists, there have been recurrent trends of hiring specialists as contractors in order to compete with the salaries offered in the private sector. A key implication of this is that contractors from outside the public sector may not have professional values and ethics aligned with the VPS Code of Conduct or may not receive the required standard of training for an employee with high levels of access to official information.

4.2 Data analytics and 'big data'

The Victorian Government has created the position of the Chief Data Officer within the Victorian Centre for Data Insights, and is seeking to transform how the public sector uses data to strengthen policy making. This process is supported by the *Victorian Data Sharing Act 2017*, which provides a legal framework for sharing and using data across the public sector.

Data analytics and 'big data'[29] is growing in its use globally as well as in Australia. More public sector agencies in Victoria are looking to use this capability, which gives opportunities for agencies to work together to address information security risks. Big data is an area of focus for the government-supported Oceania Cyber Security Centre (OCSC) in Melbourne[30] and many federal government agencies have started using big data and data analytics to better inform their strategic directions.

There are known corruption risks with big data as it brings together previously separate datasets into a new database for matching. This allows employees to access information which they previously may not have had access to, and also makes the material more valuable and sensitive as it is matched with new related information. For example, big data systems may hold multiple pieces of personal identifying information, such as details of driver licences, addresses and bank accounts, which potentially increases the consequences when this information is misused. While these processes and bodies are establishing, some agencies are beginning to assess their own data holdings, forming communities of practice and working together to address data-related corruption risks.

[28] Department of Premier and Cabinet, *Cyber Security Strategy 2016–2020*, updated July 2018.

[29] There is no definitive definition for big data; however, the Office for the Australian Information Commissioner refers to a common definition of 'high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight, decision making, and process optimization.' Office for the Australian Information Commissioner, *Consultation draft: Guide to big data and the Australian Privacy Principles*. May 2016.

[30] Coyne, Allie, *IT News*, 'Victoria opens cyber security mega-hub', 6 October 2016.

4.3 Aging technology systems

The Victorian Government *Information Technology Strategy 2016–2020* outlines that the public sector is 'struggling to work effectively under outdated technology systems that have been implemented as opportunities arose and technologies changed or were introduced'[31]. The large costs associated with new IT infrastructure, and some parts of the public sector not having the capability to manage large and complex IT projects, are two key reasons why the public sector has aging systems. However, this also puts the public sector more at risk of these systems being vulnerable to misuse as information security can be better controlled with more modern IT infrastructure.

Aging systems can also limit the ability to securely access and disclose information within agencies and with approved third parties. Systems that can encrypt data and quickly share information are now commonly used throughout society; however, certain areas of the public sector have not been able to adopt these technological advances and provide these services.

4.4 Social media policy challenges

The policies surrounding social media and smartphone use across the public sector are varied, with some agencies having guidelines and others having dedicated policies. A lack of policy, or poor policies or guidelines, may contribute to the misuse of information on social media because employees are unaware of their information handling responsibilities. Additionally there is an ongoing challenge of keeping these policies up-to-date and in line with technological advancements.

Social media and smartphone use often allows public sector employees to work more efficiently. There is guidance for public sector agencies available from the Victorian Public Sector Commission on the use of social media in the Victorian public sector that may provide a basis for agencies seeking to update their guidelines or policies.[32] Agencies should also consider more recent social media advancements and risks specific to their organisation and employees.

[31] Department of Premier and Cabinet, *Information Technology Strategy 2016–2020: Action Plan 2017–18*, updated September 2018.

[32] Victorian Public Sector Commissioner, *Guidance for the use of social media in the Victorian public sector*, 1 July 2015.

5 Prevention and detection strategies

IBAC has identified a number of potential measures to assist in preventing unauthorised access and disclosure of information, for consideration by public sector agencies seeking to strengthen their information management frameworks.

This is not intended to be an exhaustive list and not all of the measures will be suitable for all areas of the public sector. Public sector agencies have primary responsibility for ensuring the integrity and professional standing of their own organisations. Each agency is best placed to fully assess its own risks and operating environment, and to implement corruption prevention strategies accordingly.

5.1 Victorian Protective Data Security Framework implementation and increased reporting by public sector agencies

Good information management promotes good information security. The VPDSF provides a strong information security framework for the public sector, which, if fully implemented, is likely to drastically strengthen and standardise information security practices across the VPS. The standards will have flow-on effects leading to better practices in auditing and compliance, as well as providing an adequate level of assurance to the community that official information held by the public sector, including citizens' personal details, is secure.

One risk with the VPDSF is how consistently it can be implemented across the key departments and their portfolio bodies. IBAC information suggests there has been confusion in some sectors concerning the level that departmental policies can be implemented throughout portfolio bodies (including statutory bodies), and the ability of these to self-implement and fund the best practice for the public sector.

The onus is on public sector agencies to actively manage risks to their information assets and implement programs that address these risks. As of October 2019, public sector agencies are required to report to OVIC any information security incidents rated as a business impact level of two and higher,[33] including breaches of privacy. Prior to this date, agencies were not required to report information security incidents to OVIC, which relied on agencies to proactively notify it of breaches of privacy. This created an environment that enabled under-reporting. With the implementation and compliance of the VPDSF by public sector agencies across Victoria, as well as the recent changes requiring reporting of security incidents, it is expected reporting and awareness of information security will increase.

[33] OVIC has created a business impact level tool, the BIL App, to assist public sector agencies in assessing the potential business impacts of the confidentiality, integrity or availability of official information being compromised.

5.2 Increased training for employees to encourage reporting

IBAC assesses there is a general under-appreciation for information management and a lack of awareness of how information misuse can constitute – but also enable – corrupt conduct. Due to the complexity of the information management requirements in Victoria, increased training in the legislative requirements for handling official information and data is expected to assist in better practice. OVIC, PROV and the Enterprise Solutions Branch within DPC provide online education and deliver face-to-face training when requested. Many public sector agencies require employees to undergo induction training for information management, often completed through online modules, and there is scope to include training from OVIC and PROV.

Increased and regular training could also include education on the serious consequences associated with information misuse. IBAC and partner agencies have consistently found an under-appreciation for the serious nature of misusing information. Greater use of case studies of offending, where there has been investigative action resulting in termination of employees or other punitive action, could also encourage a greater understanding of the risks, and reduce future offending. Public sector agencies also have the obligation to manage the ongoing suitability and eligibility of all persons with access to official information. This should be supported by a regular program of confirmation and testing of suitability.

While the VPS is making progress in recognising information as an asset, this could be further strengthened. Information loss and theft is yet to be commonly included in theft and loss reports to VAGO, and as discussed above, information misuse is often overlooked as an offence and this enables further offending. One reason for this is the difficulty in putting a financial cost to information loss and theft.[34] Greater recognition of what constitutes information misuse, and reporting this to the most relevant body (including IBAC, OVIC, VAGO, Victorian Inspectorate or Victorian Ombudsman), may assist in deterring such behaviour over the longer term.

[34] Notification of significant or systemic fraud, corruption and other losses must be made to VAGO (among others) as soon as practicable of the incident. Department of Treasury and Finance, *Standing Directions 2018: Under the Financial Management Act 1994*, issued 11 October 2018, revised 7 December 2018.

5.3 Cultural change programs

The former Commissioner for Law Enforcement Data Security (the functions of which now form OVIC) worked with Victoria Police to deliver a long-term research project to 'assess the attitudes and behaviour of Victoria Police officers in relation to law enforcement data security'.[35] The project was informed by surveys of Victoria Police officers in 2012, repeated in 2014, and followed by further, more detailed engagements in 2015 and 2016. This design allowed Victoria Police to track changes in the culture and attitudes to information security, and the subsequent effectiveness of controls and initiatives used were assessed to build awareness and enact cultural change.

Driving the project was an assessment that many officers were taking work information offsite (including to homes) and police officers were commonly using personal devices to store and transfer law enforcement data – often due to workplace solutions being unavailable. The survey found the cultural change program had resulted in a positive change to the level of data security awareness. There also appeared to be an increased perception data security practises had improved due to better policies and procedures. IBAC's consultation with Victoria Police found the project was instrumental in affecting the cultural change program and the survey results found there was a positive impact in terms of overall awareness of practices and the perceived value in building data security awareness. However, it also found there remained issues around the availability of practical and secure systems for officers' use.[36]

This project was able to set a practical baseline to measure cultural change, and assess identified strengths and weaknesses in attitudes, behaviours, processes and systems across the organisation. Public sector agencies could replicate this project using their own surveys to initiate action and measure their cultural change program towards information security. This could assist in minimising opportunities and instances of unauthorised information access and disclosure.

Through primary research and co-design with stakeholders, OVIC intends to generate insights about the current state of information security culture across the public sector in Victoria. These insights will inform the development of a future approach to transformation of cultural attitudes towards information security across the sector. Specifically, the project seeks to:

- deliver insights into the current state of information security culture across the public sector and potential measures to help improve this
- deliver a simple shared model or narrative around information security that resonates with both OVIC and participating agencies
- unpack and understand current problems/ challenges faced within public sector agencies, with respect to their information security culture
- inform the development of targeted training and awareness material for the VPDSF and public sector agencies
- ensure executive buy-in from stakeholder agencies to increase the impact of the project
- develop innovative strategies to enhance information security practices across a diverse range of public sector agencies.

[35] Commissioner for Law Enforcement Data Security, *Survey of Victoria Police Information Security Culture* – Survey Results, November 2012.

[36] Commissioner for Privacy and Data Protection, *CPDP – Victoria Police. Wave 1& 2 – results (abridged)*, 2 March 2015.

6 Conclusions

The protection of official information is critical for the safety of the community, the appropriate use of public money for the delivery of projects and services provided by government, and for maintaining the community's confidence in the public sector. Information must be managed in accordance with its security value, and be based on business requirements, with adequate security measures in place to prevent and detect misuse, including unauthorised access and disclosures.

Raising the awareness of public sector employees and the community that information misuse can enable and also be corrupt conduct will allow for greater prevention, detection and reporting of incidents when they do occur.

This report has analysed common risks of information misuse and the drivers of these risks across the public sector. Similar risks are shared by public sector agencies across Victoria and create common opportunities to learn and identify best practices for information security.

The introduction of the VPDSF and VPDSS is a promising step as it provides Victorian public sector agencies with an opportunity to assess the information they hold and decide how best to secure it. The successful implementation of the VPDSS will result in better information management and security practices, and greater education of risks in these areas. With public sector agencies' reporting obligations on the VPDSS to OVIC having commenced in August 2018, more information will exist on how the impact of the framework's standards has likely improved the identification of information management risks and mitigations (including those related to corruption risks) for public sector agencies.

ibac independent broad-based anti-corruption commission
Victoria

Level 1, North Tower
459 Collins Street, Melbourne Victoria 3000
GPO Box 24234 Melbourne Victoria 3001
Phone 1300 735 135 | Fax (03) 8635 6444

www.ibac.vic.gov.au