CLOUD COMPUTING IN THE VICTORIAN PUBLIC SECTOR

Discussion Paper

State Government Victoria

Commissioner for Privacy and Data Protection

Cloud Computing in the Victorian Public Sector

Discussion Paper

Commissioner for Privacy and Data Protection

Document Details

Document Details	
Security Classification	UNCLASSIFIED
Version	25
Issue Date	5 May 2015
Document Status	Draft
Authority	Commissioner for Privacy and Data Protection

Contents

This page is intentionally left blank

Preface

> Ultimately, you can outsource responsibility but you can't outsource accountability.
>
> European Network and Information Security Agency (ENISA)
> *Cloud Computing: Benefits, Risks and Recommendations for Information Security*

This Cloud Computing Guide provides an overview of cloud computing in the context of Victorian public sector agencies' information management obligations under two pieces of legislation: the *Public Records Act 1973* (PRA) and the *Privacy and Data Protection Act 2014* (PDPA).[1]

It aims to provide an overview of cloud computing that is relevant to a wide range of public sector managers working in various roles across government. In doing so, it addresses such questions as: What is cloud computing? What benefits and opportunities does it offer? What new risks does it pose? How should it be assessed in terms of recordkeeping, privacy and protective security requirements?

While there is, if anything, a surfeit of publications about cloud computing, the information available is not always consistent or directly relevant to Victoria, and its sheer volume is more likely to overwhelm or confuse than help. Likewise, cloud computing continues to raise controversy – particularly in a privacy context – suggesting that further work is required to clarify – or perhaps demystify – certain of its aspects.

We are aware that there is a perception that agencies require more practical advice about how to address key recordkeeping, privacy and protective security requirements when they assess potential cloud computing solutions and – if it is decided to adopt cloud computing – how to go about ensuring that those requirements are (proactively) built into the arrangement.

The Public Record Office Victoria (PROV) and the (then) Office of the Victorian Privacy Commissioner (OVPC) have both published cloud-computing guidance materials previously. However, with the commencement of the PDPA in 2014 – which incorporates a new regulatory focus upon protective security – it seems timely to revisit the topic of cloud computing, looking at recordkeeping, privacy and security requirements in a more coordinated way.

Consistent with past advice, this guide recommends that agencies incorporate consideration of recordkeeping, privacy and security requirements into their *risk assessment* of cloud computing. It identifies methodologies, checklists and other resources to help achieve this goal. The guide seeks to *highlight areas of commonality* across the individual domains of privacy, recordkeeping and protective security while, at the same time, recognising the need for accurate use of domain-specific definitions and terminology. Overall, this is intended to foster a more holistic and coordinated approach to compliance with recordkeeping, privacy and information security obligations across the Victorian public sector.

As with any other approach adopted by agencies, the use of cloud computing must be consistent with Victorian legislative requirements, including any mandatory standards or policies. In the end, it is simply not possible to contract out of public sector accountability.

Justine Heazlewood
Director & Keeper of Public Records

David Watts
Commissioner for Privacy & Data Protection

1 This guide is not intended to provide specific advice in relation to health information, which is regulated under the *Health Records Act 2002* (Vic) (HRA), nor will the PDPA's protective security framework apply to health services. Where directly relevant, the HRA is discussed in the guide and many of the findings contained in this report are equally applicable to the HRA.

1 Introduction

Cloud computing is one of a number of ways to deliver IT services, software and infrastructure. It is not a new technology, *per se*, but rather a new business model in which third party providers supply a range of computing components to clients using the Internet as the delivery mechanism.[2]

As these computing components can be bundled in numerous ways, it is difficult to reduce 'cloud computing' to a simple definition or model. Indeed, 'cloud computing' is better understood as an umbrella term or collective phrase for various permutations and combinations of cloud computing provider(s) and computing 'components'.

In practical terms, this signals the importance of understanding exactly what a particular cloud solution consists of and how it will operate in relation to public sector agencies' legal compliance requirements.

'Cloud computing' is an umbrella term that resists reduction to a simple definition or model. Thus, while it is relatively easy to provide general advice in relation to cloud computing, in order to obtain specific and detailed advice about a particular cloud-based initiative or program, agencies need to undertake a comprehensive assessment process.

As a starting point, cloud computing raises *a number of the same issues and risks* for the public sector as those that arose when the outsourcing of IT services became widespread or when Internet-based services were first developed. As a result, some cloud computing issues and risks can be managed effectively within the parameters of solutions developed for outsourcing or the Internet. Where these are currently understood and managed effectively by the public sector, they are not discussed in detail in this guide.

On the other hand, cloud computing also presents *a number of new issues and risks* that public sector agencies need to take into account when considering the adoption of cloud computing.

There are a number of other legal and regulatory considerations to take into account when undertaking a detailed assessment of cloud computing; these are not the primary focus of this guide.

This guide seeks to summarise the key benefits, issues and risks relating to the adoption of cloud computing within the context of Victoria's *recordkeeping, privacy and protective security* regulatory framework. On the whole, this guide is concerned with the specific requirements prescribed by the following laws:

- *Privacy and Data Protection Act 2014* (Vic) (PDPA)
- *Public Records Act 1973* (Vic) (PRA)

This guide also includes reference to 'health information', which is covered by the *Health Records Act 2001* (Vic) (HRA) in Victoria. While health information is covered under separate legislation, many of the findings and recommendations contained in this guide are broadly applicable to the HRA.

These laws and the information management obligations they impose on public sector agencies are important – they provide the framework for the protection and effective management of government information, public records and personal information (including health and sensitive information). Equally important, these laws are not prescriptive; in order to achieve

2 ENISA, *Cloud Computing: Benefits, Risks and Recommendations for Information Security* (November 2009), p.10.

their objectives, they require the application of principles or standards to a particular fact situation or context.

As principle or standards-based legislation, the PRA, PDPA and HRA are not prescriptive; *they need to be applied* to a given fact situation or context.

Thus, the legislative requirements embodied in the PDPA and PRA (and the HRA) cannot be simply 'pasted on' to cloud computing; they need to be assessed against the specific details of a cloud computing proposal or initiative. In turn, this requires analysis – a thinking process – before informed decision-making can take place.

Sometimes, the requirements contained in these laws may be 'non-negotiable' in a cloud-computing context – that is, if a cloud computing provider or service cannot comply with baseline regulatory requirements, it is not an appropriate option for a public sector agency. At other times, public sector agencies will need to undertake a formal assessment of the potential benefits of a cloud-computing proposal, versus its legal and regulatory risks, in order to identify whether or not it is appropriate.

General information about cloud computing and its benefits and risks is unable to provide the level of detail required by an agency to determine whether or not a cloud solution is appropriate. This is why, so often, it is recommended that agencies undertake a risk assessment process in order to make an informed decision about a specific cloud-computing proposal.

In order to obtain an effective view of recordkeeping, privacy and protective security requirements these requirements must be built into the overarching risk assessment process. Where it is practicable to do so, recordkeeping, privacy and protective security requirements should be embodied in the main risk assessment process; they should not be assessed in isolation or treated as distinct or separate issues as this may distort the findings of the risk assessment process or fail to address requirements at the appropriate point of the development cycle.

Ensure risk assessment processes incorporate recordkeeping, privacy and protective security requirements *as a default measure*. Use, adjust or update existing risk assessment frameworks wherever possible, to ensure continuity and build upon existing internal knowledge.

It is inevitable that Victorian public sector agencies will adopt – or have already adopted – cloud computing in some shape or form. This guide makes the point that when this happens it needs to occur in a transparent and accountable way:

- Informed by an appropriate risk assessment process (i.e. one that incorporates an effective review of recordkeeping, privacy and information security requirements); and
- Subject to effective decision-making and oversight (i.e. a process in which 'the cloud' is neither embraced uncritically nor demonised).

Wherever possible, existing risk assessment frameworks should be used, along with any other relevant in-house methodologies, tools and guidelines. See, for example, Standing Direction 4.5.5 of the Minister for Finance under the *Financial Management Act 1994* (Vic)[3], the Victorian Government Risk Management Framework (VGRMF)[4], the PROV Cloud Computing Policy and

3 Minister for Finance, *Standing Direction 4.5.5 – Risk Management Compliance*, Standing Directions of the Minister for Finance under the *Financial Management Act 2004* (updated, July 2014).

4 Department of Treasury and Finance, *Victorian Government Risk Management Framework (VGRMF)*, (March 2011). See also, VMIA, *Risk Management Guide* (April 2014).

associated Guidelines[5] and the PIA Guide published by the (then) OVPC.[6] So too, the CPDP's endorsed approach to privacy management – *Privacy by Design* – is highly relevant to this guide.[7] (This topic is discussed in further detail in Chapters 4 and 5, below.)

Finally, this guide promotes the need for a *shared understanding* of the meaning of terms and definitions associated with cloud computing as well as the terms and definitions found in legislation relating to recordkeeping, information privacy and protective security as any lack of clarity regarding definitions and terminology is a risk in itself.

In some cases, the same or similar words may be used across the three domains of privacy, protective security and recordkeeping, but they do not necessarily have the same meaning. In others, legislative definitions should provide the basis for discussion, but profession-specific terms are used instead, potentially leading to misinterpretation or confusion. In order for agencies to undertake effective risk assessments of, or to discriminate between, the many different cloud services and providers on offer, it is critical that any potential for misunderstanding is minimised, if not removed altogether.

A glossary of terms and acronyms used in this guide is provided at Appendix A.

Summary of Findings

'Cloud computing' is an umbrella term rather than a specific definition. It must be looked at in context in order to be meaningful.

Currently, whenever agencies are considering a new cloud computing initiative or reviewing an existing cloud-based arrangement they are required to undertake an appropriate risk assessment process using the VGRMF. This guide recommends that, as far as possible, the risk assessment process should incorporate recordkeeping, privacy and protective security requirements as a core component of the process.

Public sector agencies are advised to take account of the approach outlined in Privacy by Design, which is also applicable to information security.

Agencies should take steps to ensure that the correct definitions and terminology for recordkeeping, privacy and protective security are used in risk assessment processes and that they are applied accurately and meaningfully. Where legislative definitions are available, these should be used in preference to professional terminology.

5 PROV, *Cloud Computing Policy, Cloud Computing Guideline 1: Cloud Computing Decision Making and Cloud Computing Guideline 2: Cloud Computing Tools* (2013).

6 OVPC, *Privacy Impact Assessments Guide* (April 2009).

7 OVPC, *Privacy by Design press release* (May 2014); Privacy by Design <privacybydesign.ca>

2 Overview of Cloud Computing

2.1 What is Cloud Computing?

In a cloud computing context, 'cloud' is a metaphor for the Internet, with 'cloud computing' used to describe the way various computing components – such as networks, servers, storage facilities, services and applications – are supplied to an organisation by a cloud provider, or providers, via the Internet. In turn, an organisation does not have to deploy its own networks, servers, storage centres and/or applications if cloud computing is utilised.

2.2 Defining Cloud Computing

The term 'cloud computing' is not subject to a single, authoritative definition. The fact that there is no universally agreed, standards-based definition of cloud computing, means that it is possible for 'the cloud' – and its related terminology – to be subject to multiple interpretations and potential misunderstandings, including what 'it' comprises and whether, and to what degree, it reproduces or differs from conventional IT models.[8]

This guide uses and recommends the NIST definition of 'cloud computing' as it is the best-known and most commonly accepted definition.

For clarity, this guide adopts the definition developed by the National Institute of Standards and Technology (NIST), as it provides the most commonly accepted definition of cloud computing.[9]

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of *five essential characteristics*, *three service models*, and *four deployment models*.[10]

In summary, NIST characterises the five essential characteristics of cloud computing as IT services that:

- Are ***broadly accessible*** (i.e. can potentially be accessed from anywhere with nothing more than an Internet connection and browser);
- Provide ***rapid elasticity*** (i.e. can be scaled up and down quickly in terms of capacity, numbers of users, etc.);
- Are charged on the basis of ***measured services*** (i.e. customers only pay for what they use and as they use it. This is often characterised as analogous to 'renting,' rather than 'buying');
- Provide ***on-demand, self-service*** (i.e. users can purchase, set up and self-manage services directly via automated, Internet-based portals); and
- Utilise ***resource pooling*** (i.e. underlying IT systems and resources are shared across many users and/or organisations, therefore enabling service providers to drive

8 While the International Standards Organisation (ISO) is still developing a cloud-specific standard, the first International Standard to focus on *the protection of personal information in the cloud* was published in August 2014 (ISO/IEC 27018:2014).

9 The NIST definition is used widely in Australia. For example, PROV adopted the NIST definition in its Cloud Computing Policy.

10 P Mell & T Grance, *The NIST Definition of Cloud Computing* (Special Publication 800-145), (October 2011) p.2.

economies of scale and avoid underutilisation of their capacity). This arrangement is also referred to as '***multi-tenancy***'.

See Figure 1, below, for a summary of the three service models associated with cloud computing according to NIST.

Cloud Computing: 3 Service Models
Software as a Service (SaaS) – the service provided to the customer is the ability to use the provider's application running on a cloud infrastructure. The applications are accessible from various client devices through, for example, a web browser (e.g. web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage or even individual application capabilities (with the possible exception of limited user-specific application configuration settings). • Services that would typically be used directly by end-users. Common SaaS offerings include Google Apps, Dropbox and Microsoft Office 365.
Platform as a Service (PaaS) – the service provided to the customer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services and tools supported by the provider. The customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems or storage but has control over the deployed applications and possible configuration settings for the application hosting environment. • Services that would typically be used by software developers to build or implement applications without them having to manage the underlying services. A common PaaS offering is Microsoft's Azure service.
Infrastructure as a Service (IaaS) – the service provided to the customer is to provide processing, storage, networks and other fundamental computing resources where the customer is able to deploy and run arbitrary software, which can include operating systems and applications. The customer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage and deployed applications and, possibly, limited control of select networking components (e.g. host firewalls). • Services that enable IT systems to be built and maintained without needing an on-premises data centre or physical IT hardware. Common IaaS providers include Amazon Web Services and Rackspace.

Figure 1 – Cloud Computing Service Models (NIST)

When the NIST definition refers to 'cloud infrastructure' in Figure 1, this describes the 'collection of hardware and software that enables the five essential characteristics of cloud computing.' 'Hardware' equates with the *physical layer* of the cloud infrastructure (e.g. server, storage and network components), which is required in order to support the provision of cloud services. 'Software' equates to the *abstraction layer*, in which software is deployed across the physical layer, which manifests the essential cloud characteristics.[11]

Each of these service models involves a different distribution of requirements, responsibilities and risks between the user of the service and the cloud service provider, which needs to be taken into account in any assessment of a cloud-computing proposal.[12]

11 P Mell & T Grance, *The NIST Definition of Cloud Computing* (October 2011), page 2, footnote 2.

12 CSCC, *Security for Cloud Computing: Ten Steps to Ensure Success, v.2.0* (March 2015), page 9.

For example, as outlined by the Cloud Standards Customer Council (CSCC), with IaaS, responsibility for basic IT resources (e.g. hardware and networks) lies with the contracted servicer provider while the service user is responsible for the operating system, the software required to run applications and the data entered into the cloud environment.[13] The service user is thus responsible for securing the applications and the data therein. On the other hand, with SaaS, responsibility for the infrastructure, software and data lies primarily with the cloud service provider as the service user has little or no control over their management (although this does not mean that the user has no responsibilities).[14]

As summarised in Figure 2, below, the four deployment models associated with the NIST definition of cloud computing comprise the following.[15]

Cloud Computing: 4 Deployment Models
Private Cloud – the cloud infrastructure is provisioned for exclusive use by a single organisation comprising multiple users (e.g. business unites) within a private network. It may be owned, managed and operated by the organisation, a third party or some combination of these. It may exist on or off premises.
Community Cloud – the cloud infrastructure is provisioned for exclusive use by a specific community of users from organisations that have certain elements common (e.g. mission, security requirements, policy and/or compliance concerns). It may be owned, managed and operated by one or more of the organisations in the community, a third party or some combination of them. It may exist on or off premises.
Public Cloud – the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed and operated by a business, academic or government organisation or some combination of them. It exists on the premises of the cloud provider.
Hybrid Cloud – the cloud infrastructure is a combination of a public cloud provider (e.g. Amazon Web Services or Google Cloud) with a private or community cloud platform. While operating independently, they can communicate with each other over an encrypted connection using technology that allows for the portability of data and applications.

Figure 2 – Cloud Computing Deployment Models (NIST)

The risks and benefits associated with each deployment model differ depending on the circumstances, with the commodity, cost, liability and assurance associated with each deployment model varying in scale depending on whether it is a public, private, community or non-cloud model (See Figure 3, below).[16] There is one element that remains fixed, whatever model is used: public sector accountability.

13 CSCC, *Security for Cloud Computing: Ten Steps to Ensure Success, v.2.0* (March 2015), page 9.

14 CSCC, *Security for Cloud Computing: Ten Steps to Ensure Success, v.2.0* (March 2015), page 9.

15 Figure 2 is derived from P Mell & T Grance, *The NIST Definition of Cloud Computing* (October 2011), page 2, with additional text on the 'hybrid cloud' drawn from ZedNet, 'Hybrid cloud: What it is, why it matters', 1 July 2014.

16 This illustration is based upon one developed by ENISA, *Cloud Computing: Benefits, Risks and Recommendations for Information Security* (November 2009), p.16, updated to incorporate an additional element: 'accountability'.

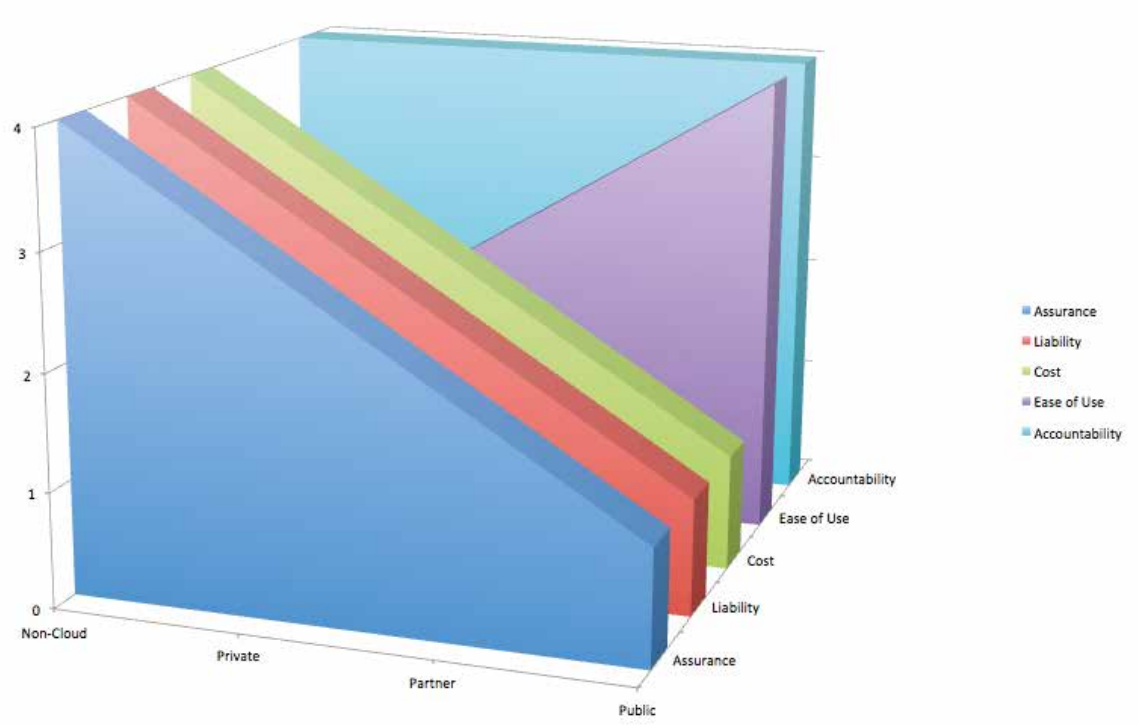


Figure 3 – Comparison of Deployment Models

This reflects the fact that the economies of scale provided by public cloud services may *deliver* the lowest cost, but that low levels of assurance and liability are also part of the bargain.[17] It also helps to explain why public clouds tend to be based upon fixed term contracts and standardisation of service.[18] In other words, you get what you pay for.

In this context, it may be unrealistic to expect that a cloud service provider will amend its standard form contract to incorporate additional Victorian legal requirements (e.g. to match those associated with a private cloud model) without the need for additional negotiation and, most likely, charging extra.

This suggests that care is required when identifying a cloud computing provider as the cheapest and easiest solution may not be appropriate, particularly where the public sector agency is responsible for the management of personal information (including sensitive or health information). Low cost, speed to market and scalability are no longer key benefits if the wrong information is sent to a cloud service.

The old adage, 'you get what you pay for', is relevant in a cloud-computing context. A particular cloud service may be low cost, but it may not provide the full range of protections required for handling government data. Without undertaking an appropriate risk assessment prior to procurement, it may end up costing a lot more than first envisaged.

17 ENISA, *Cloud Computing: Benefits, Risks and Recommendations for Information Security* (November 2009), p.83.

18 ENISA, *Cloud Computing: Benefits, Risks and Recommendations for Information Security* (November 2009), p.98.

2.2.1 Caveat

As the NIST definition of cloud computing is close to ubiquitous, it provides a useful tool to identify and describe a range of cloud-computing services and deployment models. However, not all cloud service providers subscribe to the NIST definition, which is particularly confusing when the same terminology may be used with different meanings (e.g. a reference to 'the cloud' or '… as a service').

This may lead to the assumption that the offerings of different cloud providers are equivalent (because the same terminology is used), particularly in terms of data protection features and other protective security controls. If not identified early enough, such assumptions may result in the need to 'add on' further services or controls in the future in order to meet critical public sector requirements. If a contract has already been executed, remedying this situation will increase both the complexity and cost of the service.

As part of the risk assessment process, it is important to verify precisely what a particular cloud service offering includes so that accurate comparisons can be made across various cloud service providers and between the public sector and the cloud provider.

2.3 Cloud Computing and Related Technologies

The term 'cloud' often encompasses other related or intermingled technologies. Common examples include mobile devices (e.g. iPads, Android phones etc.), websites or 'virtualisation' tools. While many of these technologies may be used to access or even support the existence of cloud computing, they are not necessarily examples of cloud computing under the NIST definition.

However, while a particular technology or tool may not meet the NIST definition of cloud, it may possess some of the same characteristics and, therefore, some of the same implications, risks or other considerations. Public sector managers may need to take this into account as part of their risk assessment process.

Key Findings

The NIST definition of cloud computing provides the most widely used and accepted definition of cloud computing. It should be adopted in Victoria in order to maximise consistency and clarity, with its terminology used in relation to any risk assessment of cloud computing providers, services and deployment models.

Expectations regarding cloud-computing benefits must be assessed against the reality of what is on offer. It is unrealistic to expect a public cloud service to alter standard terms and conditions in order to meet public sector requirements without paying extra (you get what you pay for).

A formal risk assessment is required to determine the differential impact of the various models of service and deployment upon information security, privacy and recordkeeping requirements.

3 Cloud Computing Benefits and Risks

3.1 Opportunities and Benefits

There is no doubt that cloud computing has the potential to deliver major benefits and opportunities, including:

- ***Enhanced collaboration*** resulting from easier and more effective sharing of information and systems within and across organisational boundaries, leading to more ***efficient and rapid innovation***;
- Greater ***business agility and flexibility*** through an improved ability to ***rapidly establish and scale*** systems and services to meet changing demands;
- ***Cost reduction*** opportunities through more ***optimal and efficient*** use of computing resources; and
- Improved ***resilience and availability*** of systems and services through ready and affordable access to ***higher grade IT facilities, backup, and redundancy***.

3.2 Altering the Risk Landscape

Just as clearly, the introduction of cloud computing has changed the nature of some of the risks facing agencies when they seek to outsource or assign their functions and activities to the cloud.

One of the reasons cloud computing is seen to be changing the way IT services are delivered and consumed throughout the world is that it blurs many previously extant technological boundaries, such as individual-to-organisation, organisation-to-organisation, and geography-to-geography. One of the effects of this 'blurring' is that it may not be apparent where information is being stored or processed or who has control over it. This is an example of cloud computing altering the risk landscape.

Many individuals worldwide have joined 'free' cloud services in order to obtain a benefit (e.g. email services, Facebook, etc.), although the number of individuals who understand what this means in terms of associated risks – such as how their personal information is used, where their data is stored and whether or not it is portable – is far fewer.

The situation is markedly different for public sector agencies. Before public sector agencies can utilise cloud services (or any other outsourced service, for that matter), they must identify and assess potential risks, including the likelihood of their occurrence and their degree of impact if they do occur. They also need to determine whether or not specific risks can be remediated or otherwise managed. Only then, can they make an informed decision about the adoption of a cloud solution.

In particular, public sector agencies must know where public sector data they are responsible for is being stored or processed (even if the answer is 'multiple locations') and who has control over it – both in terms of information management responsibilities and legal compliance. If a prospective cloud-based government initiative involves the creation of public records or the collection and handling of personal information, the agency must ensure that the initiative is capable of complying with all relevant recordkeeping, information privacy and security requirements – whether it is delivered directly by government (e.g. a department or agency), in partnership with a contracted service provider (e.g. department + cloud provider) or delivered entirely by an outsourced service provider (e.g. a cloud provider).

This is non-negotiable in terms of legal and contractual compliance, reputational risk and community expectations.

Risks and issues associated with cloud computing – a number of them new – may result in adverse impacts that could significantly diminish or even reverse the benefits of cloud computing unless they are identified and managed appropriately. The number of potential risks is not insignificant, including:

- ***Technical risks*** – e.g. exposure of user information to new security threats;
- ***Information management risks*** – e.g. a failure to provide appropriate governance, including effective oversight;
- ***Business operational risks*** – e.g. a lack of transparency in relation to information processing, a lack of access to audit trails, a loss of control over data in the event of system outages or security breaches;
- ***Financial risks*** – e.g. the unforeseen cost of remediating the cloud solution where it fails to provide relevant safeguards and mandatory legal requirements;
- ***Legal and regulatory compliance risks*** – e.g. a failure to cover relevant legal issues in the contract for services, privacy issues due to offshore processing of data, public records deleted without authority or not backed up; and
- ***Multi-tenancy risks*** – e.g. a service is termed a 'private cloud' but it is shared by multiple organisations (i.e. fits the NIST definition of a public cloud).

At the level of specific *information management risks* relating to privacy, protective security and recordkeeping, PROV produced the following list:[19]

- Data security and protection (encompassing a wide range of issues and risks)
- Information privacy (encompassing a wide range of issues and risks)
- Confidentiality (where relevant)
- Ability to execute authorised and complete destruction of data, and prevent unauthorised disposal
- The longevity of the systems within the cloud
- Data integrity and completeness, including maintenance of metadata
- Data authenticity and the ability to audit/demonstrate it
- Data availability (while within the cloud) and extractability and/or portability (if the service is discontinued).

Key Findings

The benefits of cloud computing have been established; the possible risks associated with cloud computing have not.

In a cloud computing context, the risk landscape includes existing and new or altered (cloud computing) risks.

In a cloud-computing context, all potential and/or actual information management risks need to be managed effectively.

19 Public Record Office Victoria (PROV), PROV Cloud Computing Guideline 1: Cloud Computing Decision Making (2013), p.5.

4 Risk Assessment: Preliminary Considerations

4.1 Background

All Victorian public sector organisations are required to comply with the PRA, the HRA and the privacy provisions of the PDPA.[20] The PDPA also includes provisions relating to protective security; these require the CPDP to develop a Victorian Protective Data Security Framework (VPDSF), including associated standards. Once developed and approved the VPDSF will apply to departments and a range of designated bodies, with a major exception in relation to health services as defined under the *Health Services Act 1988* (Vic), as they are not regulated under the PDPA.

The Australian Government's Protective Security Policy Framework (PSPF) provides the lead framework for protective security in Australia. The PSPF's focus upon international and national security requirements will have little – if any – practical impact upon the majority of the Victorian public sector. However, in terms of requirements relevant at the state level, such as the approach to classification and information security, the VPDSF will be consistent with the PSPF.

In the meantime, the requirement for agencies to use the Victorian Government Risk Management Framework (VGRMF) is binding and applies to a significant segment of the Victorian public sector (i.e. departments and agencies that report in the *Annual Financial Report for the State of Victoria*), with all other entities encouraged to adopt the VGRMF to enhance their risk management practices.[21]

Under the VGRMF, public sector agencies are required to implement and maintain a risk management framework. This framework may be leveraged and/or adapted to include specific consideration of the recordkeeping, privacy and protective security requirements discussed in this guide.

> The purpose of establishing an organisational risk management framework is to ensure that key risks are effectively identified and responded to in a manner that is appropriate to:
>
> - The nature of the risks faced by the organisation
> - The organisation's ability to accept and/or manage risk/s
> - The resources available to manage risks within the organisations
> - The organisation's culture.
>
> Ultimately risk needs to be managed so that the organisation maximises its ability to meet its strategic objective as well as associated operational targets and goals.
>
> VMIA, *Guide to Developing and Implementing a Risk Management Framework*, p.18

4.2 Overview

Agencies are routinely advised to undertake a risk assessment process in order to determine whether or not a cloud-computing proposal is appropriate. As a means of providing more practical advice about 'the how', rather than 'the what' of risk assessment, this chapter seeks

20 Further legislative references to privacy are found in Victoria's *Charter of Human Rights and Responsibilities Act 2006* (the Charter). While this guide focuses upon information privacy legal requirements, it may be necessary to consider the Charter in relation to any cloud-computing proposal impacting on individuals' privacy.

21 See, for example, Standing Direction 4.5.4 (Risk Management Compliance), *Standing Directions of the Minister for Finance under the Financial Management Act 1994* (Vic) (updated July 2014). See also, Department of Treasury and Finance: *Whole of Victorian Government Guidelines Information Security – Cloud Computing Security Considerations* [SEC/GUIDE/06] (January 2012).

to break down the tasks involved, with a particular focus upon the *preliminary steps* that need to occur before an effective risk assessment can be undertaken.

Looked at through the multiple lenses of recordkeeping, privacy and protective security, any assessment of cloud computing risks must identify and address the potential or actual risks posed by a cloud-computing proposal in relation to the PRA (including PROV Standards, Policies and Guidelines); the PDPA (including its ten IPPs); and the HRA (including its eleven HPPs).[22] In the future, designated public sector agencies will also need to comply with the VPDSF and its associated Standards (under the PDPA).[23] If these risks cannot be remediated or otherwise managed, the cloud computing solution is not appropriate.

As a starting point, it is necessary for agencies to determine whether or not the PRA, PDPA or HRA are applicable to a cloud-computing proposal and, if one or more is relevant, to identify the legal compliance requirements that come into play.

Looked at in practical terms, the following preliminary steps are required:

1. Identify the **public sector information** to be collected, transmitted, processed, stored or otherwise handled by the cloud-computing proposal.
2. Identify whether or not the **PDPA, HRA and/or PRA** apply to the cloud-computing proposal, using the information gathered in Step 1.
3. Identify the **legal compliance requirements** that need to be met by the cloud service provider *and/or* agency, using the information gathered in Step 2.

Once these three preliminary steps are complete, it is possible to undertake a risk assessment of the cloud-computing proposal (see Figure 3, below).

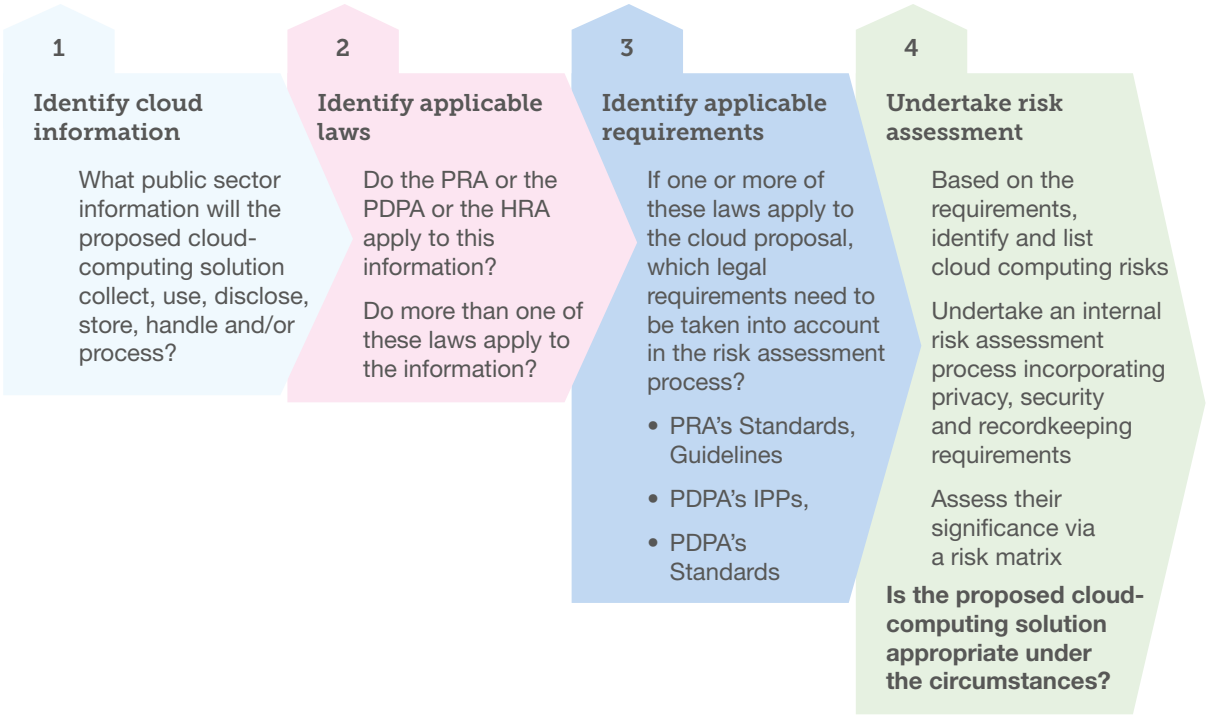


Figure 3 – Overview of Assessment Process

22 Further information about the PRA is available at: http://prov.vic.gov.au; the PDPA at http://www.cpdp.vic.gov.au; and the HRA at: http://www.health.vic.gov.au/hsc/.

23 Further information about the PDPA and protective security is available at: http://www.dataprotection.vic.gov.au.

4.2.1 Step One: Identify 'Cloud' Information

First, public sector agencies need to identify what public sector information will be 'sent' to the cloud. This information should be available in the business case proposal, business requirements document, information flows diagram or other preliminary documentation. If it is not available through these sources, it should be gathered from the project sponsor or equivalent as a matter of priority.

As far as possible, this information should be identified at a detailed level, preferably at the level of individual data fields, as this will enable the most accurate analysis to occur.

If it is not possible to identify/document this information, the proposal is not mature enough to proceed.

4.2.2 Step Two: Identify Applicable Laws

Agencies then need to assess whether or not the information identified in Step 1 is covered by the PRA, PDPA and HRA. In order to undertake this assessment effectively, it is necessary to have a broad familiarity with the key definitions and legislative frameworks embodied in the PRA, PDPA and/or HRA. A high-level understanding of the laws' objectives is also desirable. At this point of the process, it may be necessary to consult with relevant internal resources such as public records officers, lawyers, IT security managers or privacy officers.

The following diagram provides a high-level summary or overview of the PRA, PDPA and HRA (see Figure 4, below).

Recordkeeping

Public Records Act 1973

Established under the *Public Records Act 1973* (PRA), the Public Record Office Victoria (PROV) is responsible for:

- issuing **standards** regulating the creation, maintenance and security of public records, including the selection and disposal of public record not worthy of preservation
- **assisting** public officers to apply PROV Standards to records under their control
- **preserving** public records of permanent value as the state archives
- **ensuring** the archives are accessible to the Government and the people of Victoria.

A public record is defined to include:

- Any record made or received by a public officer in the course of his duties; and
- Any record made or received by a court or person acting judicially in Victoria.

Public sector agencies are required to adhere to records management standards and retention and disposal schedules issued by the Public Record Office of Victoria (PROV).

Information Privacy

Privacy & Data Protection Act 2014

In Victoria, the Privacy & Data Protection Act 2014 (PDPA) regulates the collection and handling of '**personal information**' and '**sensitive information**' by the public sector and its outsourced service providers.

'**Personal information**' is defined as:

> Information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained from the information or opinion.

'**Sensitive information**' is a subcategory of personal information, it is defined as including personal information about racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, trade union membership, sexual preferences or practices or criminal record.

Personal information, including sensitive information, must be collected and handled in accordance with 10 Information Privacy Principles (**IPPs**).

In light of its heightened sensitivity, the PDPA imposes **additional requirements** upon the collection of sensitive information.

Protective Security

Privacy & Data Protection Act 2014

In Victoria, the *Privacy & Data Protection Act 2014* (PDPA) requires the Commissioner for Privacy and Data Protection (CPDP) to develop a Victorian Protective Data Security Framework (VPDSF) and associated Standards for departments and designated bodies.

Both the framework and associated standards will draw upon the key elements of existing whole of Victorian government security policies and Australian and international security standards. It will be aligned with with the Australian Government Protective Security Policy Framework (PSPF).

The Victorian standards will depart from the PSPF in a number of ways designed to support State government service delivery functions and reflect contemporary security standards.

Once approved, agency Heads must ensure that agencies/bodies do not do anything to contravene a Victorian protective data security standard. These obligations will extend to contracted service providers.

Health services will not be covered by the VPDSF in the short term.

The development and implementation of the VPDSF will occur from 2014–2016.

Health Privacy

Health Records Act 2001

In Victoria, the *Health Records Act 2001* (HRA) regulates the collection and handling of '**health information**' by the public and private sectors.

'**Health information**' is a subcategory of personal information. It is defined as:

> Information or an opinion about the physical, mental or psychological health (at any time) of an individual; or … a health service provided, or to be provided, to an individual that is also personal information or other personal information collected to provide, or in providing, a health service.

'**Health service**' is defined as:

> An activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the organisation performing it to assess, maintain or improve the individual's health.

Health information must be collected and handled in accordance with 11 Health Privacy Principles (**HPPs**).

In light of its heightened sensitivity, the HRA imposes **additional requirements** upon the collection of health information.

Health services will not be covered by the VPDSF.

Figure 4 – Overview of Key Legislation

In particular, agencies need to identify whether a cloud-computing proposal involves:

- The collection and/or handling of *personal information* (including sensitive or health information) *contained in a record*;
- The creation or transmission of *public records*; or
- The need to apply *protective security* requirements under the VPDSF (or PSPF as adapted to Victoria until the VPDSF is issued).

Wherever possible, it is recommended that legal definitions be used in an assessment, rather than general or 'professional' terminology. For example, the PDPA contains a definition of 'personal information'. However, in a protective security context, 'personal information' is often described as 'Personally Identifying Information' or 'PII'. In an assessment of all three laws (PDPA, HRA, PRA), it is preferable to use 'personal information', as a legal definition takes precedence over a professional definition. It also helps to ensure clarity and consistency.

It is also useful to understand the degree to which the information identified in the first step may overlap in terms of its legislative status – e.g. a public record may contain personal information and, therefore, be subject to both the PRA and the PDPA's IPPs; and, if it is law enforcement data, it will also be subject to the PDPA's law enforcement data security standards.

Thus, while the PRA, PDPA and HRA are separate laws; the information or records to which they apply may overlap (see Figure 5, at right). Wherever possible, areas of overlap should be identified upfront as this has some capacity to streamline parts of the assessment.

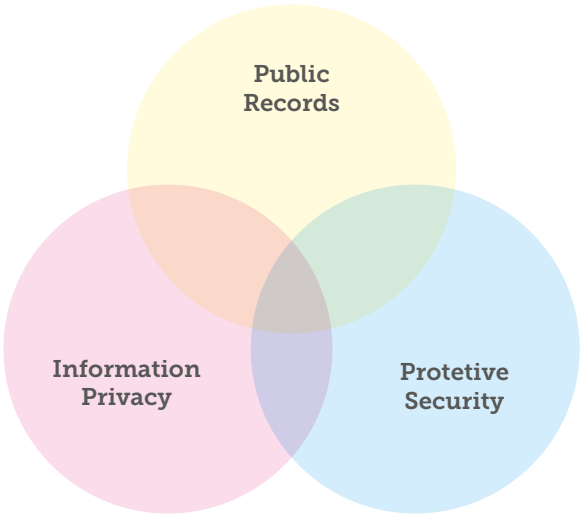


Figure 5 – Overlap of Laws

4.2.3 Step Three: Identify Applicable Legal Requirements

Once the second step is completed, it is possible to identify the applicable legal requirements. Depending on the laws involved, the third step of the preliminary process may involve different approaches, with different methodologies and/or checklists available to assist agencies determine which requirements need to be taken into account in their risk assessment process. For example, PROV's Cloud Computing Policy and two associated Guidelines include a data requirements checklist against relevant PROV Standards and a Contract Checklist. In a privacy context, a Privacy Impact Assessment (PIA) provides a useful tool for identifying and analysing privacy risks and issues, including cloud-computing proposals.

For clarity, each 'category' (recordkeeping, privacy, protective security) is discussed separately, below, although as noted above, it is possible for more than one category to apply to a specific cloud proposal. Specific legal requirements associated with the PDPA, HRA or PRA may be identified initially at a high-level; subsequently, public sector agencies should 'drill down' to capture the requirement at a detailed level.

While this discussion paper takes a category-by-category approach to each domain below (see section 4.3), a list of 'common' requirements is also documented at the end of this chapter (see section 4.3.4).

4.2.4 Step Four: Undertake Risk Assessment

At this stage of the process it is possible to undertake a risk assessment that incorporates appropriate consideration of recordkeeping, privacy and protective security. As the VGRMF is (or should be) well known to readers, the process of the risk assessment itself is not discussed further in this discussion paper. Readers interested in understanding more about risk assessment should consult the VMIA website.[24]

4.3 Recordkeeping, Privacy, Protective Security

4.3.1 Recordkeeping

The PRA needs to be taken into account if any of the information involved in a cloud-computing proposal is a public record.

In 2014, PROV issued a specific cloud-computing Policy and two associated Guidelines:[25]

- Recordkeeping Policy: *Recordkeeping Implications of Cloud Computing*
- Guideline 1: Cloud Computing Decision Making
- Guideline 2: Cloud Computing Tools.

The PROV Recordkeeping Policy applies to all Victorian public sector bodies that are bound by the PRA. The policy covers three main topics (see Figure 6, below).

24 The Victorian Government Risk Management Framework and associated resources are available at: https://www.vmia.vic.gov.au/risk/victorian-government-risk-management-framework.

25 Public Record Office Victoria (PROV), PROV Cloud Computing Policy; PROV Cloud Computing Guideline 1: Cloud Computing Decision Making, PROV Cloud Computing Guidelien 2: Cloud Computing Tools'.

1) Cloud computing decisions should be subject to a data risk assessment	2) Cloud computing use must be capable of compliance with legislation, standards and policies	3) Cloud computing agreements must adequately cover data management needs
Any decision to move public sector services and data storage into a cloud environment should be subject to a risk assessment process that considers information management risks as a specific issue. It should also include a specific data risks identification register, with accompanying risk mitigation strategies. This approach is consistent with the Victorian Government's current mandate that agencies engage in security risk assessment in relation to cloud computing decision making (*Cloud Computing Security Considerations for the Victorian Government*). Further information is provided in PROV Guidelines 1 & 2.	Public records should only be stored in a cloud environment capable of complying with all relevant Victorian legislation and policy directives. Further advice is provided in Guideline 2, in particular, the Document Map (which shows all the generic legislative, standards and policy requirements that bind Victorian public sector agencies). Where it is proposed that personal or sensitive data be stored in a public or community cloud, a data classification and sensitivity analysis should be undertaken.	Cloud vendor contracts or agreements should include sufficient and binding clauses to make certain agency data is effectively protected. This includes ensuring that the cloud service provider is capable of, and will execute, completed destruction of deleted records. Further information is provided in PROV Guideline 2. In particular, contracts or agreements must clearly identify the public sector agency as the owner of the data, including: • all transactional data created as a result of data being processed on the cloud computing service provider's systems; • all metadata relating to agency data managed in the cloud.

Figure 6 – Recordkeeping Implications of Cloud Computing

As PROV Policies derive their authority from PROV Standards (which are mandated instruments of the PRA), *they are binding* upon agencies. PROV Guidelines provide agencies with advice about the practical implementation of policy requirements.

Victorian public sector data stored in or created by any cloud solution is subject to the same PROV records management standards, guidelines, policies and obligations as public sector data stored in other environments, such as departmental IT systems and paper filing systems. In particular, public sector bodies are responsible for checking specific PROV Retention & Disposal Authorities. Guideline 2 provides a data requirements checklist against relevant PROV Standards to assist with this process.

Notably, PROV Standards can be seen to take an *information lifecycle* approach to recordkeeping in which public records are subject to strategic management throughout that lifecycle, covering the capture, storage, access and control of public records through to their (authorised) disposal.

4.3.2 Information Privacy

The PDPA and the HRA are Victoria's primary information privacy laws. The PDPA reproduces the ten Information Privacy Principles (IPPs) originally enacted in the IPA; which continue to apply to public sector organisations. The PDPA also contains new provisions relating to information sharing that are intended to provide greater certainty and flexibility to the public sector.[26] The Commissioner for Privacy and Data Protection (CPDP) administers the PDPA.

The HRA contains eleven Health Privacy Principles (HPPs), which provide the framework for health information privacy management in the public and private sectors in Victoria. The Office of the Health Services Commissioner (OHSC) administers the HRA.[27]

Privacy laws regulate the collection, use, disclosure and handling of personal information, including sensitive and health information, primarily through the application of the IPPs and the HPPs. The IPPs and HPPs embody an *information lifecycle approach* to the collection and handling of personal information. The obligations imposed by the IPPs and HPPs begin *prior to* the collection of any personal information and inform the approach to its collection, use, disclosure, storage, transfer and eventual destruction or permanent de-identification.

End-to-end refers to the way in which privacy is assured across all entities, processes and systems (internal or external) handling personal information that has been captured or created by a public sector body.

Whole-of-information-lifecycle refers to the ability to cover and/or assess the entire information lifecycle – from collection through to use and disclosure, archiving and destruction.

In certain instances – i.e. where a State contract is in place – the IPPs *may extend* to private sector organisations as the PDPA contains an outsourcing mechanism enabling Victorian public sector privacy requirements to apply to Victorian contracted service providers *as if they were* Victorian public sector agencies, as long as a suitable privacy clause is included in the contract or funding agreement. This is equally relevant to cloud-computing proposals and cloud service providers.

A Privacy Impact Assessment (PIA) enables the assessment and proposed management of privacy risks; it provides a suitable tool for the assessment of cloud-computing proposals.

A PIA is *a point-in-time assessment* of the actual and/or potential privacy impacts that an (existing or proposed) initiative, system, data collection or program may entail. It is a systematic process that examines the collection and handling of personal information (including sensitive and health information) *end-to-end* and from a *whole-of-information-lifecycle* perspective.

A PIA highlights any privacy risks. It includes recommendations to mitigate negative impacts wherever possible, as well as identifying ways to promote privacy-positive outcomes. A PIA identifies whether a project:

- Complies with privacy law requirements; and
- Does not raise significant privacy policy concerns that cannot be mitigated.

26 The PDPA contains a number of new provisions intended to support and provide clarity and flexibility for public sector agencies. In particular, an agency will not be required to comply with an IPP or IPPs in relation to an act or practice that is permitted under a public interest determination (PID) or a temporary public interest determination (TPID); or an approved information usage arrangement (IUA).

27 As noted above, this guide is not intended to provide specific advice in relation to health information, which is regulated under the *Health Records Act 2002* (Vic) (HRA), nor will the PDPA's protective security framework apply to health services. However, it is important to ensure that health information is taken into account, where relevant, in any cloud-computing risk assessment.

In essence, a PIA is a *privacy risk management tool*. By helping to identify privacy risks and potential mitigation strategies, a PIA ensures that privacy is 'built in'.

Embedding privacy into design (defined broadly) is specifically highlighted in *Privacy by Design* (PbD), a methodology endorsed by the CPDP as the preferred approach to privacy management within the Victorian public sector from 1 July 2014.[28] *Privacy by Design* has *7 Foundational Principles* that seek to address information privacy in a comprehensive and positive way; they are not intended to duplicate or seek to replace the IPPs. The seven foundational principles include:

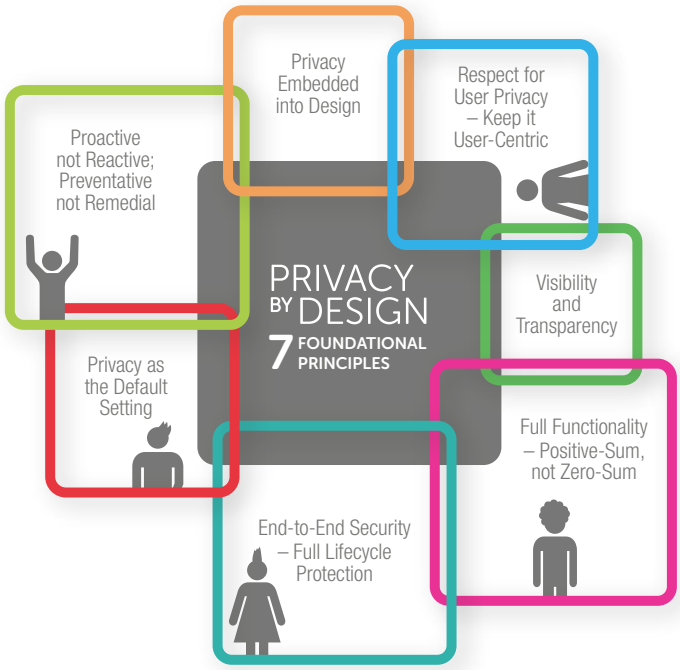


Figure 7 – The 7 Foundational Principles of Privacy by Design

If PIAs provide a key tool for the assessment of cloud-computing privacy risks, PbD provides an overarching approach to operationalising privacy management within an organisation, making a positive contribution to the privacy risk assessment process. In terms of a cloud-computing proposal, it is fundamental that privacy should be 'built in' as it may not be feasible (or affordable) to 'bolt it on' afterwards. So too, the 'balancing' inherent to risk assessment processes do not always produce the best privacy outcome. PbD demonstrates how it is possible to assess risk while working towards a 'win/win' outcome.

> '*Privacy by Design* – embedding privacy into information technologies, business practices, and networked infrastructures, as a core functionality, right from the outset – means building in privacy right up front – intentionally and with forethought. PbD may thus be defined as an engineering and strategic management approach that commits to selectively and sustainably minimize information systems' privacy risks through technical and governance controls. At the same time, however, the Privacy by Design approach provides a framework to address the ever-growing and systemic effects of ICTs and large-scale networked data systems with enhancements to traditional privacy principles.'
>
> *Operationalizing Privacy by Design*

28 OVPC, *Privacy by Design* Press Release (May 2014).

4.3.3 Protective Security

The VPDSF will provide a framework for the monitoring and assurance of the security, integrity and availability of data held by the Victorian public sector. Agencies will be required to comply with VPDSF standards, undertake a security risk profile assessment and develop and implement security plans to address protective security requirements. This will improve the consistency and coverage of protective security across the Victorian public sector, noting that agencies are not operating in a vacuum and should already be complying with general information security requirements.

As with recordkeeping and information privacy, protective security requires that the creation, storage, processing and transmission of government information must be managed appropriately and protected throughout all phases of *the information lifecycle*. It must also be consistent with all relevant legal and regulatory requirements, polices, guidelines and standards.

Law enforcement agencies and the Chief Statistician are required to comply with law enforcement data security standards tailored specifically for law enforcement data and crime statistics: *Standards for Victoria Police Law Enforcement Data Security* (SLEDS) and *Crime Statistics Data Security Standards*.[29] These are based upon the Standards for Victoria Police law enforcement data security issued under the *Commissioner for Law Enforcement Data Security Act* (2005) (CLEDS Act) in 2007.

The Victorian Government collects and handles a wide range of information in order to perform its functions and activities. Each public sector agency is currently required to ensure that it has implemented an appropriate protective security framework to protect this information from unauthorised use or accidental modification, loss or disclosure (i.e. in advance of the VPDSF). This mirrors privacy requirements imposed by IPP/HPP 3 (Data Quality) and IPP/HPP 4 (Data Security) but enables them to be addressed at a far greater level of detail.

Protective security requirements apply equally to outsourced service providers or other contractors, including cloud-computing providers. Agencies are responsible for ensuring that a contractor complies with all necessary protective security requirements, including through contractual terms and conditions. This is equally relevant to cloud computing service providers.

The VPDSF will incorporate the following security components:

- Security policies and procedures
- Security risk management
- Information access
- Security training and awareness
- Security incident management
- Third party management
- Information security information sharing
- Personnel security
- ICT security
- Physical security.

29 Commissioner for Privacy and Data Protection, *Standards for Law Enforcement Data Security* (September 2014).

4.3.4 Summary of Common Requirements

It is apparent that there are a number of common requirements applicable to recordkeeping, privacy and protective security. These include the following.

1. The PRA, PDPA and HRA all take *an information-lifecycle* approach to the regulation of public records, personal information (including sensitive and health information) and protective security. While the terminology may be different across each domain, the overarching approach is consistent. This can be leveraged to develop a comprehensive approach to any risk assessment process (encompassing recordkeeping, privacy and protective security).

2. Cloud-computing proposals must be subject to a *data risk assessment* that considers information management risks (i.e. those relating to privacy, protective security, recordkeeping) as a specific issue or component of the broader risk management assessment. This is also consistent with current requirements.

3. The Victorian Government *already mandates* that public sector agencies undertake a risk assessment using the VGRMF. Specific assessment of information management risks can be incorporated into this approach with minimum effort.

4. Some categories or types of information are so sensitive that they should never be stored in a public cloud (e.g. Cabinet documents). If 'sensitive' information is to be stored in the cloud, a private or community cloud may be a prerequisite. Other government information (e.g. publications) may be suitable for less secure (public cloud) models, subject to the results of a full risk assessment.

5. Where public sector data is to be stored in the cloud (public, private or community) steps must be taken to ensure that the information is appropriately protected from disclosure.

6. Cloud-computing contracts and agreements must cover information management requirements relating to privacy, protective security and recordkeeping appropriately. For example, this is mandated under the PROV Strategic Management Standard (PROS 10/10, v.1.1) and related Specification (PROS 10/10 S1).[30] PROV also addresses this point in its *Cloud Computing Policy Guideline 2: Cloud Computing Tools* where it states that contracts and agreements must affirm agencies' ownership of its data, including transactional data created as a result of data being processed on the cloud provider's system and all metadata relating to agency data managed in the cloud.[31]

30 PROV materials relating to Strategic Management, including the Strategic Management Standard and related Specification are available via the PROV website: http://prov.vic.gov.au/government/standards-and-policy/strategic-management.

31 PROV, PROV Cloud Computing Guideline 2: Cloud Computing Tools (June 2013), p.18.

5 Cloud Computing Responsibilities

5.1 After the Risk Assessment

Regardless of whether or not cloud computing is outsourced to a cloud service provider or undertaken by an agency itself, various cloud-related responsibilities need to be identified, allocated and/or addressed appropriately.

When government functions or activities are outsourced to a cloud service provider – either partially or entirely – public sector agencies are responsible for ensuring that relevant requirements are allocated appropriately. In terms of application, addressing requirements will be a joint responsibility of the outsourcing organisation (e.g. the department or agency) and the cloud service provider and – as relevant – its subcontractors.

Following the risk assessment process, agencies need to document requirements and allocate responsibilities between the agency and the cloud service provider.

5.2 Documenting Requirements & Allocating Responsibilities

When selecting the most appropriate type of cloud computing to use and the vendor to provide it, it is essential to consider how the cloud computing provider and its service(s) will support an agency's privacy, security and records management requirements. As highlighted in Chapter 4, these requirements range across the information lifecycle and may be legal, governance, technical, operational (including feedback loops) and/or locational in nature.

There are numerous ways to document cloud-computing requirements. For example:

- The *PROV Cloud Computing Guideline 2: Cloud Computing Tools* provides a cloud-computing checklist of data requirements against the PROV Standards.[32]
- Australian Signals Directorate (ASD) has published high-level guides to cloud-computing security from the perspectives of 'tenants' (e.g. outsourcing organisation) and cloud service providers, respectively.[33] These include one-page summaries of key risks and risk mitigations, illustrating a possible means of carrying risks identified during a risk management assessment over to the procurement phase.
- ASD also provides a more detailed assessment of cloud computing security considerations including an overview checklist and series of questions designed to help organisations undertake a risk assessment and to determine whether or not the proposed cloud-computing proposal has an acceptable level of risk.[34]

Having identified a comprehensive set of requirements, agencies need to evaluate cloud service offerings against them prior to entering into any cloud computing arrangement. Consideration also needs to be given as to how information management requirements will be reflected in the contract or service agreement. Again numerous guides to cloud-computing contracts have been published and may provide a useful model for Victorian public sector agencies. For example:

- The *PROV Cloud Computing Guideline 2: Cloud Computing Tools* includes a contract checklist.

32 Public Record Office Victoria (PROV), PROV Cloud Computing Guideline 1: Cloud Computing Decision Making (2013), p.14.
33 ASD, *Cloud Computing Security for Cloud Service Providers* (April 2015), p.2.
34 ASD, *Cloud Computing Security Considerations* (September 2012).

- The Australian Government Information Management Office (AGIMO) has published a guide in relation to negotiating legal issues in cloud-computing agreements; this includes a high-level summary of 'checkpoints'.[35]

The following diagram identifies some of the main issues that will need to be addressed from the perspective of cloud service providers and/or agencies (as/if required) (see Figure 8, below).

What are the scope and breadth of requirements for Cloud Service Providers?

Cloud computing services do not deliver ICT alone; rather, they provide bundled services (e.g. operational processes and services). Therefore, there may be a need to ensure that cloud provider personnel and facilities also comply with necessary security requirements (e.g. personnel clearances).

Consider whether are any requirements relating to:

- information
- ICT security
- physical security
- personnel.

Which cloud service models are 'fit for purpose'?

Different cloud service models (e.g. IaaS, PaaS, SaaS, etc.) typically cover different levels of requirements. For example, for SaaS, Cloud Service Providers can be expected to take responsibility for the security of application software as well as underlying IT servers and data centres. For IaaS, however, Cloud Service Providers do not typically provide application security.

It is important to understand the type of responsibilities that need to be met by Cloud Service Providers and to align them with the cloud service model selected. A failure to do this may result in significant gaps against requirements.

What needs to happen if an incident arises?

Incidents can arise in terms of privacy, security and/or recordkeeping. Many cloud service contracts do not guarantee notification of data breaches and therefore need to be examined carefully.

A wide range of incidents may occur, including breaches of information privacy and/or confidentiality, loss of information integrity or availability or disruption and/ or outage of service.

Cloud Service Providers typically have processes for handling incidents, but the processes need to be understood clearly, as they may not align with agency requirements.

Key aspects to consider include:

- how do Cloud Service Providers define what is, and what is not, an incident?
- which incidents are notified to the customer, when are they notified and what type of information is provided?
- who is responsible for managing an incident?
- for incidents that involve loss of availability or integrity of information or services, who ensures that backups are available and that successful recovery can take place?
- how are incidents investigated? Who is involved and what information is made available to the customer (e.g. legal discovery, forensics evidence, audits logs, etc.)?

What does the cloud services contract need to cover?

If an agency relies on Cloud Service Providers to execute many of their privacy, security and recordkeeping responsibilities, it is important that these requirements are clearly stated and agreed to in the cloud service contract.

Key contractual matters include:

- confirming all agency information remains the property of the State of Victoria (including any necessary metadata);
- commitments that information will be collected, handled, stored, backed-up and/or deleted in the required manner and in the required locations;
- addressing responsibilities for effective operation of controls (technical and procedural);
- provision of commitments to provide regular assurances over controls;
- stating the requirements for notifying and handling incidents; and
- addressing procedures for notifying any changes to cloud computing service features.

Additionally, many Cloud Service Providers use other cloud providers for support services, e.g. SaaS providers may run their application in IaaS environments run by another provider. Any contractual requirements applying to CSPs must extend to any subcontractors involved in handling the agency's data.

Figure 8 – Summary of Cloud Computing Responsibilities

35 AGIMO, *Negotiating the Cloud – Legal Issues in Cloud Computing Agreements* (February 2013, v.1.1).

5.3 Additional Precautions

Depending on the type of cloud computing service being used and the nature and sensitivity of the information being handled, an agency may need to implement additional measures to ensure that its privacy, security and/or recordkeeping requirements are addressed appropriately. These may include additional technical or contractual controls or operational procedures.

As these measures might require additional planning and cost to an agency or technical integration with the cloud computing service, it is important that they are considered upfront and prior to engaging the service (or as soon as possible thereafter if it is a question of extending scope over time). The following diagram identifies some of the key issues to be addressed (see Figure 9, below).

What additional measures may be needed in relation to a particular cloud service model?	**What additional measures are required in the event of an incident arising?**	**Can addtion controls compensate effectively for gaps in requirements?**
As described above, different cloud models typically cover different levels of requirements. It is important to understand what responsibilities are to be met by Cloud Service Providers and ensure that those not addressed are covered by other means. For example, a PaaS service provider might provide security of data centres and servers, but not application security, which may need to be addressed by an internal security team and/or another service provider.	As outlined above, it is important to understand what actions the Cloud Service Provider will undertake if and when an incident arises. It is equally important to understand what residual actions the agency may need to take and how these action will be coordinated. In particular, in cases where an incident is only partially identified and/or managed by the Cloud Service Provider (e.g. IaaS and PaaS), the organisation needs to ensure that it has adequate incident detection and response practices in place for services not covered by the Cloud Service Provider (e.g. Application-related incidents).	In some cases, it is possible that additional controls can be added by agencies to compensate for gaps in the cloud service being provided. For example, if a Cloud Service Provider's security practices are not considered adequate for requirements, sensitive information could be encrypted or "tokenised" to reduce the risk of a privacy breach. In determining the feasibility of such an approach, its effectiveness needs to be considered carefully. If additional controls are provided by the Cloud Service Provider but rely on the customer to deploy them appropriately, agencies must ensure that they take advantage of the additional controls.

Figure 9 – Cloud Computing: Additional Precautions

5.4 Ongoing Assurance

Agencies need to obtain periodic assurance that cloud services are operating as required and that recordkeeping, privacy and security requirements are being adhered to. Assurance is required for a number of reasons, including the need to satisfy audit or regulatory requirements or in order for management to retain oversight of its information risks.

The 'sensitivity' of information and associated management requirements will need to be re-assessed periodically. For example, as system usage grows it is common for more data elements to be added, information volumes to grow and, as a result, levels of sensitivity to change. It is important that information risks are periodically reviewed to ensure that the risk assessment made at the time of a cloud implementation remains valid.

Additionally, for many widely accessed cloud services, such as email, file storage and collaboration tools, it is easy and common for sensitive information to 'leak' into the cloud, for example via email attachments stored in cloud-based mailboxes. This can happen when users store sensitive information in a cloud service that does not have the necessary security in place. These factors should be considered both at the time of the initial information risk assessment and during periodic reviews. If necessary, additional measures may need to be implemented (e.g. usage policies, data detection tools) to mitigate these risks.

It is more difficult to obtain visibility of cloud computing service providers' systems and operations than is the case with conventional ICT service providers. Indeed, obtaining assurance from cloud providers may only possible if it is a term of the contract. It is therefore critical that relevant requirements are identified prior to entering into a cloud-computing contract.
The following diagram identifies some of the key issues to be addressed (see Figure 10, below).

What assurance is required from Cloud Service Providers?	Will it be necessary to conduct audits of the cloud services?	Is it acceptable to rely on audit reports and certifications supplied by Cloud Service Providers?
For agencies to demonstrate that they are meeting their privacy, security and record keeping accountabilities when their information is in the cloud, they need to obtain regular assurance regarding the Cloud Service Provider's operational controls, processes and procedures. **How often should it be obtained?** The depth and frequency of such assurance will depend on a number of factors including the nature and sensitivity of the information and specific legislative and regulatory requirements affecting the organisation.	A key difference between conventional ICT providers and Cloud Service Providers is that conventional ICT service providers often have audits conducted of their own systems. This may not be possible with Cloud Service Providers unless it is a term of the contract. If such audits are necessary, but not available, this may create significant regulatory and/or risk management issues. Before entering into a cloud contract that does not allow for audits to be performed, it is important that assurance requirements are well understood and alternative approaches investigated, e.g. use of independent 3rd party audits.	In lieu of allowing customers to perform their own audits, many Cloud Service Providers will offer access to reports performed by their own independent auditors and/or details of certifications they have received (such as ISO Standard certificates). Relying on such reports and certifications may be an acceptable substitute, provided that: • the details of the reports and certifications are made available for the agency to review on a regular basis (usually annually); • the scope of the audits cover the cloud services being used and are performed in the locations where they are operating; • the audits are performed by a suitably-independent audit and the nature and extent of audit procedures are acceptable; and • these requirements are agreed to in the cloud service contract.

Figure 10 – Cloud Computing: Ongoing Assurance

6 Next Steps

This discussion paper is designed to provoke comment and feedback across the Victorian public sector and the community at large. Comments are encouraged and should be sent by email to cloud@cpdp.vic.gov.au by COB on 3 July 2015.

In the meantime, we will be holding multiple discussion forums. More details about these forums will appear shortly on our website www.cpdp.vic.gov.au . A final, facilitated forum will be held to review the document following the end of the feedback period.

This paper on cloud computing is a key part of our work on strategic issues surrounding record keeping, privacy and data security. For the Office of the Commissioner for Privacy and Data Protection, its completion is central to our ongoing workplan, which is currently developing authoritative guidance on:

- Big Data
- How to undertake a Privacy Impact Assessment
- Public sector information sharing
- Identity management.

Cloud computing is a key enabling technology to developing more sophisticated approaches to the management of public sector information, so a broad discussion of the risks, benefits and implications of its use, leading to reasoned and concrete guidelines is necessary.

Appendix A – Glossary and Acronyms

ASD	Australian Signals Directorate
AGIMO	Australian Government Information Management Office
APPs	Australian Privacy Principles (Cth)
CPDP	Commissioner for Privacy and Data Protection
The Charter	*Charter of Human Rights and Responsibilities Act 2006 (Vic)*
Cloud infrastructure	The collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually, the abstraction layer sits above the physical layer. (*NIST Definition of Computing*, p.2, footnote 2)
Data security standards	Under the PDPA means: a) protective data security standards; or b) law enforcement data security standards.
De-identified	In relation to personal information, means personal information that no longer relates to an identifiable individual or an individual who can be reasonably identified (s.3, PDPA)
DLM	Dissemination limiting marker. A marker that indicates access to public sector data should be limited.
Document	Under the *Evidence Act 2008* (Vic) means any record of information and includes: a) anything on which there is writing; or b) anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them; or c) anything from which sounds, images or writings can be reproduced with or without the aid of anything else; or d) a map, plan, drawing of photograph
ENISA	European Network and Information Security Agency
Handling	Under the PDPA means: Collection, holding, management, use, disclosure or transfer of personal information

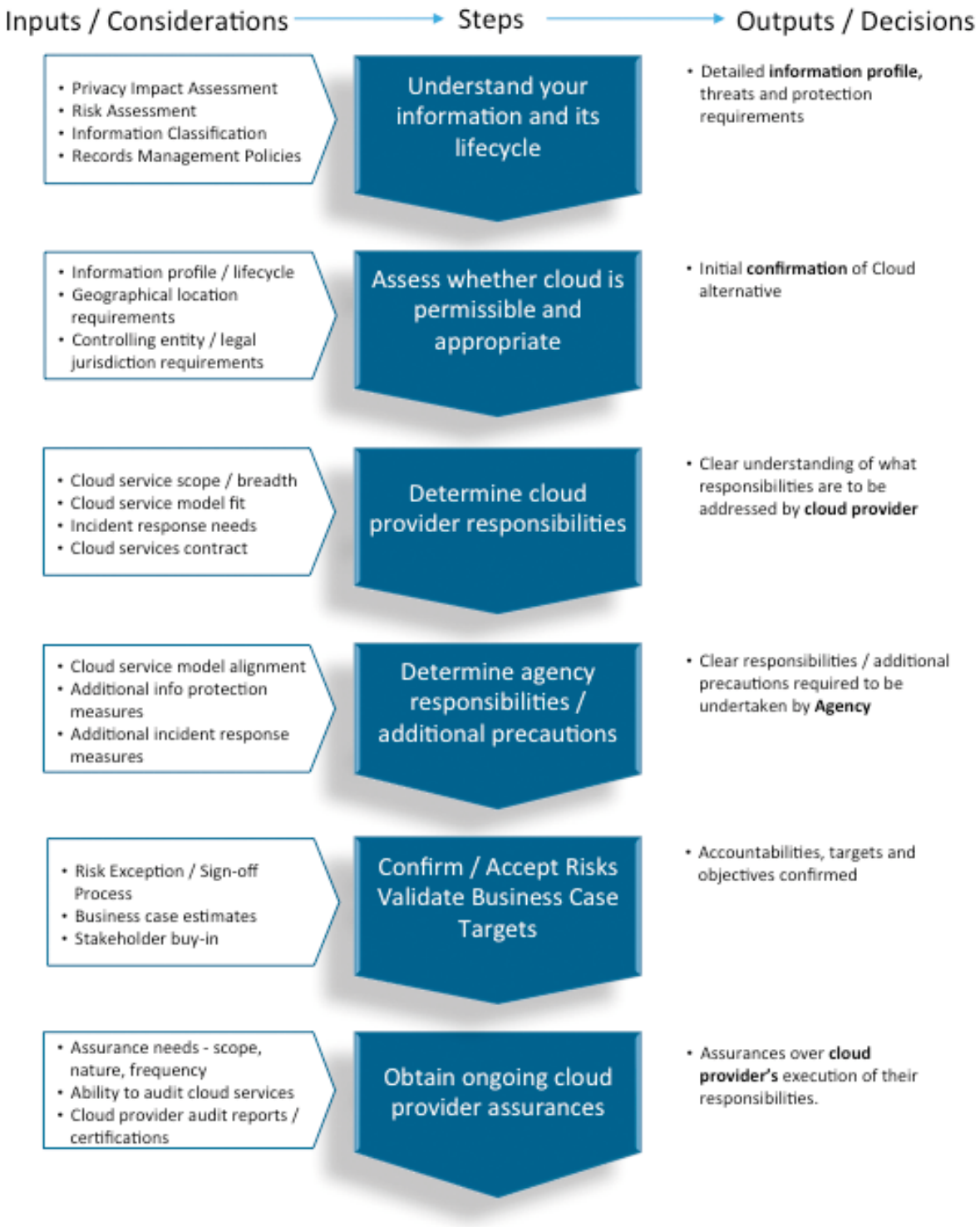
Health information	Under the HRA means: a) information or an opinion about- i. the physical, mental or psychological health (at any time) of an individual; or ii. a disability (at any time) of an individual; or iii. an individual's expressed wishes about the future provision of health services to him or her; or iv. a health service provided, or to be provided, to an individual- that is also personal information; or b) other personal information collected to provide, or in providing, a health service; or c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or d) other personal information that is genetic information about an individual in a form which is or could be predictive of the health (at any time) of the individual or of any of his or her descendants; but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of the *Health Records Act 2001* generally or for the purposes of specified provisions of the *Health Records Act 2001*
HPPs	Health Privacy Principles (Vic) Refers to the HPPs as set out in Schedule 1 of the HRA
HRA	*Health Records Act 2001* (Vic)
Identifying data	Identifying data are those data elements from which the identity of a specific individual is apparent (NHMRC, National Statement)
Information	As defined in Part 2 of the PDPA means: a) Personal information; or b) Public sector data; or c) Law enforcement data; or d) Crime statistics data
Information security (INFOSEC)	All measures used to protect public sector data from compromise, loss of integrity or unavailability
ISM	Information Security Manual (covers controls, principles and rationale for information security on ICT systems)
Law enforcement data security standards	Means the *Standards for Law Enforcement Data Security* to be issued under section 92 of the PDPA
IPPs	Information Privacy Principles (IPPs) Refers to the IPPs as set out in Schedule 1 of the PDPA
Metadata	Descriptive information about the content and context used to identify information.
National Statement	National Statement on Ethical Conduct in Human Research (2007)
Need-to-know	Refers to a need to access information based on an operational requirement
NHMRC	National Health and Medical Research Commission
NIST	National Institute of Standards and Technology (United States)

Non-identifiable	Data which have never been labelled with individual identifiers or from which identifiers have been permanently removed, and by means of which no specific individual can be identified. (NHMRC, National Statement)
OHSC	Office of the Health Services Commissioner
OVPC	Office of the Victorian Privacy Commissioner
PDPA	*Privacy and Data Protection Act 2014* (Vic)
Personal information	As defined in the PDPA means: Information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information of a kind to which the Health Records Act applies
Personal privacy	As defined in the PDPA means the privacy of personal information
PIA	Privacy Impact Assessment
PRA	*Public Records Act 1973* (Vic)
Privacy Act	*Privacy Act 1988* (Cth)
PSPF	Protective Security Policy Framework (Cth)
Public record	Defined in the PRA as: Any record made or received by a public officer in the course of [his/her] duties
Public sector	As defined in the *Public Administration Act 2004* (Vic), means: The sector that comprises: a) The public service; and b) Public entities; and c) Special bodies
Public sector agency	As defined in the PDPA means: A public service body or a public entity within the meaning of the *Public Administration Act 2004* (Vic)
Public sector body	As defined in the *Public Administration Act 2004* (Vic), means: a) A public service body; or b) A public entity; or c) A special body
Public sector data	As defined in the PDPA means: Any information (including personal information) obtained, received or held by an agency or body to which Part 4 applies, whether or not the agency or body obtained, received or holds that information in connection with the functions of that agency or body
Public sector data system	As defined in the PDPA includes: a) Information technology for storage of public sector data, including hardware and software; and b) Non-electronic means for storage of public sector data; and c) Procedures for dealing with public sector data, including by use of information technology and non-electronic means

Public service body	As defined in the *Public Administration Act 2004* (Vic), means: a) A Department; or b) An Administrative Office; or c) The Victorian Public Sector Commission
Public entity	In Victoria, public entities are organisations that exercise a public function and are established outside the public service. They operate at 'arm's length' from Government. Public entities can be established in a variety of legal forms, including statutory authorities, non-statutory advisory bodies and Corporations law entities. There are more than 1800 Victorian public entities with employees. A definition of 'public entity' is provided in the *Public Administration Act 2004* (Vic).
Record	Under the PRA means any document within the meaning of the *Evidence Act 2008*
Re-identifiable	Data in which identifiers have been removed and replaced by a code, but it remains possible to re-identify a specific individual by, for example, using the code or linking different data sets. (NHMRC, National Statement)
Sensitive information	As defined in the PDPA means: Personal information that is also about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, or criminal record
SLEDS	*Standards for Victoria Police Law Enforcement Data Security*
Third party	As defined in the PDPA means: A person or body other than the organisation holding the information and the individual to whom the information relates
Unique identifier	As defined in the PDPA means: An identifier (usually a number) assigned by an organisation to an individual uniquely to identify that individual for the purposes of the operations of the organisation but does not include an identifier that consists only of the individual's name but does not include an identifier within the meaning of the *Health Records Act*
VGRMF	Victorian Government Risk Management Framework
VPDSF	Victorian Protective Data Security Framework Means the VPDSF to be developed under s.85 of the PDPA

Appendix B – Cloud Computing Decision Flow Chart

Below is a suggested 'decision flow' to assist users of this document to apply the above guidance in a structured manner.



Appendix C – References

Legislation

Crimes (Document Destruction) Act 2006

Evidence Act 2008

Evidence (Document Unavailability) Act 2006

Freedom of Information Act 1982

Health Records Act 2001

Privacy and Data Protection Act 2014

Public Records Act 1973

Victorian Government

Public Record Office Victoria (PROV), PROV Cloud Computing Guideline 1: Cloud Computing Decision Making (2013), accessed April 2015

PROV, *PROV Cloud Computing Guideline 2: Cloud Computing Tools* (June 2013), accessed April 2015

PROV, *PROV Cloud Computing Policy* (June 2013), accessed April 2015

Department of Treasury and Finance, *Victorian Government Risk Management Framework* (March 2011)

VMIA, *Risk Management Guide* (April 2014)

Office of the Victorian Privacy Commissioner, Information Sheet: Cloud Computing (May 2011)

Minister for Finance, *Ministerial Standing Direction 4.5.5 – Risk Management Compliance*, Standing Directions of the Minister for Finance (July 2014)

Victorian Government Solicitor's Office (VGSO), *Cloud Computing in a Government Context* (October 2011)

VGSO, *Client Newsletter: Head in the Cloud, Feet Firmly Planted* (August 2011)

Australian Government

Australian Communications and Media Authority (ACMA), *The Cloud – Services, Computing and Digital Data* (June 2013), Occasional Paper 3, accessed April 2015

ACMA, *Privacy and Personal Data* (June 2013), Occasional Paper 4, accessed April 2015

Australian Attorney-General's Department (AGD), *Australian Government Protective Security Policy Framework* (November 2014), accessed April 2015

AGD, *Information Security Management Guidelines: Risk Management of Outsourced ICT Arrangements (including Cloud)* (August 2014), accessed April 2015

Australian Government Information Management Office (AGIMO), *Privacy and Cloud Computing for Australian Government Agencies* (February 2013), accessed April 2015

AGIMO, *Negotiating the Cloud – Legal Issues in Cloud Computing Agreements* (February 2013), accessed April 2015

Australian Signals Directorate (ASD), *Information Security Manual* (April 2015), accessed April 2015

ASD, *Cloud Computing Security for Tenants* (April 2015), accessed April 2015

ASD, *Cloud Computing Security for Cloud Service Providers* (April 2015), accessed April 2015

ASD, *Cloud Computing Security Considerations* (September 2012), accessed April 2015

Other References

Cloud Security Alliance (CSA), *The Notorious Nine: Cloud Computing Top Threats in 2013* (February 2013), accessed April 2015

CSA, *Cloud Adoption Practices & Priorities Survey Report* (January 2015), accessed April 2015,

Cloud Standards Customer Council (CSCC), April 2014, *Practical Guide to Cloud Computing, v.2.0*, accessed April 2015

CSCC, *Security for Cloud Computing: Ten Steps to Ensure Success, v.2.0* (March 2015), accessed April 2015

European Network and Information Security Agency (ENISA), *Cloud Computing: Benefits, Risks and Recommendations for Information Security* (November 2009), accessed April 2015

ENISA, February 2015, *Security Framework for Governmental Clouds*, accessed April 2015

P Mell & T Grance, *The NIST Definition of Cloud Computing* (October 2011), National Institute of Standards and Technology, accessed April 2015

This page is intentionally left blank

Commissioner
for Privacy and
Data Protection