Maintaining the Integrity and Confidentiality of Personal Information

Victorian Auditor-General's Report

November 2009

2009-10:8

VICTORIA

Victorian
Auditor-General

Maintaining the Integrity and Confidentiality of Personal Information

Ordered to be printed

VICTORIAN
GOVERNMENT PRINTER
November 2009

PP No 258, Session 2006–09

ISBN 978 1 921650 20 8

VAGO

Victorian Auditor-General's Office

Auditing in the Public Interest

The Hon. Robert Smith MLC
President
Legislative Council
Parliament House
Melbourne

The Hon. Jenny Lindell MP
Speaker
Legislative Assembly
Parliament House
Melbourne

Dear Presiding Officers

Under the provisions of section 16AB of the *Audit Act 1994*, I transmit my performance report on *Maintaining the Integrity and Confidentiality of Personal Information.*

Yours faithfully

D D R PEARSON
Auditor-General

25 November 2009

Contents

Audit summary

Background

The public sector is a complex business. In its normal, day-to-day activity it legitimately gathers and uses personal information about citizens, and shares it with a range of entities both within and outside government.

Personal information is information about an individual that identifies a person. Information such as your name and address may be readily accessible, and well known within the community. However, other information, such as your health or criminal record, may not be well known and should not be easily accessible.

This report examines how personal information is stored, processed and communicated by the public sector. It evaluates whether its confidentiality and integrity has been maintained.

Maintaining confidentiality means that personal information is accessed only by those who need it to perform their duties. Maintaining integrity means that information provided is not later corrupted or lost, either intentionally or inadvertently.

Personal information can be misused with potentially serious consequences. For example, an individual can suffer financial loss or damage to their credit rating, their medical records can be compromised, or they may suffer from threats, and/or harassment if their identity is 'stolen'. To redress the damage, a person may also suffer loss of time and money.

Effective information security controls that focus on safeguarding all information and information systems are needed. Securing information, including personal information, requires a balanced and integrated approach to people, process and technology, with a strong security governance framework.

This report assesses whether governance and risk management practices in three departments have been sufficient, and whether central policy direction and guidance has effectively driven the public sector to achieve this aim.

Overall conclusions

The confidentiality of personal information collected and used by the public sector can be, and has been, easily compromised. While we examined only three departments, the ability to penetrate databases, the consistency of our findings and the lack of effective oversight and coordination of information security practices strongly indicate that this phenomenon is widespread. Recent incidents of personal information being found in public places or in the hands of unauthorised persons, are further evidence of this.

This situation has arisen partly because information security policy, standards and guidance for the sector are incomplete and too narrowly focused on ICT security.

The central direction and effective coordination of the broad scope of information security risks remains weak. Neither the Department of Treasury and Finance nor the Department of Premier and Cabinet have addressed all aspects of information security following the disbanding of the Office of the Chief Information Officer and its supporting committees in 2006.

In the absence of strong and consistent central leadership and effective oversight, the importance of protecting personal information has not been properly understood by the sector. The departments examined have recently strengthened their information security governance, but information security risks have not been managed effectively. Elements of organisational culture, practices and controls all have weaknesses that can be exploited to breach confidentiality in the systems examined. There is also little assurance that the integrity of data has been maintained in these systems.

Weaknesses in controls over the confidentiality and integrity of financial information have been identified through our annual financial audits and reported to the Parliament for many years. It is disappointing that the important lessons about security of information also translate into non-financial information.

Main findings

Governance

The way in which the Victorian public sector does business is increasingly sophisticated and the relationships it develops, increasingly complex. The exchange of information with other agencies, the private sector and across jurisdictions creates a range of challenges such as, who owns the information, how can recipients be directed to provide equivalent standards of privacy and security over the information shared, and who is responsible if the information is lost or leaks and confidentiality is breached.

The approach to managing information security has not met these challenges or kept up with how the sector does business nor the complexity of its business relationships.

It is imperative that action is taken quickly to provide more effective governance and leadership so that these situations are remedied.

The Department of Treasury and Finance and the Department of Premier and Cabinet have not fulfilled their responsibilities to develop and maintain whole-of-government information security standards and guidance, to improve the coordination of identity and information management systems at state level, and to provide policy advice on emerging trends and issues in identity and information management.

Under the state’s governance arrangements, responsibility and accountability for departmental performance rests with departmental secretaries. However, our findings from within three departments, and our wider discussions in the sector, demonstrate that departments and the wider public sector need better direction about information security and management. More timely development of standards and guidance relevant to local conditions and risks is needed; as is better identification and effective management of risks, including emerging whole-of-government risks; better education and awareness-raising across the sector; and allocation of resources to achieve the minimum standard required.

Most public sector agencies are currently not mandated to comply with public sector information security policy and standards. Given that information is legitimately shared by agencies throughout the sector, this has the potential to compromise the mandated information security arrangements in place in departments.

Culture, practice and technology

Fundamental flaws are evident in the way the Victorian Government Risk Management Framework is applied, and greater guidance across the sector is needed. Risks cannot be managed where an agency is not aware of them, or does not understand their significance. Without substantiation, attestations by agency heads about the effectiveness of controls have no value.

Information security risks were not effectively managed within the three departments. In one, threats to and vulnerabilities of the systems and networks were understood within the information technology section but advice had not made its way to senior management and so were not effectively managed. Similarly, in the two other departments, business units were aware of the risks to the information but the risks were not uniformly managed across the department.

Databases that stored personal information could be accessed by unauthorised people, quickly and easily. This was because the information was not appropriately classified and the necessary controls were either missing, or were not operating as required.

Departments could not be sure their systems had not previously been breached and personal information accessed by unauthorised parties or stolen, because logs of access and changes were either not maintained or not reviewed on a timely basis.

Since the audit the departments have acted to improve security over the databases examined.

Data was transmitted from the three departments by emails in formats that were easily read. This means they could be accessed by someone other than the intended recipient.

Personal information was stored on portable storage devices, CDs and DVDs that are vulnerable to loss, in easily-read formats. Personal information was exchanged via personal email accounts, some of which were particularly vulnerable to unauthorised access. Extracts or whole copies of personal information from the selected databases were stored in unsecured shared drives on departmental networks accessible by unauthorised staff. Compliance by staff with information security requirements was not monitored by any of the three departments.

All three departments provide personal information to third parties—organisations that provide services on their behalf; that provide ICT services; or that host their information systems. Departments did not require independent certification, or carry out their own assessment, that the security third parties had in place met the required public sector security standards. There was little assurance that information was adequately protected by third parties to whom the information was legitimately provided.

Recommendations

Number	Recommendation	Page
1.	The Department of Treasury and Finance and the Department of Premier and Cabinet should: • clarify their respective roles and responsibilities for information security, to better coordinate their activities, and to address the functions of the disbanded OCIO and its supporting committees • expedite the release of a comprehensive, integrated suite of standards and guidance that address all aspects of information security including protective security, and which are based on risk and relevant to local conditions • mandate that all public sector agencies adopt the whole-of-government information security policies and standards • establish clear oversight to monitor implementation of information security policies and standards and compliance with the reporting requirements • establish a process to identify and communicate emerging information security risks to the sector.	16
2.	All public sector agencies should assign responsibility for information security practices both to senior management, and to line management at appropriate levels throughout the organisation.	16

Recommendations – *continued*

Number	Recommendation	Page
3.	To adequately protect the integrity and confidentiality of citizens' personal information each public sector agency should: • Develop more robust risk management practices, which demonstrate that annual risk attestations are based on substantiated evidence that information controls are effectively addressing risks. • Include in staff training, the importance of information security; the range of threats to information security and the vulnerabilities of electronic and hardcopy records and physical security in workplaces. • Regularly monitor compliance by staff with information security policies, standards and required practices. • Conduct an inventory of all the information they store, process and communicate, assess its criticality, classify the information; and determine, and put in place, the minimum controls needed to protect it. • Assess the threats and vulnerabilities, both internal and external, to their ICT systems, implement appropriate controls to address them and regularly monitor that the controls are in place and operating as required. • Regularly monitor logs and records of access and changes to information. • Establish agreements with third party service providers to clearly specify minimum standards of security over information handled, at least equal to those required of the public sector, and that provide for regular certification of compliance with the standards. • Conduct periodic random checks of the controls in place at third party service providers over citizens' personal information.	26

Audit Act 1994 section 16—submissions and comments

Introduction

In accordance with section 16(3) of the *Audit Act 1994* a copy of this report, or relevant extracts from the report, was provided to the Department of Premier and Cabinet, the Department of Treasury and Finance and the three other departments audited with a request for comments or submissions.

The comments and submissions provided are not subject to audit nor the evidentiary standards required to reach an audit conclusion. Responsibility for the accuracy, fairness and balance of those comments rests solely with the agency head.

Submissions and comments received

RESPONSES provided by the Secretaries of the three other departments audited

One Secretary provided a response for inclusion in the report indicating that he agreed with the relevant recommendations.

Another Secretary provided a favourable response but indicated the response was not for inclusion in the report.

RESPONSE provided by the Secretaries of the Department of Premier and Cabinet and the Department of Treasury and Finance

The Department of Premier and Cabinet (DPC) and the Department of Treasury and Finance (DTF) are pleased to submit a joint response to this report, which will provide a valuable contribution in relation to information security. Information security is a challenging issue for governments worldwide; as governments seek to offer more efficient and effective technology-enabled services to citizens, so they must also employ increasingly sophisticated techniques to prevent inappropriate access to and use of personal information.

The report is timely as work is currently underway across government to strengthen information security practices. The report will therefore assist in providing a greater focus on this important area in order to enhance current policies, processes and standards.

RESPONSE provided by the Secretaries of the Department of Premier and Cabinet and the Department of Treasury and Finance – continued

The report acknowledges that, departments have acted to improve security over the databases examined and enhance staff awareness of information security issues. This is a reflection of the fact that the issue is one of high priority, and is taken very seriously at the most senior levels of government. Steps are also being taken through existing Whole-of-Government forums to ensure a coordinated and consistent approach to information security continues to be promoted.

The following responses to the audit recommendations are offered by DPC and DTF:

Recommendation 1

The Department of Treasury and Finance and the Department of Premier and Cabinet should:

- clarify their respective roles and responsibilities for information security, to better coordinate their activities, and to address the functions of the disbanded OCIO and its supporting committees

  Response: *DPC and DTF accept this recommendation, and will review and articulate their respective roles more clearly to departments and agencies.*

- expedite the release of a comprehensive, integrated suite of standards and guidance that address all aspects of information security including protective security, and which are based on risk and relevant to local conditions

  Response: *Consistent with other jurisdictions, the Victorian Government's information security strategy will continue to align with the integrated and comprehensive international, national and Commonwealth Government information security standards. DPC and DTF will continue to review these standards from the perspective of local conditions and Department/Agency risk profiles.*

- mandate that all public sector agencies adopt the whole-of-government information security policies and standards

  Response: *The Victorian Government Risk Management Framework mandates a widely accepted best practice approach to be adopted by all departments and public sector agencies to ensure risks are effectively managed.*

  In September 2009, a new Ministerial Direction was issued by the Minister for Finance under the Financial Management Act 1994, mandating a risk based approach to the management, collection and storage of information and also referencing the DTF standards 'Information Security Management Framework' and 'Information Security - Data Classification and Management'.

RESPONSE provided by the Secretaries of the Department of Premier and Cabinet and the Department of Treasury and Finance – continued

Recommendation 1 – *continued*

The Department of Treasury and Finance and the Department of Premier and Cabinet should:

- establish clear oversight to monitor implementation of information security policies and standards and compliance with the reporting requirements

  Response: *DPC and DTF agree with this recommendation. The report acknowledges the reporting regime already implemented by DTF, and the recent assignment of central responsibility for the coordination of information security to the Deputy Secretaries Leadership Group. These arrangements will be reviewed with a view to further strengthening the existing oversight arrangements undertaken via the Whole of Victorian Government Chief Information Officers Council and Whole of Victorian Government IT Directors Forum, and to take into account the matters raised in the Report.*

- establish a process to identify and communicate emerging information security risks to the sector

  Response: *The report acknowledges that the Whole of Victorian Government Chief Information Officers Council and Whole of Victorian Government IT Directors Forum already considers information security matters, including identifying and communicating emerging information security risks to the sector. These forums, together with security staff nominated by each agency, are already used to identify and communicate information security risks within inner-budget agencies. DPC and DTF accept the need to strengthen this process and put in place formal interaction with the other Victorian Government entities with responsibility in this area (for example the Victorian Privacy Commissioner).*

Recommendations 2 and 3

DPC and DTF agree in principle to recommendations 2 and 3, noting that the priorities and need for action in each agency will be informed by the robustness of existing practice within the agencies, and by each agency's assessment of its own agency-specific risks in information security.

Further, DTF will explore avenues to strengthen support of the existing Victorian Government risk management framework to assist in its effective implementation by agencies.

1 Background

Public sector agencies process, store and communicate huge volumes of information. This information is stored both in hardcopy and, increasingly, in electronic format. It is communicated in a variety of ways; email, fax and over the phone; on portable storage devices such as CDs, DVDs and USB keys; and through the postal system or by point to point courier.

The way the public sector conducts business requires information sharing both within and outside government. Increasingly, non-government organisations and the private sector are relied upon to deliver services. Much of the public sector's information and communication technology (ICT) services are outsourced, with computer hardware, software, communication, and electronic storage being managed by the private sector. The public sector also legitimately exchanges information with organisations in other jurisdictions, both domestic and international. These jurisdictions may have different privacy legislation or information security standards.

These ways of doing business give the public sector the ability and flexibility to communicate quickly. However, they also increase the potential for information to be lost, corrupted or misused, either deliberately or accidentally.

1.1 Information security

Implementing and maintaining effective information security is needed to achieve three objectives:

- **confidentiality**—information should be accessible only to those authorised to access it
- **integrity—**processing methods should safeguard the accuracy and completeness of information
- **availability**—authorised users should have access to information when required.

In short, the right people should get the right information, at the right time.

Information security and privacy are complementary, but are not the same. Privacy legislation and information privacy principles focus on the way information about individuals should be obtained and handled. Information security goes beyond that to the systems and processes used to store, access, exchange and safeguard the information itself.

An effective information security framework protects both individuals' privacy and the integrity of the information. The framework needs to include policies, standards and guidelines that direct governance and risk management. It also needs sound controls to secure the systems that hold personal information either electronically or in hardcopy, to prevent either its malicious or accidental misuse.

Securing personal information

This audit focuses on personal information. Public sector agencies collect, create, use, hold and distribute a wide range of personal information. In many cases providing personal information to the public sector is compelled, for example, when registering life events such birth, death and marriage; for property and business transactions; for obtaining public hospital treatment; for obtaining a concession or access to public housing.

Personal information is defined in the *Information Privacy Act 2000* as information, whether fact or opinion, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. The definition captures a large range of information.

Examples of personal information can include:

- your name, address, phone number and email address
- your photograph, a video recording of you whether on CCTV or otherwise
- your salary, bank account and financial details
- allegations of wrongdoing against you and details of wrongdoing and offences you have committed
- details of your land ownership and disputes about that land
- your qualifications and educational activities
- your medical details and health information
- your fingerprints and blood type
- your religious and sexual preferences
- your membership of professional and other bodies.

Some personal information such as your name and address may be relatively easily available and well known within the community. However, some, such as your health or criminal record, may not be well known.

Information security risks and threats

Failure to maintain the confidentiality of personal information exposes both the individual and the public sector to loss. This ranges from damage to reputation, to identify theft and fraud, and potentially to physical harm.

Failure to maintain the integrity of personal information can lead to incorrect decisions with adverse consequences. Decisions made using personal information cover a range of matters including eligibility for services, allocating resources, claims management and generally addressing or planning for community needs.

Some recent incidents where confidentiality of personal information has been breached include:

- **International**—In 2007 CDs containing personal information: government benefits, names, addresses, dates of birth and bank account details, of 25 million United Kingdom citizens were lost, resulting in the resignation of the Chief Executive of Her Majesty's Revenue and Customs. More recently, in October 2009, users of Hotmail, Google and Yahoo web-based email across the world became victims of hackers. The hackers gained users passwords and security information by tricking unsuspecting account holders to provide personal information, and then posted the information online.
- **National—**In 2006 a high-ranking army officer left a CD containing a report into the death of an Australian soldier in Iraq in a computer at Melbourne airport. Another passenger found the CD and gave it to a media outlet.
- **State—**In July 2009, client files were found in filing cabinets after they were sold at auction. The cabinets were previously owned by an independent community service organisation established to protect and care for children in difficulty; and in September 2009 an official report book from ticket inspectors was found at a tip containing the names and addresses of 45 commuters accused of offences such as fare evasion.

Within Victoria we found no data to estimate the size of the problem. However, recent studies show that internationally, the incidence of data loss is significant. For example, data from 2009 shows that 70 per cent of UK organisations have had at least one data breach in the past year. Of these organisations, the public sector experienced the highest number of data breach incidents, reporting an average of 4.5 breaches per organisation.

Other data show that worldwide, from 2005 to 2008, 280 million people lost personal details. Almost one fifth of these data loss incidences were linked to government organisations and 46 per cent of the data had no form of protection.

1.2 Audit objectives and scope

The objective of this audit was to determine whether the integrity and confidentiality of personal information held by agencies has been maintained.

Specifically the audit examined whether:

- appropriate policy direction and guidance is in place to drive a focus across the public sector on adequately protecting personal information
- selected agencies had established and complied with governance and risk management practices that protect the confidentiality and integrity of, and access to, personal information
- personal information had been, or could be, compromised.

Audit approach

This audit evaluated whether the governance and risk management arrangements at the whole-of-government level provided sufficient policy direction and guidance to public sector agencies. At the whole-of-government level we focused on the roles and activities of the Departments of Premier and Cabinet, and Treasury and Finance.

To test whether appropriate governance and risk management arrangements are established and operating to protect personal information we examined these aspects within three departments.

Within each department we examined a database that held sensitive personal information. We reviewed the policies, procedures and practices associated with the use of this information in these databases; assessed the effectiveness of the controls over confidentiality and integrity; and carried out penetration testing within the network to determine if we could circumvent these controls.

Our evaluation used criteria derived from the legislative framework and internationally recognised best practice.

The audit was conducted in accordance with the Australian auditing standards applicable to performance audits.

The total cost of the audit was $725 000, which includes staff time, overheads and printing.

2 Governance

At a glance

Background

Good governance provides a solid foundation for managing resources well, including information resources. We assessed whether governance at whole-of-government level and within departments has provided sufficient policy direction, standards and guidance to maintain the integrity and confidentiality of personal information.

Findings

- A comprehensive suite of standards to guide and support effective information management and security practice across the public sector, which are based on risk and relevant to local conditions, has yet to be implemented.
- The current policies apply only to 11 departments, and to four inner budget agencies; and primarily address ICT risks.
- Misconceptions and misunderstandings about information security are common, and have adversely affected how departments, including central agencies, manage information security.
- In the absence of clear leadership, the importance of protecting the integrity and confidentiality of personal information has not been properly understood, and effective oversight not provided for the sector.

Recommendations

The Department of Treasury and Finance and the Department of Premier and Cabinet should:

- clarify their respective roles and responsibilities for information security
- quickly release standards and guidance that address all aspects of information security, based on risk and relevant to local conditions
- mandate all public sector agencies adopt the whole-of-government information security policies and standards
- establish oversight of application of information security policies and standards and compliance with reporting requirements
- establish a process to identify and communicate emerging information security risks to the sector.

All public sector agencies should assign responsibility for information security practices to appropriate levels throughout the organisation.

2.1 Introduction

Good governance provides a solid foundation for managing resources well, including information resources.

The public sector governance framework provides that day to day management of information security rests with agency heads. However, this cannot be effective if done by individual agencies in isolation. The need to exchange information between agencies, and outside the public sector, requires a common security management framework. Otherwise, information secured under standards and controls in one agency, could be compromised by poor practice and standards in another.

A common set of information security policies, principles and standards that apply to all agencies, their staff and contractors is needed to set minimum expectations for the protection of information. This was recognised in 2005 with the approval and issue of the Information Security Management Policy, which came into effect from 1 July 2005.

2.1.1 Central agency roles and responsibilities

The Department of Treasury and Finance (DTF) and the Department of Premier and Cabinet (DPC) are the central agencies with responsibility for information security across the public sector.

Since late 2006 the Government Services Group (GSG) in the Department of Treasury and Finance has had responsibility for establishing and maintaining Whole-of-Victorian-government (WOVG) information security and technology policies, standards and guidelines. Before then, this responsibility rested with the Office of the Chief Information Officer (OCIO), which was disbanded in 2006.

In late 2008 the Department of Premier and Cabinet established an Identity Policy Team. Its role is to:

- take a lead in developing Victoria's position on the National Identity Security Strategy and other national initiatives
- improve the coordination of identity and information management systems at state level
- lead the development of a WOVG strategic framework in this area
- provide policy advice on emerging trends and issues for the public sector in the areas of identity and information management.

In this chapter we examine whether:

- appropriate central policy and guidance are in place to drive the adequate protection of personal information across the public sector
- departments have established sound governance and comply with practices to protect the integrity and confidentiality of personal information.

2.2 Central policy and guidance

2.2.1 Information security management policy

This 2005 policy, issued by the OCIO, mandated that departments and agencies will use approved standards and guidelines to manage their information and communications technology (ICT) security.

The purpose of the policy, as set out in the document, is ‘to establish consistent appropriate level of security for ICT’ recognising that ICT systems are a ‘critical enabler for confidentiality, integrity and availability of government information and services’. Specifically, the statement of policy within the policy document indicates that ‘Victorian Government Departments and Agencies will use identified and approved Whole of Victorian Government (WoVG) standards and guidelines to manage ICT security appropriate to the sensitivity of information and assets to be protected’.

The expected benefits set out in the policy included: industry standards-based risk management practices and increased and consistent protection of the state’s systems and data. However, there are two aspects of the policy that constrain potential benefits.

First, while its title reflects the broad sweep of ‘information security’, its scope and content is limited to ICT security. This means that other aspects of protective security arrangements that directly affect information security, such as physical and environmental security; and human resources security, including staff responsibilities, their suitability for roles, and screening for sensitive jobs, are not dealt with. It also means that the protection of information that is not stored or communicated electronically is not addressed.

Second, it is ‘badged’ as a whole-of-Victorian-government policy, but most public sector agencies are not covered by it. It applies only to the 11 departments, and to four inner budget agencies: the State Revenue Office, VicRoads, Victoria Police and the Environment Protection Agency.

2.2.2 Information security standards

Implementation of the policy is to be supported by an approved standards-based information security management framework, ICT standards, guidelines and procedures defined and issued by GSG.

Information security management framework standard

The OCIO released the Information Security Management standard in 2005. GSG rebadged and renamed this standard to the Information Security Management Framework standard in April 2009. At that time it also established compliance reporting requirements.

The standard provides for departments and agencies to develop an Information Security Management Framework consisting of:

- **Information security policy**—a high level document covering the principal security objectives.
- **Information security management system** (ISMS)—a description of the ISMS and its operations.
- **Risk assessment report**—risk assessment performed on the scope of the ISMS.
- **Statement of applicability**—a description of each of 132 ICT controls and how they are achieved.

The standard 'applies to the management of all aspects of the security of ICT' and mandates compliance with the *International Standard for Information Security Management, Specification for Information Security Management* (ISO 27001:2006) and *Code of Practice for Information Security Management* (ISO 27002:2006), 'an international standard providing best practice guidance on security controls for consideration for implementation within an organisation' and the Australian information security risk management guidelines.

The potential benefits from the standard are limited by the same two factors noted for the Information Security Management Policy: its scope and content is limited to ICT security; and while badged as whole-of-Victorian-government it applies only to the 11 departments and four agencies previously mentioned.

The international standards refer to other aspects such as physical and environmental security and human resources security. GSG advised that linking the standard to the international standards is sufficient to extend the Information Security Management Framework Standard's applicability to all aspects of information security. Accordingly, GSG does not plan to issue standards for all security aspects addressed by the international standards. However, the international standard lacks detail and, being a general document, cannot take account of the Victorian public sector context.

To some extent this limitation has been recognised by GSG through the issue of more detailed standards—the Data Classification and Management Standard, and four Identity Access Management Standards—despite those aspects being addressed in the international standard. Two additional standards—Use of Portable Storage Devices and Penetration Testing—were released on 13 November 2009.

Reporting on progressive compliance with the standard

The standard requires progressive compliance from its date of effect, 9 April 2009. The first mandated milestone was for departments and agencies to develop a draft plan outlining how they were to achieve progressive compliance with the standard, and to submit this to GSG by 9 October 2009.

No draft plans were submitted by that date. The guidelines and templates to assist the development of each of the four components of the framework were not released by GSG until 20 October 2009. The reporting time line has been extended to 30 November 2009.

Data classification and management standard

This standard was also approved and released in April 2009. It requires departments and agencies to undertake formal assessments of the risk of inappropriate release, access or modification of information.

To undertake this risk assessment agencies first need to classify the information they hold in terms of the consequences, both to government and other parties, of its unauthorised release.

For much information held by departments and agencies, there will be little or no consequence if it is released, and this information therefore does not need to be classified. For example, information that is already in the public domain.

However, information such as personal information requires classification because of the potential harm that can arise if it is released, or accessed by those without authority.

The standard mandates that the information classification scheme used by the Commonwealth Government be adopted. This scheme, set out in the Commonwealth Protective Security Manual (PSM), first separates information into two categories—that with implications for national security, and non-national security information. Within each category, a series of increasingly higher classifications are defined to distinguish the various classes of information in terms of the risk from their exposure.

Figure 2A sets out the two classification schemes.

Figure 2A
Australian Government information classification schemes

National security classifications	Non-national security classifications
Top secret	
Secret	Highly protected
Confidential	Protected (includes Cabinet-in-Confidence)
Restricted	X-in-confidence

Source: Victorian Auditor-General's Office, based on the *Australian Government Information and Communications Technology Security Manual, 2008*. <http://www.dsd.gov.au/library/infosec/ism.html> accessed 14 October 2009.

The overwhelming majority of data held by the Victorian public sector will be non-national security information, hence mandating a classification scheme for this data has the greatest potential to improve security.

However, the Victorian public sector's approach to non-national security data classification has changed twice between the 2005 policy and the current standard. In December 2007 the Strategic Coordination and Management Council, approved a 'Framework for the Management and Protection of Security Classified Information'. This framework was developed primarily to implement a 2007 memorandum of understanding with the Commonwealth Government on the protection of national security classified information. Notwithstanding this, it mandated that the classification scheme in the PSM apply immediately to all sensitive information, including non-national security information.

The advice to departments about this decision, issued in February 2008, required heads of all agencies to achieve reasonable progress toward the minimum standards in their agencies by June 2008.

In December 2008, four months before the release of the latest standard by DTF's GSG, the Secretary of the DPC issued an amendment to the December 2007 framework that removed its mandated application to non-national security information.

Advice to agencies about the reasons for the decision stated that 'applying PSM to all non-national security classified information, in the case of some agencies, would require significant security upgrades, particularly for IT systems, and require more resources than anticipated'. The advice goes on to note that the decision will mean that there will not be a common classification system or security standard across the Victorian public sector.

The April 2009 standard largely reinstates the situation that applied from December 2007 to December 2008, that is, that all sensitive information including non-national security information should be classified. The primary distinction between the two is that the 2009 standard's application is limited to departments and four inner budget agencies, whereby the 2007 framework applied to all agencies.

Progress on other information security standards

The *Identity Access Management Policy*, released in September 2006, is directed to making sure that only known, authorised users gain access to systems and information. The policy says that standards were 'to be developed in the coming months' to cover:

- information sensitivity classification and related processes
- identification authentication and authorisation of user
- recording and auditing of activities
- detection reporting and collection of evidence related to unauthorised access to information or systems.

In July 2009 GSG advised that there were a number of information security standards ready to be rolled out. On 20 October 2009 four Identify and Access Management Standards were released, more than three years after release of the policy.

Our examinations of policies, practice and controls in three departments indicate that in the interim, agencies were operating with insufficient guidance. We cannot be assured that during that time, the risks of access to personal information by unauthorised persons were effectively managed.

Conclusion

A comprehensive suite of policies and standards to guide and support effective information management and security practice across the public sector has yet to be implemented despite the policy being approved in 2005. Progress to date has been slow, and little real change is evident. Plans are no substitute for action, and the mandated plans are now overdue.

The rapidly changing policy position on the classification of non-national security information indicates the need for better role delineation between the two central agencies.

2.2.3 Central oversight and coordination

From December 2003 to late 2006, the OCIO was to coordinate and integrate information management and security across the public sector. The role was supported by a committee structure, including a policy council with deputy secretary level representatives from each department.

The OCIO had the opportunity to provide direction and encourage achievement of minimum information security standards across the sector.

In late 2006, the OCIO and the supporting committees were disbanded. The OCIO’s functions were distributed among DTF’s Government Services Group, DPC and the then Department for Victorian Communities. Both the functions of the OCIO, and their allocation between the departments were unclear. We found that GSG is uncertain about its mandate in this regard.

Department of Premier and Cabinet

To date the Identity Policy Team in DPC has focused its efforts on contributing to the development of the National Identity Security Strategy and working on a national document verification service and standards. It has yet to address its wider responsibilities for improved coordination of identity and information management systems at state level, or providing policy advice on emerging trends and issues for the public sector in the areas of identity and information management.

In November 2005 the OCIO commissioned a study of the adequacy of the public sector's information security systems and protocols. Responsibility for supporting departments to implement recommendations was not allocated, following the disbanding of the OCIO. This study was passed from GSG to DPC in June 2008. To date, DPC has not addressed the study's recommendations.

Other entities

There are a number of entities or office bearers with a specific interest in maintaining privacy and information security within Victoria, including the:

- Commissioner for Human Rights and Equal Opportunity
- Commissioner for Law Enforcement Data Security
- Health Services Commissioner
- Ombudsman
- Public Records Office
- Victorian Privacy Commissioner
- Victorian Managed Insurance Authority.

The Privacy Commissioner provides a vital role in enforcing privacy principles, raising awareness of privacy matters, handling complaints and investigating reported breaches. The Commissioner for Law Enforcement Data Security was appointed to improve security and integrity of Victoria Police's law enforcement data following a series of leaks from Law Enforcement Assistance Program.

Other entities and office bearers provide important support to the activities of the sector. For example, the Victorian Managed Insurance Authority monitors risk management by departments and the Public Records Office develops recordkeeping standards to help the public sector create and maintain better records.

The Department of Justice convenes an inter-departmental committee of agency privacy managers, which focuses on putting privacy requirements into practice. The WOVG Chief Information Officers Council and the WOVG IT Directors Forum chaired by DTF also consider information security matters.

However, there is currently no forum to coordinate the approach to information security across the Victorian public sector, either among the 'other entities' or office bearers, or between them and public sector agencies. In its absence, consistency in approach to information security relies upon office bearers and entities establishing professional relationships. In some cases, these relationships appear strong. In others, they have yet to be established.

As a result of this audit, the Deputy Secretaries Leadership Group accepted responsibility for the coordination of information security and will receive formal advice from the WOVG Chief Information Officers Council.

Conclusion

The way in which the public sector does business is increasingly complex, and presents challenges for managing information security. Who owns the information exchanged with third parties, how it makes sure that recipients have equivalent security over the information; and who is responsible if the information is lost, leaks or its integrity and confidentiality is compromised, are just some of the emerging challenges faced by the sector. Lack of effective leadership means that these challenges have not been addressed and the approach to maintaining information security has not kept up with changes in the sector's business environment.

It is evident that there has been no effective oversight and coordination of information security for the public sector.

It is not clear which central agency has overall responsibility for information security, as opposed to ICT security. It is clear, however, that neither DTF nor DPC has fully addressed all aspects of information security.

2.3 Departmental governance

Like other important aspects of agency business, information security requires an effective governance framework: one that defines leadership responsibilities; articulates the roles; and maintains a culture of information security awareness.

To effectively govern information security, agency management must also establish and maintain policies and guidance that address the breadth of information security activities and requirements.

However, appropriate governance and management structures do not, on their own, guarantee effective information security. There also needs to be real commitment to and ownership by people tasked with implementing it.

Within the three departments we found that:

- each had a governance structure with cross-organisational representation at a sufficiently senior level to facilitate information security governance. However, in one department there was no central information security management or governance function before May 2009
- responsibility for making sure compliance with information security requirements was not clearly assigned
- information security was not well understood by staff
- training was not well focused.

Despite obvious differences, there were also some similarities observed in the three departments. Figure 2B provides an overview of our findings relating to information security governance in the departments.

The rating scale used to evaluate each department's practices/capability and maturity levels in each of the information security governance attributes reviewed by us, is also provided below.

Figure 2B
Information security governance—assessments in three departments

Information security governance attributes	Department A	Department B	Department C
Governance structure with senior management representation	Developing to established	Established	Established
Roles and responsibilities for information security assigned at appropriate senior management	Developing to established	Established	Established
Roles and responsibilities for information security practices assigned to line management throughout organisation	Initial	Established	Initial
Information assets are identified	Developing	Established	Initial
Information is classified	Developing	Established	Initial
Controls to provide appropriate level of security applied to classified information identified and put into practice	Developing	Developing	Developing
Oversight or monitoring of compliance of staff and third parties with information security, standards and guidelines	Initial	Initial	Initial
Assurance required in relation to third-party compliance with standards	Initial	Initial	Initial

Legend for rating criteria

Initial	Department has limited capability.
Developing	Department is working on developing practices/capability.
Established	Department has developed practices/capability and is operating in a steady state.
Continuous improvement	Department is focused on continuous improvement, effective practices and optimising capability.
Good practice	Department has developed and implemented effective practices and is a leader in the area.

Source: Victorian Auditor-General's Office.

Governance of information security in each department should be improved. This can be achieved by:

- allocating responsibility for information security throughout the department
- implementing effective information classification systems and controls over information assets
- putting in place arrangements for supervising compliance of staff and third parties with information security requirements.

By doing this, management can raise the profile of information security and its importance in day to day business.

Throughout the audit, in documents examined, and during our discussions with the audited agencies, including the central agencies and other parties, we found a series of common misunderstandings about information security, including:

- a belief that compliance with information privacy principles alone is sufficient to protect the integrity and confidentiality of personal information
- a belief that information security is a technology issue, rather than a combination of people, process and technology responses to managing information
- a belief that information security relates only to electronic records and not hardcopy records.

These misconceptions have adversely affected how well departments, including central agencies, manage information security.

Policies and guidance

All three departments had developed policies and guidance to provide direction and support about information security. However, without whole-of-Victorian-government (WOVG) leadership, the focus of the policies and guidance varied, there were gaps in coverage and the focus was astray in at least one department.

Not all departments had addressed high risk areas such as security requirements for laptops, portable storage devices, user access, security incidents, certification and accreditation of third parties and physical security.

Only one department had comprehensive policies for protecting personal information, which mirrored international ICT security standards. However, improvement is required to its compliance monitoring policy and its information classification arrangements.

Another's department-wide information security policy was not in place until April 2009—some four years after the release of the WOVG information security management policy. However, its recently developed policies and guidelines are in line with information security better practice and seek to achieve department-wide compliance with relevant information security standards.

In the third department, policies and standards focused on managing hardcopy records or managing documents within its records management system rather than on the security of all information held across the department and its ICT networks.

Information security policies and guidance in each of the three departments need improvement to comprehensively address ICT, management of physical records and physical security.

2.4 Conclusions

Governance over information security in each department can be improved. This can be achieved by:

- clarifying that all staff, contractors and service providers are responsible for maintaining information security

- developing and implementing effective information classification systems and controls over information assets
- putting in place arrangements for supervising compliance of staff and third parties with information security requirements.

By doing this, management can raise the profile of information security and its importance in day to day business.

Information security policies and guidance in each of the three departments also need improvement. The shortcomings threaten the confidentiality and integrity of personal information in those departments.

Under the state's governance arrangements, responsibility and accountability for the departmental performance rests with departmental secretaries. However, based on our findings from within the three departments, discussions within the sector and the results of financial audits conducted by VAGO, there is strong evidence that the audit findings are likely to be reproduced across the sector. This demonstrates that the public sector needs better direction about information security in order to protect the integrity and confidentiality of the information it handles.

The sector needs timely development of relevant standards and guidance; identification of emerging risks; education and awareness raising; and the encouragement to achieve the minimum standard required, across the public sector.

Recommendations

1. The Department of Treasury and Finance and the Department of Premier and Cabinet should:
   - clarify their respective roles and responsibilities for information security, to better coordinate their activities, and to address the functions of the disbanded OCIO and its supporting committees
   - expedite the release of a comprehensive, integrated suite of standards and guidance that address all aspects of information security including protective security, and which are based on risk and relevant to local conditions
   - mandate that all public sector agencies adopt the whole-of-government information security policies and standards
   - establish clear oversight to monitor implementation of information security policies and standards and compliance with the reporting requirements
   - establish a process to identify and communicate emerging information security risks to the sector.
2. All public sector agencies should assign responsibility for information security practices both to senior management, and to line management at appropriate levels throughout the organisation.

3 Culture, practice and technology

At a glance

Background

Securing information requires a balanced and integrated approach to people, process and technology. Senior management needs to understand and effectively manage information security risks in all agency business. We examined whether selected departments have established and comply with sound risk management and whether they are maintaining the integrity and confidentiality of citizens' personal information.

Findings

- There are two flaws in the application of the risk management framework:
  - Risks cannot be managed where agency management is not aware of, or does not understand, the significance of the risk.
  - Attestations about control and management of risk exposures, without evidence to verify the effectiveness of controls, are of no value.
- In each department unauthorised people could access personal information quickly and easily. The database controls were either missing or not operating.
- Because systems logs are either not maintained or not routinely reviewed, the departments cannot determine whether these systems had previously been breached and personal information accessed by unauthorised parties or stolen.
- Personal information is being stored and exchanged in unsecured formats.
- Third parties to whom personal information is provided are not required to certify that their security arrangements at least equal public sector requirements.

Recommendations

To protect personal information each public sector agency should:

- develop more robust risk management practices
- include the importance of and threats to information security in staff training
- monitor compliance with information security policies, standards and practices
- identify and classify all information they capture, and establish controls
- assess and act on the threats and vulnerabilities to their ICT systems
- monitor logs and records of access and changes to information
- establish minimum standards of security for information handled by third parties and require certification of compliance with the standards
- conduct random checks of controls in place at third party service providers.

3.1 Introduction

Securing information, including personal information, requires a balanced and integrated approach to people, process and technology.

Information-security risks need to be understood by senior management. This understanding should translate into assessing the level of risk and effectively managing security threats throughout the organisation. Employees and other authorised users of information, such as the third parties that agencies do business with, need to be aware of risks to personal information and schooled in how to effectively manage them.

Information handling processes—including at the front counter, in administrative areas, in databases, filing systems, and in exchanges via email and portable electronic devices—need to be designed and operate so that the integrity and confidentiality of information is maintained.

Standards and procedures to guide work practices need to be in place; and databases and other technology need to have controls that protect vulnerable parts of the business against threats to security.

In this chapter we examine whether:

- selected departments have, through their risk management, established and comply with sound practices to protect the confidentiality, and integrity of, and access to, personal information
- the integrity and confidentiality of personal data has been maintained in practice.

3.2 Risk management

All public sector agencies are required to manage their risks within the Victorian Government Risk Management Framework. The framework requires chief executive officers and departmental secretaries to attest each year that a system of internal controls is in place to enable the executive to understand, manage and satisfactorily control risk exposures. A responsible body or audit committee is to verify the attestation.

3.2.1 Risk management practice in departments

We examined risk management practice within three departments to determine how well they were managing risks to information security. In each case we found that the attestation under the Victorian Government Risk Management Framework was not based on any substantiation that identified risks had been mitigated.

We also found that:

- In one department, senior management had recently identified information security as an important risk needing to be managed and established an information security governance committee. The risk previously had not been a strategic priority for action at the whole-of-department level. Periodic assessments of information security risks had not been conducted across the department. Information security risks were not consistently managed throughout the department.
- In another department, the concept of information security risk was understood at senior levels and identified as a strategic risk in its risk register. However, the threats to information security within the department's business environment were not understood: a significant risk to a major information database was unknown. Information security risks to the selected database were not assessed or documented. A lack of communication and coordination between the IT technical area and the managers of the database had contributed to the risk.
- In the third, information security was recognised as a strategic risk to the department and appeared in its strategic risk register. However, threats identified in the risk register for the system we audited were not based on a recognised framework such as the international ICT security standard, and risks and threat analysis of databases were not regularly conducted by the department.

In one department, threats to and vulnerabilities of the computer information systems and networks were well understood by staff within the information technology section, but advice of these had not been communicated to senior management to enable their management. In the other departments, business units were aware of risks inherent in the personal information they handled, but the risks were not uniformly managed across the department.

We concluded that the application of the risk management framework within the three departments was ineffective and that information security risks were not being effectively managed. Results of our testing, outlined later in this chapter, proved this.

3.2.2 Flaws in applying the risk management framework

Our observations reflect two fundamental flaws in the application of the risk management framework:

- risks are not identified or managed where an agency management is not aware of, or does not understand, the significance of the risk
- attestations about the control and management of risk exposures, made without evidence that substantiates the effectiveness of controls, are of no value.

The framework recognises that '… under the *Information Privacy Act 2000*, the Government has a requirement to actively manage the risk of breaches to a citizen's privacy'. It also states that 'The Government Services Group (GSG) provides services aimed at a more integrated government focus on information and communication technology'. It refers agencies to further information on relevant policies and standards at the DTF website.

Our findings about the deficiencies in information security policies and guidance currently available to agencies; and the way in which risk management is being implemented and the quality of practices and controls in place within departments, prove the need for greater guidance across the sector is urgent.

3.3 People: culture

An agency's information security is only as strong as its business environment's weakest link. Experience shows that organisations lose more sensitive information from human error than as a result of poor ICT controls. Human error can include loss of laptops, portable storage devices and hardcopy documents; misdirection of emails; working on laptops or documents where content can be viewed by others; talking about business or classified matters with, or in front of, people who have no need to know; failing to follow workplace physical security arrangements; disposing of documents in the general rubbish; and leaving computers, screens or documents unsecured on desks. Culture is therefore a critical part of an agency's information security environment.

We looked at the level of awareness of the need for information security throughout the three departments: that is, whether there is a culture of information security. Training is important to establishing and maintaining awareness, so we examined the content of information security training in the departments.

Senior management in the three departments now recognise how significant the risks to their information security are. But we found that information security awareness is not uniform across or within the three departments. One department has a high level of awareness about privacy, another of fraud prevention.

To some extent the cultural difference is due to the different nature of their businesses, or the focus put on information security within individual business units or regions. However, it is also an indication of the different levels of awareness, or misconceptions about privacy and information security, and what and where the risks are.

All three departments have worked to strengthen the awareness of their staff of information security. The quality of information security content in training programs in the three departments varied and improvements are needed in all. One department's training program addresses protecting information and contributes to creating awareness by promoting a culture of security as well as privacy. The program gives staff the tools and resources they need to meet their information security obligations.

Effort to embed an information security culture in all public sector agencies needs to continue. It should include a focus on developing understanding that information security is not only a technology-based activity, but also includes effective management of the security of hardcopy records; limiting opportunities for inadvertent sharing of information within the workplace, or in public areas; and maintaining physical security in workplaces.

These efforts should be supported by the development and delivery of training covering information security priorities and better practice for both electronic and hardcopy records. The training needs to be delivered regularly and the level of training attendance and staff awareness of security practices monitored.

3.4 Process: work practices

All three departments apply risk management to their processes and work practices. However, we found significant deficiencies that were, for the most part, common across the three departments.

3.4.1 Classifying and protecting personal information

While some records had been categorised, all three departments lacked appropriate information security classification schemes.

Only one department had undertaken a systematic review to identify all the information it stores, processes and communicates. None had conducted an assessment of the criticality of its information so that they could appropriately classify it and determine the minimum controls needed to protect it.

One department had set up controls within its records management system, but the controls needed to restrict access to sensitive and personal information held outside the records management system, for example, on departmental networks or in hardcopy records, had not been defined.

Without a complete and accurate information inventory or a classification system, departments could not provide assurance that their information assets were secure or that appropriate practices were in place for staff to manage the information.

3.4.2 Storing personal information

We looked at the way information is stored. We selected one significant database within each of the three departments and assessed whether and how staff stored personal information outside the database.

Personal information from each database was stored in places that were not secure, or exchanged in formats that were not secure. For instance, we found personal information:

- In shared drives freely accessible to others within departments. In one department we identified over 5 500 documents containing personal information on shared network drives.
- In staff personal folders. In one department we found around 5 000 documents containing personal information in staff folders on networks.
- Copied outside the secure database to a less secure test area on the network.
- Stored on portable storage devices, CDs and DVDs that are vulnerable to loss, in formats that were easily read by anyone who found or received the device.

Compliance by staff with information security requirements was not monitored by any of the three departments.

3.4.3 Sharing personal information

All three departments share personal information within the organisation, or with third parties including other jurisdictions, as part of their normal business activities. Third parties may include non-government organisations that provide services on their behalf, other departments or government agencies that use the information for investigations, planning or the provision of services, or ICT companies that provide information technology services for the departments or host departmental data on their sites or hardware.

The audit examined how the three departments share information in the course of daily business and found personal information transferred by emails in easily read form. If misdirected, this information could be easily read by someone other than the intended recipient. In one department in a selection of emails, we identified around 600 emails and attachments sent outside the department that contained confidential information in an easily read form.

The audit found personal information sent to staff or third parties, including business partners, at personal email accounts or web mail accounts such as yahoo and hotmail in easily read form. Some of these accounts are particularly vulnerable to unauthorised access or to practices of unscrupulous people who encourage sharing of access details by unsuspecting account holders.

We also found personal information emailed, faxed or mailed to other government agencies without appropriate arrangements being established. One department had protocols for sharing confidential and sensitive information. The protocols stressed the protection of personal information and identify. However, they did not set out the information security controls needed to protect the information shared. For example, they did not address the security classification of the data, appropriate controls to securely exchange and store the information, or the audit trails needed to provide assurance that access to the information was controlled.

Sharing with funded non-government organisations

For one of the databases selected, we examined its use by four non-government organisations that legitimately access and share the information held by or collected on behalf of the related department. The ability of these organisations to protect personal information varied. We found both good and bad practice. In particular, we found:

- Only two of the four had policies consistent with the department's mandatory requirements or with its requirements that non-government organisation policies be based on specified information security standards.
- None of the four had performed a threat and risk assessment against the information security standards or assessed their compliance with the department's information security policy.
- Non-compliance with the department's security policies, including:
  - poor physical security, for example, computer servers containing an organisation's data located behind the front reception desk in a non-secure area
  - poor password management, with passwords not changed regularly. Some staff had not changed their passwords for over two years
  - no minimum level of security such as a definition and mandatory use of antivirus software for home or remote access
  - 'protected' data held offsite in a home office.

While the three departments require third parties to have systems or records management arrangements with security equal to the public sector requirements, they do not require them to provide independent certification that their security meets the standards, or conduct checks to gain this assurance.

In some cases, departments share information with large numbers of third parties and because of the number of parties, it can be difficult to ensure adequate information security is in place in each. Nevertheless, accountability for the expenditure of public moneys within the Victorian public sector rests with departmental secretaries. It is their responsibility and in their interest to establish adequate arrangements to satisfy themselves that the risks of providing citizens' personal information to third parties are effectively managed.

Sharing with ICT service providers or hosts

All three departments use ICT service providers to provide IT infrastructure facilities management and hosting services. One department has not finalised a service level agreement with its ICT service provider. Without such an agreement, the department is not able to enforce performance standards or security standards of the ICT provider.

The other two departments have agreements in place but there was scope for improvement. The agreements do not address the controls needed to protect information; are not clear on the classification of the information being protected, the controls needed to securely exchange and store information, or audit trails to provide evidence that access to the information has been controlled.

As is the case for funded external service delivery agencies, the ICT service providers are not required to provide independent certification that their security meets the standards, and the departments do not conduct checks to gain this assurance.

3.5 Technology: ICT systems controls

We assessed the computer controls over the personal information stored within the three selected databases. We identified likely threats to the integrity and confidentiality of the databases and attempted to take advantage of the weaknesses identified from our risk assessment.

We were able to break into databases and access personal information from within departmental networks because of weak or missing controls. For one department, sensitive information about the technology used to support the system was publicly available. We were able to use this public information to break into the database from within the department's network.

We found examples where the databases or associated systems or networks:

- were at significant risk of being broken into by unauthorised parties and personal information accessed because the security at their boundaries was not sufficient
- could be accessed from any location, and from any device such as web browsers, personal digital assistants and smart-phones. This is a significant exposure for the department and risk to the confidentiality and integrity of the system. It can give an attacker, either from inside or outside the department, full control of all functions of the system and the personal information in it.
- had not been updated to address or 'patch' known security weaknesses, in two departments. This left the systems open to exploitation by individuals who knew of the vulnerabilities of the systems.
- had poor password controls, in two departments. In one, the passwords were easy to guess and there were no restrictions on the number of logins allowed on the system, with the same password, at the same time. In the other, we were able to access the system using a default password most likely created and unaltered at the time the system was installed.

In two departments, we found entire databases containing personal information copied outside the database to a less secure test area. The controls in place over the test environment were not sufficient, and increased the risk of loss of confidentiality of the information.

In one department there were a number of viruses on the network. At the time, the department was not aware of the viruses. Viruses can threaten the confidentiality of personal information and affect the availability of a network and system. Depending on the virus, it may also be spread unknowingly by email or USB keys, infecting systems of other departments, agencies or third parties.

In another, the network structure does not segregate systems that contain data of different criticality or sensitivity. Breaking through the controls into one system on the internal network may allow an attacker to access other internal systems and access information that should not be accessed.

Departments could not identify recent changes to data within databases or who had accessed them, either because they did not log access and changes to systems and networks; or because they did not routinely review logs before they were overwritten. These control weaknesses also meant that the departments could not tell whether the systems had been accessed or information changed by unauthorised persons, that is, people who had no right or need to access or change the information. In one case a lack of control meant there was a high risk that records could be deleted without management being aware whether the deletions were valid.

Most seriously, two departments had not routinely tested whether their databases or networks could be broken into by parties outside the department or from other parts of the organisation.

3.6 Conclusions

In each department we proved that the personal information stored in the selected databases could be accessed by unauthorised people, quickly and easily from within the network. The necessary controls were either missing or were not operating as required.

We identified that databases, and networks were at risk of being broken into by unauthorised parties, either from inside or outside the department, and personal information accessed because the security at their boundaries was not sufficient.

We also proved that data was transmitted from the departments by emails in easily read form and was not being adequately protected by third parties to whom the information was legitimately provided.

The combination of poor logging practice and weaknesses in access controls means that departments were not able to provide assurance that the integrity of the information in their databases had not been compromised.

As a result of our audit, the risks to personal information have been elevated to senior management. All three departments apply a risk management framework across their business activities, but our audit shows that the management of information security risks remains inadequate.

Weaknesses in information security controls threaten the confidentiality and integrity of personal information held, used and shared by the departments. These weaknesses mean that departmental systems and information are vulnerable to attack.

During the audit, each of the three departments has acted to improve security over the databases we examined and to enhance their information security. However, until a strong information security culture, proper practice and effective controls are in place across the sector, the integrity and confidentiality of citizens' personal information remains at risk.

Recommendations

3. To adequately protect the integrity and confidentiality of citizens' personal information each public sector agency should:
   - Develop more robust risk management practices, which demonstrate that annual risk attestations are based on substantiated evidence that information controls are effectively addressing risks.
   - Include in staff training, the importance of information security; the range of threats to information security and the vulnerabilities of electronic and hardcopy records and physical security in workplaces.
   - Regularly monitor compliance by staff with information security policies, standards and required practices.
   - Conduct an inventory of all the information they store, process and communicate, assess its criticality, classify the information; and determine, and put in place, the minimum controls needed to protect it.
   - Assess the threats and vulnerabilities, both internal and external, to their ICT systems, implement appropriate controls to address them and regularly monitor that the controls are in place and operating as required.
   - Regularly monitor logs and records of access and changes to information.
   - Establish agreements with third party service providers to clearly specify minimum standards of security over information handled, at least equal to those required of the public sector, and that provide for regular certification of compliance with the standards.
   - Conduct periodic random checks of the controls in place at third party service providers over citizens' personal information.

Auditor-General's reports

Reports tabled during 2009–10

Report title	**Date tabled**
Local Government: Results of the 2008–09 Audits (2009–10:1)	November 2009
Public Hospitals: Results of the 2008–09 Audits (2009–10:2)	November 2009
Towards a 'smart grid'—*the roll-out of Advanced Metering Infrastructure* (2009–10:3)	November 2009
Responding to Mental Health Crises in the Community (2009–10:4)	November 2009
Management of the Community Support Fund (2009–10:5)	November 2009
Auditor-General's Report on the Annual Financial Report of the State of Victoria, 2008–09 (2009–10:6)	November 2009
Water Entities: Results of the 2008–09 Audits (2009–10:7)	November 2009

VAGO's website at <www.audit.vic.gov.au> contains a comprehensive list of all reports issued by the Office. The full text of the reports issued is available at the website.

VAGO

Victorian Auditor-General's Office

Auditing in the Public Interest

Availability of reports

Copies of all reports issued by the Victorian Auditor-General's Office are available from:

- Information Victoria Bookshop
  505 Little Collins Street
  Melbourne Vic. 3000
  AUSTRALIA

  Phone: 1300 366 356 (local call cost)
  Fax: +61 3 9603 9920
  Email: <bookshop@dvc.vic.gov.au>

- Victorian Auditor-General's Office
  Level 24, 35 Collins Street
  Melbourne Vic. 3000
  AUSTRALIA

  Phone: +61 3 8601 7000
  Fax: +61 3 8601 7010
  Email: <comments@audit.vic.gov.au>
  Website: <www.audit.vic.gov.au>