information and privacy commission new south wales

Guide – Transition to the cloud: Managing your agency's privacy risks

May 2021

Contents

Commissioner's Foreword

Adoption of innovative technologies is key to the NSW Government's success in achieving its digital transformation agenda. Whether by developing apps to achieve public health outcomes in a pandemic or sharing data amongst agencies to develop better informed policies and initiatives, rapid innovation is at the centre for delivering the best results for the people of New South Wales.

The adoption of cloud-based technology plays an increasingly important role in this evolution. The Government has set itself the goal of having all NSW Government agencies using public cloud for a minimum of 25% of their ICT services, by 2023[1].

As this transition occurs it is critical that we manage the evolving risks that come with new ways of collecting, using, storing and transferring the personal information of the people of New South Wales. The NSW Government's *Cloud Strategy*[2] sets a common vision, direction, and approach for consuming cloud services to enable agencies to transform and accelerate digital service delivery. It lists security as one of six strategic outcomes, noting that "adhering to this strategy guidance regarding usage of cloud services will ensure NSW Government agency assets and data are secured."[3]

The effective management of privacy by New South Wales agencies is a key concern for my Office and has led to the development of this guide. Whilst information security forms part of effective privacy management under Information Protection Principle 5 and Health Privacy Principle 5, the objective of this guide is focused on adopting sound privacy practices throughout the process of using third parties to deliver services for and on behalf of regulated entities

This guide is intended for audiences at all levels of the agency. The Executive Summary gives agency heads an overview of the adoption of cloud by the NSW Government, associated privacy risks and tactics for mitigating those risks. For those responsible for the management of privacy risks and for technology strategy, the guidance also includes a checklist that summarises how personal information can be safeguarded in the cloud.

Being a part of the digital evolution of New South Wales and making the most of data assets requires the adoption of reliable and repeatable risk management and decision-making processes. I trust that this guide will assist agencies to consider and address privacy risks when adopting cloud solutions.

I encourage agencies to build this guidance into their digital transformation agenda.

Samantha Gavel

Privacy Commissioner

Information and Privacy Commission NSW

[1] Digital.NSW, *Cloud Strategy*, last updated 7 October, 2020. Available at: https://www.digital.nsw.gov.au/policy/cloud-strategy-and-policy/cloud-strategy

[2] Ibid.

[3] Ibid.

Executive Summary

Increased adoption of cloud-based technologies and services is a central element of the NSW Government's ICT strategy, and the Government has set ambitious goals for the adoption of public cloud across the sector. However, unless privacy risks are properly managed in the uptake of cloud, the impacts on both government and the people of NSW will outweigh the benefits. A multidisciplinary approach with clear strategic direction can ensure privacy risk is identified and managed throughout cloud adoption and use.

This guide has been designed to explain the key privacy risks that come with the use of cloud-based technologies by government, along with the potential impacts. It maps out a framework for addressing these privacy risks across the entire cloud adoption lifecycle. Each section of the framework contains practical advice for different professionals within the agency, including ICT, cyber and information security; procurement; people management; risk management and information and privacy professionals.

The guide contains references to other resources on cloud and on managing third party service providers. It is not our intention to restate the guidance that these resources deliver, however we refer NSW Government agencies to these guides as part of establishing their cloud adoption strategies and risk management processes. We have also included a glossary of terms and a checklist of questions about cloud adoption and use which are intended to make this guidance more practical.

By using this guide to build privacy into every facet of their cloud strategy and arrangements with cloud providers, agencies will both deliver great results for the people of NSW and protect the Government's reputation as a trusted custodian of personal information.

Introduction

The NSW Government partners and engages with various third parties in the delivery of programs and services across its portfolios, including both public-facing services and those that support the administration of government.

There are a range of matters that need to be considered in any arrangement under which an agency contracts out its business to a third-party service provider, regardless of the nature of that business – from a one-off engagement to build infrastructure to outsourcing managed ICT or HR services. These matters include ensuring transparent and fair procurement processes, proper contract inclusions, effective contract management, risk management over the life of the engagement and appropriate termination procedures.

When arrangements with a third-party involve that provider accessing, holding, using or disclosing personal information to deliver the services, privacy must become a key consideration in all aspects of the selection, engagement, management and termination of the service provider. In cases where the provider is delivering services via the cloud, there are specific privacy risks and controls that are relevant to that mode of delivery. These are the focus of this guide.

The move to cloud

Over the last decade, the NSW Government has pursued a strategy to increase cloud adoption. This started with a consolidation of data storage via a private cloud strategy and is now expanding to an uptake of public cloud, with an emphasis on software-as-a-service (SaaS). The Government's vision is to:

> "Enable government-wide adoption of public cloud services in an aligned and secure manner, to accelerate innovation, modernise service delivery and drive better outcomes for the citizens of NSW," (Digital.NSW, *NSW Government Cloud Strategy,* 2020).

The move to cloud: Helping the NSW Government take advantage of innovative technologies

Government is increasingly looking to cloud services for access to cutting edge technologies and large computing capacity.

For example, Transport for NSW has built a proof-of-concept using cloud-based data storage and machine learning technology from Microsoft to identify potentially dangerous traffic intersections and fast-track remediation works. The 'dangerous intersections' proof-of-concept, which took place last year, analysed telematic data collected from 50 vehicles travelling on Wollongong's roads over a 10-month period.

(Source: "NSW Transport and Microsoft use machine learning and data to reduce road accidents", *ZDNet*, 18 November 2020 https://www.zdnet.com/article/nsw-transport-and-microsoft-use-machine-learning-and-data-to-reduce-road-accidents/)

Privacy risks and impacts associated with using cloud services

The NSW Government expects agencies to have established risk management programs that are appropriate to each agency's size and risk profile, and properly resources to systematically identify the risks in the agency's operations that can affect achieving its objectives. The program should ensure the agency is making informed decisions about these risks and that it measures the success of any controls implemented. Risk framework advice and tools are available from agencies such as the NSW Treasury (see the References section of this guide).

Depending on the nature of the third-party engagement and the agency's operating environment, privacy risks can emerge from:

- poor security arrangements by cloud providers (including lack of data level controls), and insufficient assessment and monitoring of those arrangements;
- inadequate business continuity planning by cloud providers;
- data being stored in unknown or unauthorised storage locations, including in geographic regions with privacy laws that are less stringent than Australia's;
- inadequate access controls and related procedures for cloud services;
- personal information not being destroyed by cloud providers at the end of the engagement; or
- use of unauthorised cloud services by employees and contractors, or cloud services using unauthorised sub-contractors.

Privacy impacts that can flow from these risks can include:

- potential harm to individuals whose information is vulnerable to unauthorised access, for example identity theft;
- use of personal information for purposes unrelated to the purpose for which it was collected, for example for marketing;
- failure by an agency to meet legislative requirements pertaining to privacy or information access;
- business disruption flowing from loss of access to data or data quality issues where data is not centrally controlled; or
- damage to Government trust and reputation as custodians of the personal information of the people of NSW.

Each of the privacy risks identified above is described in more depth in the following sections.

Risk: Poor security arrangements by cloud providers

Cloud services providers that store or process personal information have a duty to their customers to uphold the highest standards for security, and to ensure routine monitoring of their environments as new threats emerge.

Cloud security failure: PageUp hacked

In 2018, the data held by international recruitment services company PageUp was compromised, resulting in unauthorised access to the personal information of job applicants. Thousands of job applicants' personal details may have been compromised in the breach. The PageUp service was being used by many large companies and agencies including Telstra, Wesfarmers, Linfox, the Reserve Bank, the ABC and some NSW Government agencies, to manage job applications via an online process.

(Source: "Page Up data breach: thousands of job seekers' details potentially exposed", *The Guardian*, 7 June 2018)

In many cases (like the PageUp breach), the compromise of a service can present serious potential harm to individuals. For example, when the personal information includes data such as date of birth or even tax file number or passport number, impacted individuals are exposed to the risk of identity theft.

Risk: Unknown storage locations for personal information in the cloud, including in geographic regions with privacy laws that are less stringent than Australia's

As is the case with most new products or services, the competitiveness of the product is predominately based upon its pricing. This is especially true in regard to cloud services, as many services have a free service offering. This dynamic however, can lead to many cloud services looking for the cheapest possible cloud computing and storage to build their service upon.

Whilst this model can support a competitive price point, it can also increase the risks to any personal information held within the service where the subcontracted providers have less robust security controls or are located in regions with privacy laws that do not meet the standards set by local laws.

Risk: Inadequate access controls and related procedures for cloud services

The risks associated with access control increase significantly as they are applied to cloud services. These risks can include a limited ability to apply suitably granular access controls or provision of access via internet-facing portals that are vulnerable to hacking.

Accordingly, the move to integrate cloud-based access control into agency-controlled access control (such as Single Sign On or 'SSO') is now a priority for many cloud-first organisations.

Risk: Personal information not being destroyed by cloud providers at the end of the engagement.

It is common for contractual arrangements with providers of cloud services to include provisions regarding the return or destruction of the customer's data at the conclusion of the engagement. In many cases these provisions state that these matters are at the discretion of the customer.

In cases where no instructions are given to the provider, the data may be retained by them beyond the termination of the engagement. This is particularly important when the data contains personal information: if there is no continuing agreement with the cloud provider to deliver services to government, they should not continue to have access to the data.

Risk: Unauthorised use of cloud services by government employees and contractors

There are a range of cloud services that can be purchased easily and for little cost, to perform functions such as data analytics, file or code editing and sharing, and storage. Because these services can be procured quickly and solve common business problems, they are sometimes seen by employees and contractors as being more convenient to, or as a "work around" to limitations with in-house software and internal approval processes.

Studies have shown that employees can often turn to 'shadow IT' to get their job done in time, and that use of such services can easily spread to teammates. Common examples of services that are widely known and used as a matter of convenience include among many others Dropbox, Google Docs, Slack and GitHub.

Typically, these free tools are unauthorised and have not been assessed by agencies for the adequacy of their privacy and security features, let alone having use of the service by employees monitored or audited. This in turn entails risks to information used on these platforms.

Additionally, widely used and in some cases free tools such as these are often a greater target for cyber criminals.

Shadow IT: A growing risk

A 2019 cloud risk report found that the use of cloud services among the organisations assessed had increased by 15% from the prior year. It was also noted that the average number of distinct cloud services used by each organisation was 1,935 services, while most organisations estimated they used far fewer.

The report also found:

- 21% of all files in the cloud contain sensitive data, this was up 17% over the previous two years;
- the number of files with sensitive data shared across cloud services had increased 53% year-over-year;
- that sharing sensitive data with an open, publicly accessible link had increased by 23% over the past two years;
- threat events in the cloud, i.e. compromised account, privileged user, or insider threat have increased 27.7% from the previous year; and
- the threats focused on the Microsoft Office 365 service have grown by 63% in the last two years.

(Source: McAfee, *McAfee Cloud Adoption and Risk Report, 2019)*

Storing personal information with unauthorised or 'shadow' cloud providers could mean an agency is unable to fulfil its requirements under the *Privacy and Personal Information Protection Act 1998* (PPIP Act) or the *Health Records and Information Privacy Act 2002* (HRIP Act).

Under the Act, a public sector agency that holds personal information must, at the request of the individual to whom the information relates and without excessive delay or expense, provide the individual with access to the information. Agencies must also, if requested, make appropriate amendments (whether by way of corrections, deletions or additions) to ensure that the personal information is accurate, relevant, up to date, complete and not misleading. An agency officer with the responsibility to identify and action such requests under these PPIP Act provisions will not have visibility over or a means of extracting data from unauthorised cloud services.

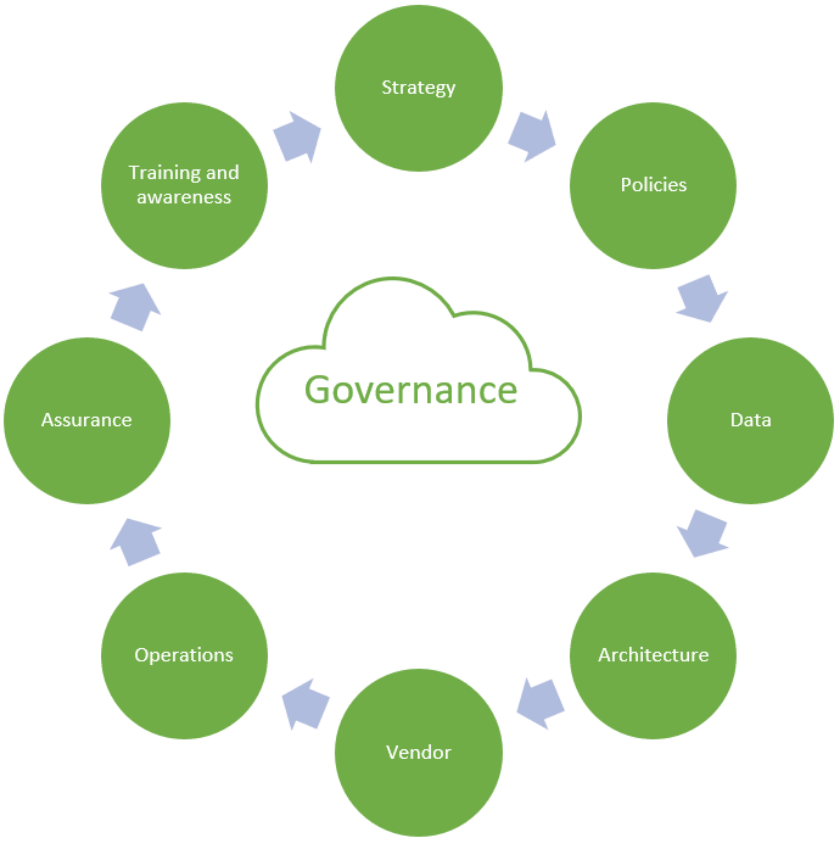
Use of unauthorised cloud services may also leave an agency unable to fulfil its obligations under section 121 of the *Government Information (Public Access) Act* (GIPA Act), under which contracts to provide services to the public on behalf of an agency must provide for the agency to have an immediate right of access to the following information contained in records held by the contractor.

Managing cloud risks

Effective and proactive management of the privacy risks associated with the use of cloud services requires a holistic approach comprising policy, leadership and technology measures across the full lifecycle of deploying cloud computing capabilities, from the consideration of a cloud service for a particular function or service, to the termination of the arrangement.

A framework to govern and manage cloud risks

The model below offers a framework for considering the decision-making processes, criteria and policies that are involved in the planning, architecture, acquisition, deployment, operation and management of an enterprise cloud computing capability.



Strategy:	Sets out how the organisation will consume cloud services, and for what purpose(s).
Policies:	Defines obligations, benefits and areas of risk intolerance.
Data:	Articulation and awareness of the data stored or processed by cloud services.
Architecture:	Monitors the alignment to the strategic vision and enterprise architecture.
Vendor:	Monitors vendor risk, shadow cloud usage and portfolio management.

Operations:	Monitors the delivery of corporate cloud services, performance, usage levels and orchestration.
Assurance:	Provides controls assurance of the key cloud governance controls.
Training and awareness:	Ensures behaviours are aligned with the strategy and risk controls are effective.
Governance:	Regular meetings enabling those charged with governance to proactively monitor cloud usage and make strategic decisions.

The following sections offer practical advice on each of the functional domains which make up the framework.

Strategy

A strategic direction should be set regarding the use of cloud services, and it should be informed by not only business outcomes, but also data risks – including privacy considerations. As articulated in previous sections, the management of privacy risks is a key element in creating confidence in the government's service delivery capability and should therefore shape an agency's strategic approaches to cloud services.

A cloud strategy should also consider the purposes of the services, the suitability of cloud and how personal information is stored or processed.

Risk tolerance should be defined, so that strategic decision making about cloud and privacy risk can be done consistently and appropriately.

Conducting a Privacy Impact Assessment prior to cloud adoption – and again, throughout the engagement

A Privacy Impact Assessment (PIA) should be done as early as possible when contemplating the use of cloud services and should be updated over time or in the event of a significant change in requirements or to the nature of the services delivered. A PIA should involve an assessment of:

- positive and adverse privacy impacts including community reaction;
- data flows, including across organisational and territorial boundaries;
- the types and sensitivity levels of personal information to be collected, stored or used;
- stakeholders in the proper management of the personal information;
- compliance with privacy laws and other relevant legislation; and
- measures to reduce any identified risks to privacy.

By ensuring that this information is kept up to date, the framework to manage cloud risks will be designed to suit the specific requirements of the service and the regulatory, business and societal context in which it operates.

It is important to remember that a PIA is not the 'be all and end all' for managing privacy risk. It is an important element of planning and can contribute to the identification of new risks as engagement changes over time, but it is one of many tactics across this framework.

For more on doing a PIA in the NSW Government see the IPC's *Guide to Privacy Impact Assessments in NSW*.

Policies

Agencies' policy frameworks may need adjustment to accommodate cloud use and any associated privacy and data risks. For example, existing policy on use of authorised ICT tools and technologies may need to be updated to prohibit the use of unauthorised cloud-based tools and technologies, particularly when personal information is involved.

Agencies' Privacy Governance Frameworks, should address privacy risks associated with the use of cloud services, and should be checked for alignment with cloud policy and governance.

Any adjustments to existing policy or new policies should take into account:

- the nature of the agency's business and the data it collects, shares and manages;
- whole of government policy on the use of cloud;
- agency obligations and areas of risk intolerance, such as ruling out the use of services storing data in certain geographical regions owing to incompatible privacy legislation;
- roles and responsibilities with regard to managing privacy risks when using cloud technologies; and
- agency policy on incident response and breach notification, with reference to the NSW Government's Mandatory Notification of Data Breach Scheme.

Data

It is important to understand whether new privacy risks have been introduced to the agency's data when cloud services are being used. This will dictate any additional data level controls that may be required, such as encryption of data during transfer to the provider, or deidentification of personal information. In order to make these decisions, agencies should understand the types of data stored or processed by cloud services – during the selection of such services and over time, as data types may change.

Key internal contacts for understanding more about agency data may include privacy officers, records and information managers, or security and data architecture professionals. Existing analyses of data types the agency collects, stores and transfers, prepared for a Privacy Management Plan, may be leveraged for these purposes. Similarly, resources such as data inventories, business classification schemes or retention and disposal schedules prepared for records management and other purposes may be useful indicators.

When engaging a cloud provider, refer to the authorised retention and disposal rules for the agency to determine how long the data must be retained. This period may exceed the duration of the arrangement with the service provider, in which case retaining and protecting the data remains the responsibility of the agency. For help on understanding retention requirements, consult with the agency's records manager or contact the State Archives and Records Authority.

Data: Special requirements for health information

While it is important to understand the nature of any personal information that will be processed or stored by a cloud provider, it is vital that health information is identified as early as possible, as there are specific requirements that apply to this information.

Notably, Health Privacy Principle 14 under the HRIP Act prohibits the transfer of health information about an individual by a NSW health service provider to any person or body who is in a jurisdiction outside New South Wales, unless under certain exceptions stated in the Act. Therefore, in selecting a cloud service where health information is involved, an agency should only consider on premise or cloud solutions that ensure compliance with this requirement. Other legislative schemes may also apply depending on the nature of the health information, these should be identified and considered as early as possible.

Architecture

It is generally the responsibility of the ICT function within an agency to monitor the alignment of any new service to its strategic vision and overall ICT architecture. Agencies should ensure that cloud services approved for use are compatible with its security policy and standards, which are designed to protect personal information and other sensitive data. Matters to assess here may include:

- whether the cloud service integrates with the agency's existing enterprise identity and access management system; or
- whether users are prevented from using unauthorised cloud services.

Agencies should be aware that some cloud providers will leave the implementation of security controls entirely to the customer. This is particularly prevalent with some large 'Infrastructure-as-a-service' providers. Failure to apply controls can lead to serious vulnerabilities for the data stored with the providers.

Vendor

It is important that there are clearly defined procedures for assessing vendor risk and that these encompass privacy risks. Privacy risks should be tracked throughout the vendor lifecycle, from engagement to termination.

Different cloud models have different levels of shared responsibility between the vendor and the customer. Therefore, it is important to identifying the boundaries of responsibility as early as possible in the engagement to avoid any accountability gaps in critical areas.

The agency should consider the 'privacy track records' of cloud providers to inform the selection process. Has the provider suffered breaches in the past? What processes do they have in place for identifying and dealing with breaches? How did they respond to the breach? Do they provide detailed information to prospective customers regarding their privacy and security policies?

Where possible, contractual arrangements with cloud-based service providers should facilitate monitoring or audit by the agency. This may mean having the ability to access audit logs or conduct audits. Arrangements should also clearly outline the provider's role in managing cyber security incidents and data breaches, including undertakings regarding notification.

Depending on the agency's risk profile and the nature of the outsourced arrangement, some ICT or cyber teams may also conduct ongoing threat intelligence monitoring to detect any new cyber risks or incidents affecting the agency or the vendors it works with.

An agency should ideally only accept a standard set of terms and conditions precluding such controls where an arrangement has been assessed as low risk from a privacy perspective. In these cases, terms should be carefully reviewed with an eye to any potential for heightened privacy risk.

Vendor: Checking the terms and conditions

In cases where a standard set of terms and conditions is offered by a cloud provider that will be collecting, storing or otherwise processing personal information, check for clauses that:

- describe the security measures that will be applied to the agency's data, including whether the data will be encrypted at rest and in transit;
- indicate whether the provider has certifications that boost confidence in their ability to safeguard personal information, such as the ISO 27000 series or SOC 2[4];

[4] ISO 27000 is a suite of International Standards that establish measurable requirements for information security. Developed by the American Institute of CPAs, SOC 2 defines a set of auditable "trust service principles"—security, availability, processing integrity, confidentiality and privacy.

- indicate an understanding of and commitment to adhere to applicable policy such as the *NSW Cyber Security Policy*;
- commit to compliance with local privacy, records or other legislation that the agency is subject to; or
- address where the data will be stored, including with any sub-contracted entities. The purpose of this is to avoid the storage or processing of personal information in countries with privacy regimes less rigorous than Australia's.

Publicly available resources such as data protection 'heat maps'[5] can help with comparing the strength of privacy regimes in different countries.

Operations

Even when an agency is using third party providers to deliver services on their behalf, accountability for compliance with privacy laws and requirements remains with the agency, making careful oversight and monitoring of the services critical.

Agencies should have the capability to determine and then actively monitor what cloud services are in use, and know, as part of that, which services are handling personal information. Like the monitoring of on-premise technologies, agencies should monitor the delivery of cloud services, performance, usage levels and orchestration.

Operations also means dealing with 'shadow IT' – unauthorised uses of cloud services, which can potentially lead to privacy breaches. Here security software tools can play an important role, and are more effective when implemented with other elements of the framework described in this guide.

Operations: Tools for intercepting unauthorised cloud use

Software tools are available that can assist in the management of privacy risks that come with 'shadow IT'. One such tool is a 'cloud access security broker', or CASB.

A CASB enforces the organisation's security policies by monitoring the environment – typically inclusive of the multiple types of devices that may be in use, both on-premise and cloud based – to track user access to cloud services. The data that is collected by the tool, including the nature and origin of the access, allows it to identify and block uses that are not authorised, such as an upload of data containing personal information to a free online tool not approved for use.

Successful deployment of a CASB depends on a number of elements of the framework described in this guide, including knowing your data and your vendors, as well as maintaining routine monitoring of the effectiveness of this control under your assurance program.

In addition to specialised tools, another tactical approach that can be used to manage the risk of 'shadow IT' is to use traffic data from the organisation's internet gateway to develop a list of commonly accessed cloud services. This list can be reviewed to determine which services are approved and which should be blocked. It can also be used to identify areas that should be addressed in planning, as their repeated use may indicate functionality 'gaps' in the suite of tools available to users. This approach can be seen as managing privacy risk from an architectural perspective, as described in the 'Architecture' element of this framework.

[5] An example of a publicly available data protection 'heat map' can be found at https://www.dlapiperdataprotection.com/

Training and awareness

Where an agency outsources business and systems to a third party such as a cloud provider, additional training and awareness may need to be provided to ensure agency staff understand how to manage privacy and security risks in relation to those services. The table below outlines content and messages that may be relevant to particular groups.

Role	Key messages
Employees and contractors	• Using unauthorised cloud services is strictly forbidden • Convenience never trumps protecting personal information • There are serious consequences to knowingly using unauthorised cloud services where personal information is concerned
Information security professionals	• Once adopted, public cloud services are part of the agency's technology footprint and should meet the security standards in accordance with the agency's security policy and standards • Where possible, include third party cloud services in security risk monitoring
Procurement and contract management personnel	• Privacy risk is an important consideration in all third-party engagements • Cloud brings specific risks that should be addressed in selection, contracting and monitoring • Personnel should be given specialist training and resources they can use to build data privacy into existing procurement processes
ICT professionals	• Data level controls that can be used to manage personal information in transit and at rest • Good practices and tools for monitoring cloud services use
Privacy professionals	• Cloud technologies and information security literacy to complement knowledge of privacy requirements

Training and awareness: Avoiding 'Shadow IT' incidents

A great way to deliver effective messages for managing privacy risk – particularly risks coming from the use of unauthorised services – is to understand common use cases for cloud, and then clearly communicate the approved option for each.

For example, a training story could start with: "I need to do X in my role, so I downloaded Y. I didn't know we had an authorised tool that can do that". Then follow up with specific advice on the tools that can be used for different data types:

- to share documents with your colleagues, use OneDrive;
- to transfer any data containing personal information with another agency, use the encryption and password protection tool 'X'; or
- to share code, use the agency' enterprise licence GitHub account – not your own.

Assurance

Controls that specifically address privacy risks associated with cloud services (including risks associated with unauthorised uses) should be clearly defined and documented, and periodic assurance over these controls should take place. With technologies evolving as quickly as they are today, these controls should be tested regularly and monitored over time.

Defining controls for protecting personal information where cloud services are in use should start with the Information Protection Principles (IPPs) from the PPIP Act.

Privacy controls for cloud: Examples	
Information Protection Principle	Control example
IPP 11: Disclosure – Restricted	The agency monitors, audits, and trains its staff on when transfer of personal information to a cloud provider is authorised, and the consequences of unauthorised use or sharing of personal information.
IPP 10: Use – Limited	Commercial terms with cloud providers limit the uses to which the personal information can be put by the third party.

Cloud services uses should be considered as part of the whole of enterprise risk framework. Performance audits of cloud arrangements should be included in existing auditing activities, and the results submitted to senior management and to oversight bodies such as an audit and risk committee.

Reporting arrangements should align with the agency's risk framework and obligations under the whole of government *Cyber Security Policy*'s compliance reporting and attestation provisions.

Governance

Cloud governance should be implemented by senior management and privacy risks and incidents should receive senior management attention and response.

Communication is key. A collaborative and informed approach is needed to successfully identify and act on emerging privacy risks flowing from new or changed cloud usage. This means maintaining regular communication amongst key leaders to proactively monitor cloud usage and make strategic decisions, as well as responding to and capturing lessons learned from privacy incidents. Leaders should routinely check in on the use of cloud by the agency and stay informed of any emerging risks.

Checklist for the management of privacy risks when using cloud technologies and services

Framework element	Ask…	Refer to...
Strategy:	• Has a strategic direction been set regarding the use of cloud services? • Are privacy risks considered as part of the setting of the strategic direction? • Has a risk tolerance been set?	• Strategic planning • ICT plan / roadmaps • NSW Government Cloud Strategy and Policy • NSW Treasury Risk Maturity Assessment Tool
Policies:	• Do your policies consider cloud use and associated privacy and data risks? • Are there gaps in your policy framework given cloud uses with privacy implications?	• Information and cyber security policies • Privacy management plan • Privacy governance framework
Data:	• What new privacy risks have been introduced to your data now that cloud services are being used? • Are additional data level controls required now that cloud services are being introduced?	• Data inventories • Data classifications • Retention and disposal schedules • NSW Information Management Framework
Architecture:	• Does the cloud usage align to your enterprise architecture model? • Are cloud services approved for use compatible with your security policy and standards?	• Enterprise architecture model for your agency • Data access policies and procedures
Vendor:	• Do your vendor risk assessments adequately consider the privacy risk associated with cloud vendors? • How are you monitoring the cloud vendor landscape for emerging cyber and other risks? • Have you checked the commercial terms for cloud providers for any red flags?	• Publicly available information on cyber risks and incidents • Risk management frameworks • NSW Government Procurement Policy Framework
Operations:	• Do you have the capability to determine and then actively monitor what cloud services are in use? • Have you identified which of those services involves personal information and may therefore require greater scrutiny?	• Role descriptions • System logs • Service provider contracts • Attestation reports from service providers

Assurance:	• What level of assurance is being sought over the privacy controls which protect data hosted in or processed by cloud services? • Have assurance arrangements been clearly defined and communicated to the right people?	• Attestations supplied to government for cyber risk purposes
Training and awareness:	• Have groups and roles requiring help with privacy and cloud been identified? • Does training and awareness address known privacy risks in a way that is meaningful to each group?	• Agency training strategy, plans • Existing privacy e-learning • Agency intranet
Governance:	• Is there a forum in place that allows senior management to regularly assess the privacy risks of using cloud services?	• Risk or other centralised committees' terms of reference and minutes

Glossary

Cloud access security broker (CASB) – on-premises or cloud-based software that monitors all activity occurring between users and cloud applications and enforces security policies.

Infrastructure as a service (IaaS) – a cloud computing model in which services such as storage, networking and servers are delivered to customers remotely over the Internet.

Platform as a service (PaaS) – a cloud computing model in which services need to develop, run, and manage software applications are delivered remotely over the Internet. Such services are often used by organisations doing in-house software development.

Private cloud – computing services solely dedicated to one end user, usually within the user's firewall. Although private clouds have traditionally been run on-premise, some organisations build private cloud infrastructure on rented, vendor-owned data centres, located off-premise.

Public cloud – computing services offered by third-party providers over the public Internet, available to anyone who wants to use or purchase them.

Shadow IT – technologies, including cloud-based services, deployed by departments or individuals outside of the controls and authorisations set up by the parent organisation.

Software as a service (SaaS) – a cloud computing model in which software is centrally hosted by a provider and is delivered to users of the software remotely over the Internet.

References

- Australian Cyber Security Centre, *Cloud Computing Security Considerations*, 2020
- Buy.NSW, *Procurement Policy Framework*, 2021
- Data.NSW, *NSW Data Governance Toolkit*, 2020
- Data.NSW, *NSW Information Management Framework*, 2018
- Digital.NSW, *Cyber Security Policy*, 2020
- Digital.NSW, *NSW Government Cloud Policy*, 2020
- Digital.NSW, *NSW Government Cloud Strategy,* 2020
- *Health Records and Information Privacy Act 2002* (NSW)
- Information and Privacy Commission NSW, *Data Breach Guidance for NSW Agencies*, 2020
- Information and Privacy Commission NSW, *Fact Sheet – Digital Projects*
- Information and Privacy Commission NSW, *Fact Sheet - Guide to section 121 of the GIPA Act for agencies*
- Information and Privacy Commission NSW, *Guide to Data Sharing and Privacy*, 2020
- Information and Privacy Commission NSW, *Guide to Privacy Impact Assessments in NSW*, 2020
- Information and Privacy Commission NSW, *Privacy Governance Framework*, 2016
- NSW Treasury, *Risk Management Toolkit,* 2021
- *Privacy and Personal Information Protection Act 1998* (NSW)
- State Archives and Records NSW, *Using Cloud Services Advice*, 2020

Document information

Identifier/Title:	Guide - Transition to the cloud: Managing your agency's privacy risks
Business Unit:	Investigation and Review
Author:	Director, Investigation and Reporting
Approver:	Privacy Commissioner
Date of Effect:	5 May 2021
Next Review Date:	5 May 2022
EDRMS File Reference:	D21/016125/DJ
Key Words:	Cloud storage, privacy