

Report 16 of 2021

Cloud computing in
SA Government



Report of the Auditor-General

Report 16 of 2021

Cloud computing in
SA Government

Tabled in the House of Assembly and ordered to be published, 26 October 2021

Second Session, Fifty-Fourth Parliament

By authority: S. Smith, Government Printer, South Australia

*The Auditor-General's Department acknowledges and respects
Aboriginal people as the State's first people and nations, and
recognises Aboriginal people as traditional owners and occupants of
South Australian land and waters.*



**Auditor-General's
Department**

www.audit.sa.gov.au

Enquiries about this report should be directed to:

Auditor-General
Auditor-General's Department
Level 9, 200 Victoria Square
Adelaide SA 5000

ISSN 0815-9157



25 October 2021

Level 9
State Administration Centre
200 Victoria Square
Adelaide SA 5000
Tel +618 8226 9640
Fax +618 8226 9688
ABN 53 327 061 410
audgensa@audit.sa.gov.au
www.audit.sa.gov.au

President
Legislative Council
Parliament House
ADELAIDE SA 5000

Speaker
House of Assembly
Parliament House
ADELAIDE SA 5000

Dear President and Speaker

**Report of the Auditor-General:
Report 16 of 2021 *Cloud computing in SA Government***

Under section 36(1)(b) of the *Public Finance and Audit Act 1987*, I have conducted a review of cloud computing in SA Government.

I present to each of you my report on the findings of the review.

Content of the Report

This Report is not based on the results of an audit, as no testing was performed. We performed a high-level review of seven agencies to understand the level and maturity of their cloud computing governance processes. We also looked at the extent of services and data that these agencies have moved to a cloud computing environment, the type of cloud service models used and the associated costs.

We found that the level of governance over cloud computing exercised by most of the agencies we reviewed could be improved in the following areas:

- some agencies do not perform risk assessments or relate with their ICT service team before engaging cloud computing service providers
- most agencies were not performing annual independent assessments of their cloud computing service provider arrangements
- some agencies had not developed or finalised cloud computing service level agreements for all established service provider engagements

- some agencies had not developed or finalised cloud computing policies and procedures to support their current arrangements.

The State's current cloud computing approach could be strengthened through increased collaboration between agencies and centralised reporting to either the Department of the Premier and Cabinet or some form of inter-agency forum. The aim would be to help agencies while they move their services to the cloud by providing guidance, risk mitigation strategies, a more consistent approach to managing cloud computing and the integration of security governance.

Acknowledgements

The audit team for this Report was Andrew Corrigan, Brenton Borgman, Tyson Hancock, Abhinav Tomar and Spoorthy Chitti.

We appreciate the cooperation and assistance given by staff of the agencies we reviewed.

Yours sincerely

A handwritten signature in black ink, appearing to read 'Richardson', with a long horizontal flourish extending to the right.

Andrew Richardson
Auditor-General

Contents

1	Executive summary	1
1.1	Introduction	1
1.2	Our review	1
1.3	What we found	2
1.4	What we recommended	4
2	Background	5
2.1	Cloud computing	5
2.1.1	Types of cloud service models	5
2.1.2	Cloud computing deployment models	6
2.2	Benefits of using cloud computing	7
2.3	Risks of adopting cloud computing	8
2.4	Relevant ICT frameworks and standards	9
2.5	SA Government's adoption strategy for cloud computing	9
3	Review objective, scope and approach	10
3.1	Our mandate	10
3.2	Our objective, scope and approach	10
4	Cloud computing summary	11
4.1	Cloud services adopted by agencies	11
4.2	Extent of agency applications and ICT services in the cloud	11
4.3	Cloud service models used by agencies	12
4.4	Deployment models used by agencies	12
4.5	Agency cloud computing spends	13
4.6	Internal resources allocated to support cloud services	14
4.7	Data classifications in cloud services	14
4.8	Geographical locations of agency cloud data	15
4.9	Most important consideration when evaluating cloud services	16
4.10	Agency adoption of new cloud services	17
4.11	Major challenges or concerns faced by agencies	18
4.12	Agency key security risks and threats	18
4.13	Agency cloud incident management	19

5	Cloud computing governance findings	20
5.1	Some agencies have not formally documented their policy and procedures for procuring and managing cloud services	20
5.2	Some agencies are not engaging their ICT team during the cloud evaluation process	21
5.3	One agency has not always performed a risk assessment before establishing a cloud service engagement	22
5.4	Some agencies are not performing an annual review of cloud provider independent assurance reports	22
5.5	Some agencies are not consistently establishing and documenting service level agreements in cloud contracts	23
5.6	Some agencies' user access management practices could be improved	24
	Appendix: Explanation of terms used in this Report	26

1 Executive summary

1.1 Introduction

Cloud computing delivers computing services over private network connections or the internet (the cloud) using several different service delivery and deployment models. It can involve service delivery for servers, software applications, storage, databases and networking.

The use of cloud computing can help agencies increase their business and innovation opportunities, lower their operational costs, introduce infrastructure efficiencies and increase operational scalability.

Rather than managing and administering IT services internally using agency resources and infrastructure, cloud computing services are typically outsourced to external service providers.

Like any outsourced arrangement in the public sector, risk remains with the agency. This is because the agency is the information asset owner. Agencies must still ensure that appropriate cyber security controls are applied to manage their cloud computing risks.

The SA Government's current ICT strategy has a number of objectives and actions regarding cloud computing to help 'enable agile approaches' to providing digital services to the public. This strategy is based on 'Cloud Right' as the preferred option for cloud adoption, meaning that agencies should assess the benefits of it before embracing it.

We use a number of technical terms in this report that we explain in Appendix 1.

1.2 Our review

This Report is not based on the results of an audit, as no testing was performed. We performed a high-level review of seven agencies to understand the level and maturity of their cloud computing governance processes. We also looked at the extent of services and data that these agencies have moved to a cloud computing environment, the type of cloud service models used and the associated costs.

From the information we gathered from these agencies we have made a number of observations and recommendations.

We found that the level of governance over cloud computing exercised by most of the agencies we reviewed could be improved in the following areas:

- some agencies do not perform risk assessments or relate with their ICT service team before engaging cloud computing service providers
- most agencies were not performing annual independent assessments of their cloud computing service provider arrangements

- some agencies had not developed or finalised cloud computing service level agreements (SLAs) for all established service provider engagements
- some agencies had not developed or finalised cloud computing policies and procedures to support their current arrangements.

The State’s current cloud computing approach could be strengthened through increased collaboration between agencies and centralised reporting to either the Department of the Premier and Cabinet or some form of inter-agency forum. The aim would be to help agencies while they move their services to the cloud by providing guidance, risk mitigation strategies, a more consistent approach to managing cloud computing and the integration of security governance.

1.3 What we found

Based on the responses we received from the agencies we sampled, we found the following.

Focus area	Details
Cloud computing summary (section 4)	<p>The seven agencies we reviewed maintain 178 cloud computing environments, comprising:</p> <ul style="list-style-type: none"> • Cloud services model: <ul style="list-style-type: none"> — 131 software as a service — 29 platform as a service — 9 infrastructure as a service — 9 combination of the above cloud service options (refer section 4.2) • Cloud deployment model: <ul style="list-style-type: none"> — 111 public cloud — 53 private cloud — 14 hybrid cloud <p>The data security classifications assigned to these cloud computing environments were:</p> <ul style="list-style-type: none"> • 118 OFFICIAL: Sensitive • 60 OFFICIAL. <p>On average 26% of the sampled agencies’ ICT services were in the cloud.</p> <p>Of the 178 cloud computing environments, 72 were defined by the agency as services that they considered to be key to their business operations. This included six financial applications, 64 operational applications and two that are a combination of both.</p> <p>Six agencies individually spend more than \$1 million on cloud services annually.</p>
	<p>Four of the sampled agencies advised that they did not have sufficient internal resources to properly support their cloud computing services.</p> <p>16% of the 178 cloud environments store data outside of Australia.</p>

Focus area	Details
	<p>The agencies we reviewed thought that the most important considerations when evaluating a cloud service solution were:</p> <ul style="list-style-type: none"> • data security (100%) • performance, features and functionality (100%) • cost (86%) • vendor experience and reputation (71%). <p>Six of the agencies we reviewed expect to increase their use of cloud computing services within 24 months.</p> <p>Major concerns or challenges that agencies can experience and that may impact their overall cloud adoption include:</p> <ul style="list-style-type: none"> • ICT budget limitations • loss of governance and data security • lack of internal resourcing • inability to attract and retain skilled ICT staff • accidental exposure of information or unauthorised access. <p>The top three security threats and risks highlighted by agencies using cloud computing services were:</p> <ul style="list-style-type: none"> • data loss or leakage (100%) • misconfiguration of cloud services (86%) • accidental exposure or unauthorised access (71%). <p>Six agencies advised us that they have a formal policy and procedures for incident management that is in line with the South Australian Cyber Security Framework (SACSF). The remaining agency has drafted a policy and procedure that is awaiting internal approval.</p> <p>Three agencies advised us that they experienced a small number of security incidents/disruptions in the last three to four years that specifically related to their cloud services providers.</p>
<p>Cloud computing governance findings (section 5)</p>	<p>Three agencies do not have formally documented policies and procedures for procuring and managing cloud computing services.</p> <p>Three agencies advised us that their ICT team was not always engaged in the cloud computing evaluation process.</p> <p>One agency advised us that a risk assessment was not always performed prior to establishing a formal cloud computing service engagement.</p> <p>Six agencies were not performing an annual review of cloud provider independent assurance reports.</p> <p>Five agencies were not consistently establishing and formally documenting agreed SLAs in cloud computing contracts.</p> <p>Two agencies were not regularly reviewing or monitoring their user access (including privileged users) on their cloud applications for appropriateness.</p>

1.4 What we recommended

Our recommendations to address the agency findings in section 5 of this Report include strengthening the following controls.

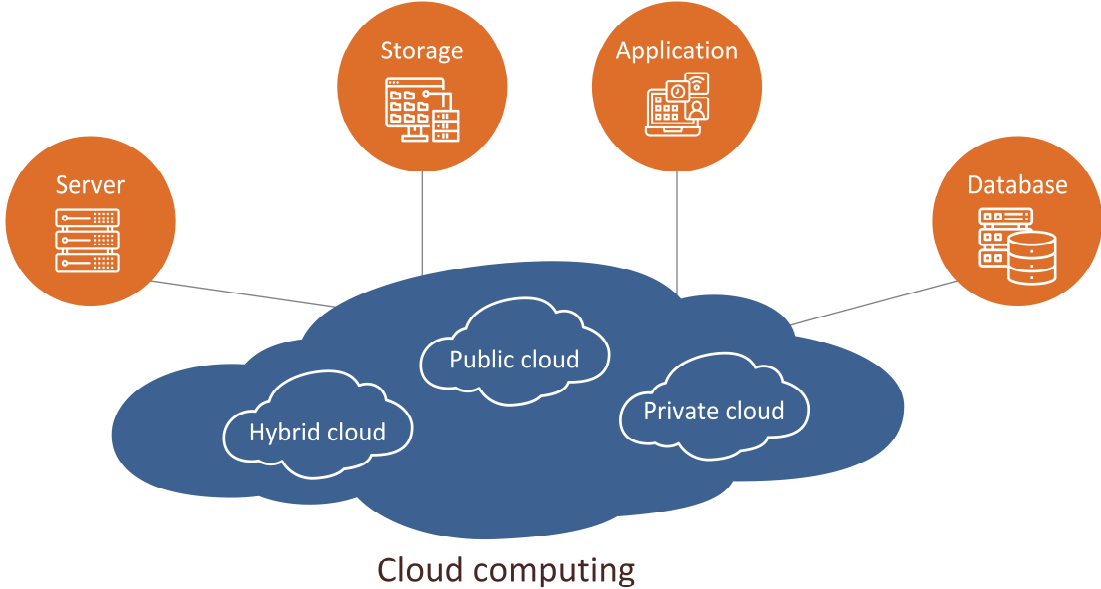
Focus area	Key recommendations
Policies and procedures on the use of cloud computing services	Agencies should develop policies and procedures to support their cloud computing activities.
ICT security team involvement during evaluation	Agencies should involve ICT security team(s) during the evaluation of new cloud services to ensure that their ICT security needs are met.
Risk assessments of cloud services	Agencies should perform a risk assessment before implementing a cloud computing service.
Certification of cloud service provider	Agencies should annually review the cloud service provider's security compliance certificates and independent ICT security audit reports. This could potentially be managed centrally at a whole of government level.
Contract management and controls	Agencies should ensure that contract arrangements for all cloud service providers include acceptable service levels for responsiveness, throughput, availability, reliability and redundancy. This could potentially be managed centrally at a whole of government level.
User access management	Agencies should conduct regular user access reviews of their cloud computing environments to ensure that access is appropriately applied.

2 Background

2.1 Cloud computing

Cloud computing delivers computing services over the internet (the cloud) using several different service delivery and deployment models.

Figure 2.1: Cloud computing environment



2.1.1 Types of cloud service models

Cloud computing environments can be delivered under several different service models, all with differing costs and responsibilities.

The following diagram shows the cloud service delivery models available and how responsibilities are assigned to the agency (shown in blue) and the service provider (shown in grey) under each option.

Figure 2.2: Cloud responsibility matrix

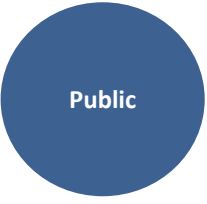

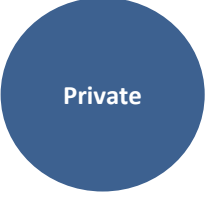

	Mostly agency responsibility		Mostly service provider responsibility	
	On-premises	Infrastructure as a service (IaaS)	Platform as a service (PaaS)	Software as a service (SaaS)
Application	Application	Application	Application	Application
Security	Security	Security	Security	Security
Database	Database	Database	Database	Database
Operating system	Operating system	Operating system	Operating system	Operating system
Server	Server	Server	Server	Server
Storage	Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking	Networking
Data centre	Data centre	Data centre	Data centre	Data centre

When considering the differences between on-premises infrastructure and cloud computing, the cloud creates the need for a shared responsibility model between agencies and service providers. To protect the information asset, it is important to clearly identify these responsibilities, including ownership arrangements and information custodians. Once responsibilities have been identified, controls can be applied based on the preferred service model and the assigned information classification.

2.1.2 Cloud computing deployment models

Cloud computing deployment models indicate how the cloud services are made available to users. Figure 2.3 explains the different models available.

Figure 2.3: Types of cloud computing deployment models

 <p>Public</p>	<p>A public cloud deployment model is where access to the cloud computing service is not restricted to a particular agency or community and is generally available to the public. This offers rapid access to affordable computing resources where users do not need to purchase hardware, software or supporting infrastructure.</p>
 <p>Community</p>	<p>A community deployment model is used by a specific community of consumers who have similar concerns and interests in which an organisation’s infrastructure is shared.</p>
 <p>Private</p>	<p>A private cloud is owned and operated by a service provider that controls the way virtualised resources and automated services are customised and exclusively used by a single agency.</p>
 <p>Hybrid</p>	<p>A hybrid cloud is where more than one cloud model (private, community or public) is integrated with on-premises infrastructure to provide greater flexibility between cloud solutions.</p>

A general comparison of cloud computing deployment model characteristics is provided in figure 2.4.

Figure 2.4: Cloud deployment models characteristics

Characteristic	Public	Community	Private	Hybrid
Setup and use	Handle in-house	Requires ICT professionals	Requires ICT professionals	Requires ICT professionals
Privacy and security	Low	Medium	High	Varies from low to high
Control of data	Low	Medium	High	Medium
Overall reliability	Medium	Medium	High	Medium to high
Flexibility and scalability	High	Medium	Medium	Very high
Cost	Lowest	Variable	Relatively high	Medium/Variable
Hardware	Third party	Variable	Variable	Medium/Variable

2.2 Benefits of using cloud computing

Cloud computing offers a range of potential benefits to agencies including flexibility, efficiency and strategic value. These characteristics are explained as follows:

- **Flexibility** – Agencies can adapt services to fit their needs, customise applications and access cloud services using the internet through:
 - **Scalability:** Cloud infrastructure can be scaled on demand to support fluctuating workloads.
 - **Deployment:** Assist agencies in determining infrastructure, ownership, access, and data storage space requirements.
 - **Storage options:** Agencies can choose public, private or hybrid storage offerings, depending on security needs and other considerations.
 - **Control choices:** Agencies can determine the level of control they exert over their systems when considering their available service options. These include SaaS, PaaS and IaaS, as defined in section 2.1.1.
- **Efficiency** – Agencies can make the best possible use of cloud applications and resources without worrying about underlying infrastructure costs or maintenance through:
 - **Cost effectiveness:** Agencies only pay for the service provider’s resources they use and save the cost of acquiring infrastructure (servers and other equipment), where applicable.
 - **Data accessibility:** Cloud-based applications and data are accessible from multiple locations and devices that have internet connections.
 - **Availability and redundancy:** Cloud services provide opportunities for a robust and modern infrastructure that reduces the potential for data loss and excessive equipment downtime.
- **Strategic value** – Cloud services may provide advantages to agencies by utilising innovative technologies through:
 - **Collaboration:** Agencies can collaborate and utilise services spread across various locations.

- **Streamlined work:** Cloud service providers manage the infrastructure, enabling agencies to focus on other priorities.
- **Regular updates:** Service providers regularly update offerings to give agencies the most up-to-date technology.

2.3 Risks of adopting cloud computing

Cloud computing can introduce many complexities into an agency's governance approach. Agencies should consider the use of a cloud service provider to be a partnership, not a method of risk transference. Their cloud services should be assessed as part of their risk assessment strategy.

When adopting a specific type of cloud service and deployment model, the following risks need to be considered:

- **Lack of transparency and visibility:** There is a risk that the cloud service provider may not provide sufficient information about their processes, operations, security controls, and underlying methodologies.
- **Reliability issues:** There is a risk that the cloud service provider may not be able to provide adequate service availability. This could impact agency operations, performance and business continuity, and could have financial cost impacts.
- **Lack of application portability:** Based on the potential dependency on a service provider and customised service arrangement, there is a risk that agencies may have significant challenges in migrating cloud services from one provider to another. This may also restrict the future ability to migrate data and services back to an in-house IT environment, if required.
- **Loss of confidentiality or data leakage:** There is a risk that data being stored on a service provider platform could potentially increase the opportunity for unauthorised access. Also, when services are transferred to another provider, fragments of data held under a prior arrangement may not have been successfully removed. This increases the risk of a data breach and may compromise data confidentiality.
- **Inadequate cloud provider viability:** There is a risk the cloud service provider could go out of business. This may leave agencies without an infrastructure, applications or data.
- **Insufficient cost considerations:** There is financial risk that cloud services provided to agencies could result in unexpected higher costs in the future. This may occur if agencies underestimate their requirements or do not consider higher cloud provider fees for additional services and other supporting costs, such as storage and connection upgrades. This could impact future financial benefits that agencies anticipated when adopting cloud services.
- **Lack of privacy agreement and SLA:** There is a risk that a cloud SLA has not been established before a service commences. This may increase complexity and uncertainty across areas of accountability, responsibility, security control and performance when meeting agency expectations.

- **Failure to outline security and data protection:** There is a risk that security and data protection expectations are not clearly defined between the service provider and the agency, which may increase the potential for compliance violation, malware infection and data breaches.
- **Misconfiguration of cloud services:** There is a risk that security control configurations across cloud services and their interfaces are not adequately applied. This may contribute to inappropriate data storage permissions, insufficient network functionality, deficient password requirements and unauthorised access to encryption keys.

Agencies need to consider these risks in their initial and ongoing cloud computing risk assessments.

2.4 Relevant ICT frameworks and standards

There are several ICT frameworks and standards to help agencies understand and identify their responsibilities and obligations when adopting cloud services. This includes helping to understand key risks and to safeguard the integrity, confidentiality, and availability of their data.

ICT frameworks and standards that include cloud computing guidelines include:

- SACSF
- ISO/IEC 27001 *Information Security Management Standard*
- National Institute of Standards and Technology
- Commonwealth Information Security Manual.

2.5 SA Government's adoption strategy for cloud computing

In November 2018, the SA Government released the Whole of Government ICT Strategy 2018. It sets the strategic direction for agencies' cloud computing services. This includes outlining a number of objectives and key actions that agencies need to adopt when implementing cloud computing digital services to the public.

This strategy gave agencies the opportunity to invest in cloud services that were deemed to be operationally suitable. It also confirmed that the SA Government had changed its focus from a 'Cloud First' position to a 'Cloud Right' approach. In practical terms this meant that agencies had a more flexible cloud approach, that embraces the business needs of the agency.

3 Review objective, scope and approach

3.1 Our mandate

The Auditor-General has authority to conduct this review under section 36(1)(a)(iii) of the *Public Finance and Audit Act 1987*.

3.2 Our objective, scope and approach

The objective of our review was to understand the implementation status of and governance arrangements for cloud computing across SA Government agency environments. As part of this review, we sought to gather some high-level information from several government agencies.

We randomly selected seven agencies across the SA Government sector and related with them to obtain specific information about their use of cloud computing services.

The initial information we sought from these agencies included:

- a list of all business systems that utilise cloud services
- the type of service model used for each cloud service eg IaaS, PaaS, SaaS
- the type of deployment model used for each cloud service eg private, hybrid etc
- the classification assigned to the agency data stored in each cloud environment (eg 'OFFICIAL',¹ 'OFFICIAL: Sensitive'² or 'Protected'³)
- costs and support arrangements associated with the operation and maintenance of each cloud environment
- whether independent compliance audit reports were provided and reviewed across each cloud service.

A further questionnaire was then sent to each participating agency to gain additional information specific to the management of their cloud computing environments.

We relied on the completeness and accuracy of the information provided by these agencies and did not perform validation testing.

¹ OFFICIAL as defined by the Commonwealth is information that was created or processed by the South Australian public sector with a low business impact.

² OFFICIAL: Sensitive as defined by the Commonwealth indicates that compromise of this type of information may result in limited damage to an individual, organisation or government generally.

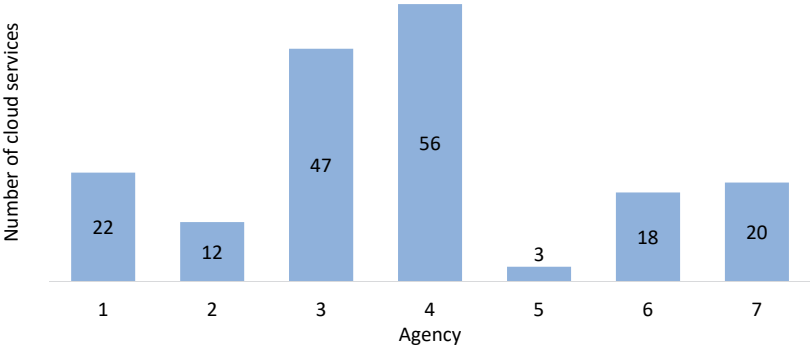
³ PROTECTED as defined by the Commonwealth indicates that compromise of the information may result in damage to state or national interests, organisations or individuals.

4 Cloud computing summary

4.1 Cloud services adopted by agencies

We identified 178 cloud service environments that were maintained by the seven agencies we reviewed.

Figure 4.1: Agency cloud environments reviewed

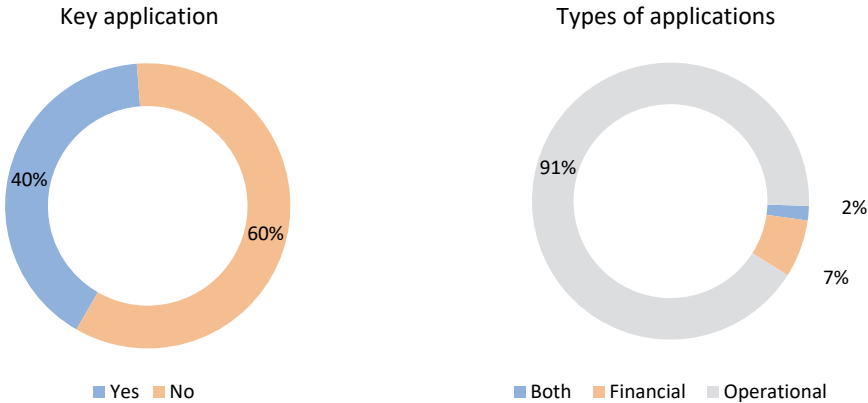


4.2 Extent of agency applications and ICT services in the cloud

Knowing the importance of each cloud application helps an agency to understand the associated risks and any potential negative impacts on their data and underlying business operations.

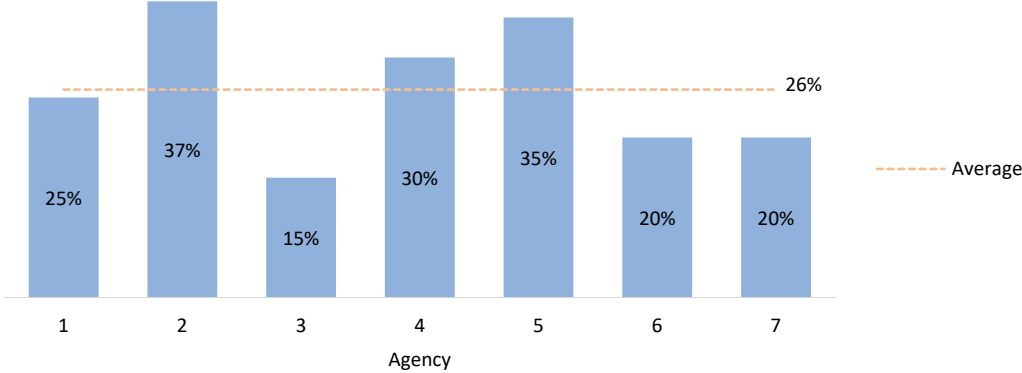
For the seven agencies we reviewed, 72 of their 178 cloud computing services were defined by the agency as being services they considered to be key to their business operations. They include six financial applications, 64 operational applications and two that are a combination of both.

Figure 4.2: Types of applications in the cloud



In addition, for our sample agencies, an average of 26% of the total agency ICT services are currently held in the cloud.

Figure 4.3: Agencies ICT services in the cloud

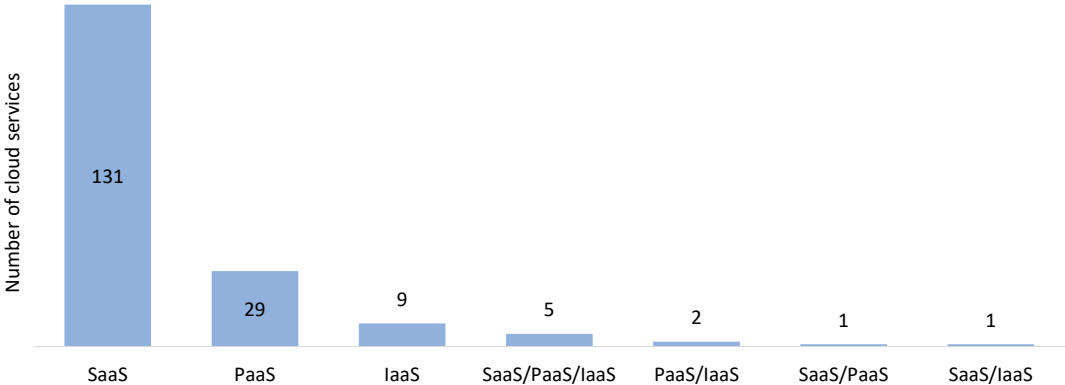


4.3 Cloud service models used by agencies

There are three main cloud service models: IaaS, PaaS and SaaS. The responsibilities of agencies and service providers will depend on the service adopted.

Of the 178 identified cloud services, we confirmed that 131 were SaaS, 29 were PaaS, nine were IaaS and the remaining nine were a combination of these service models. Each of these models has potential benefits and risks, which we discuss in sections 2.2 and 2.3.

Figure 4.4: Cloud services used by agencies

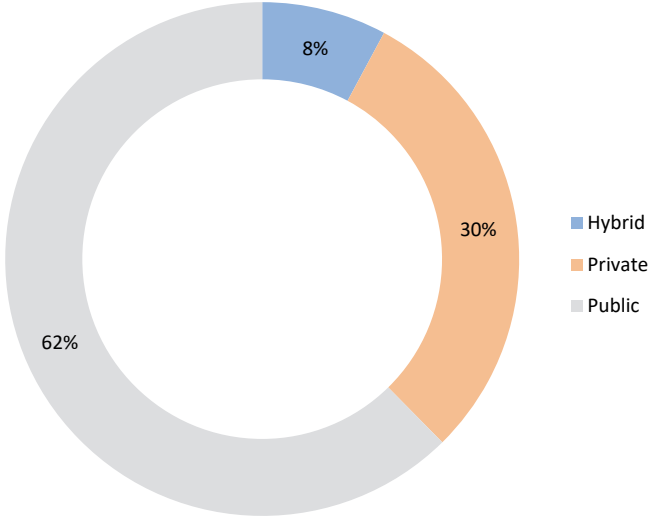


4.4 Deployment models used by agencies

There are several cloud deployment models, including public, private and hybrid models. The model used determines the responsibilities for controlling the infrastructure and where its data is stored.

In the agencies we reviewed there were 111 public, 53 private and 14 hybrid models.

Figure 4.5: Cloud deployment models used by agencies



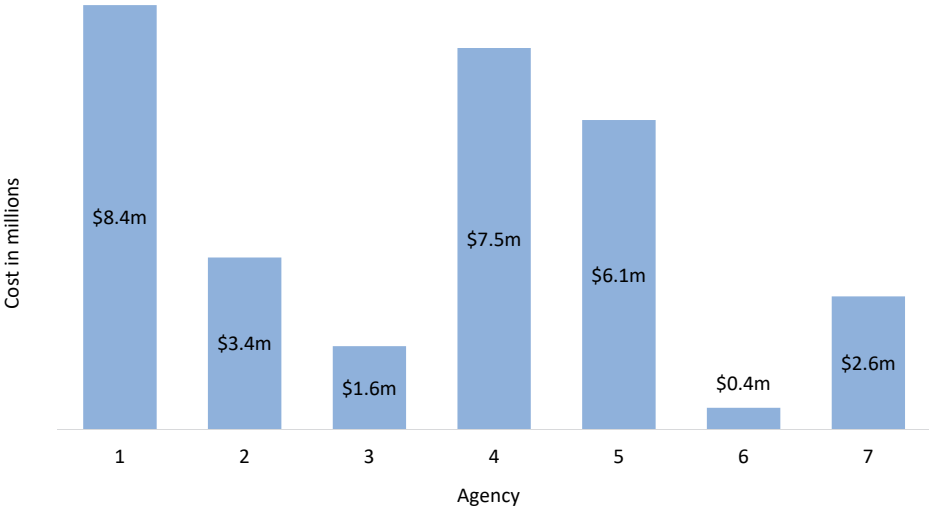
Public cloud environments often have multiple data storage systems located in several data centres, sometimes separated by country or geographical regions. Consequently, this makes it difficult for agencies to easily track the specific location of all data.

4.5 Agency cloud computing spends

We asked agencies about the maintenance and support costs associated with managing their cloud services. For the seven agencies we reviewed, the total cloud services costs were around \$30 million per annum.⁴

Six agencies are currently spending more than \$1 million annually on their cloud services.

Figure 4.6: Annual agency cloud costs



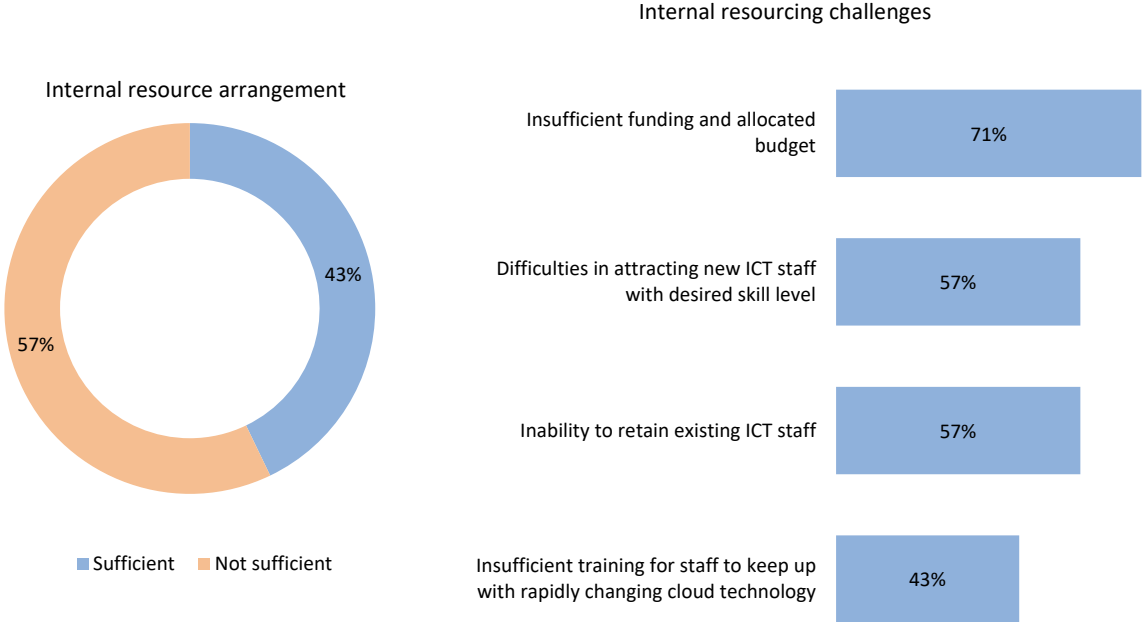
⁴ These figures were provided by the agencies we reviewed and are unaudited.

4.6 Internal resources allocated to support cloud services

Most agencies confirmed that they intend to increase their use of cloud services in the future. Five agencies advised us that they do not have sufficient internal resources and expertise to support their current and future cloud service needs. These agencies indicated that they face several challenges in meeting their resource requirements, including:

- insufficient funding and allocated budget
- difficulties attracting new ICT staff with the desired skill level
- inability to retain existing ICT staff
- lack of specialist ICT training.

Figure 4.7: Internal resourcing challenges faced by agencies

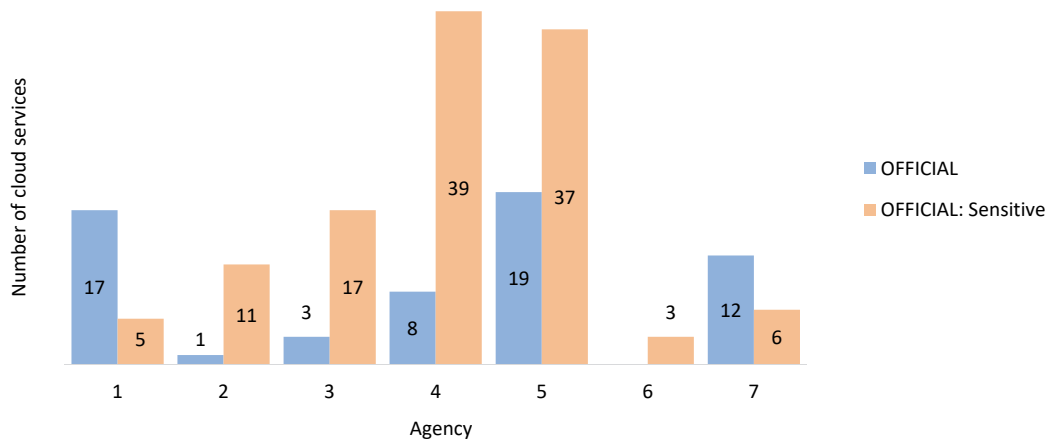


4.7 Data classifications in cloud services

It is important for agencies to formally classify their information assets in line with the SACSF and the South Australian Information Classification System (ICS). Data classifications help agencies determine the value and confidentiality requirements of their data.

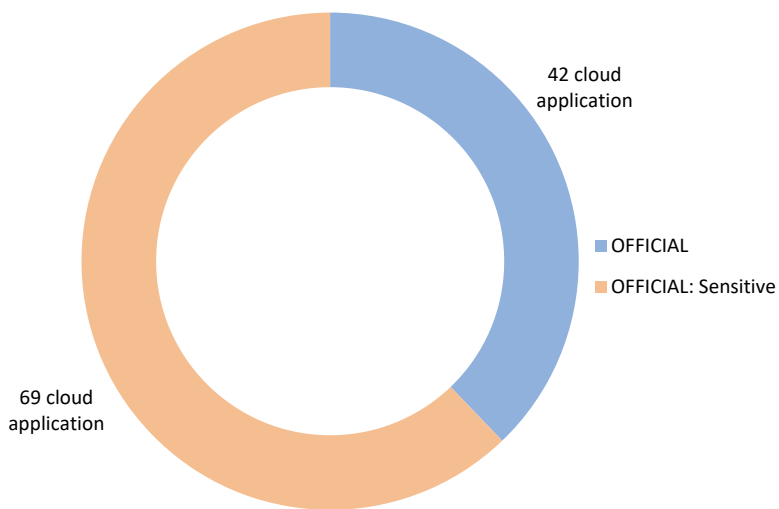
We noted that of the 178 cloud computing environments identified, 118 contain or can access information classified as OFFICIAL: Sensitive.

Figure 4.8: Cloud services and data classifications



Of the 111 cloud applications that are using the public deployment model, 69 cloud applications contain information classified as OFFICIAL: Sensitive.

Figure 4.9: Agency data in public cloud environments

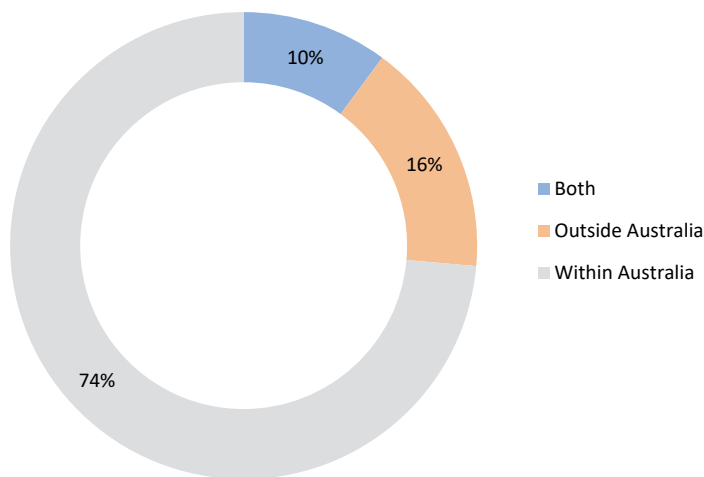


4.8 Geographical locations of agency cloud data

All of the seven agencies we reviewed confirmed that they use cloud services that store data at both onshore and offshore locations.

Of the 178 cloud services identified, 131 maintain data within Australia, 29 outside Australia and the remaining 18 are a combination of both.

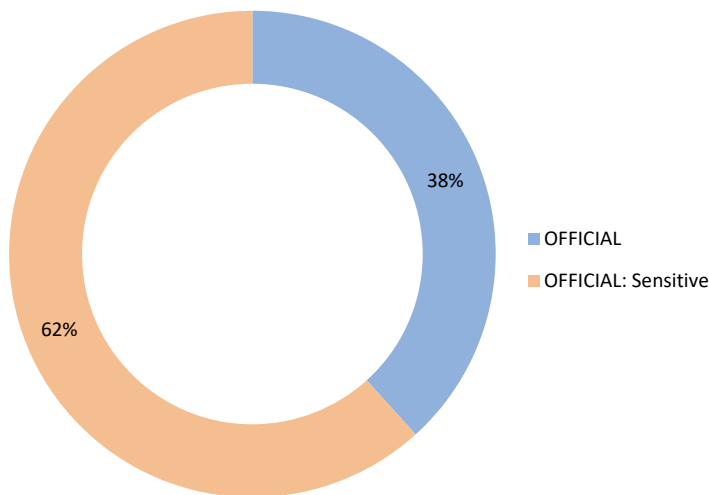
Figure 4.10: Geographical locations of agency cloud data



SACSF Ruling 2 *Storage and processing of South Australian Government information in outsourced or offshore ICT arrangements* require that information that is classified as PROTECTED or above cannot be processed or stored outside of Australia unless the State’s Principal Contract Administrator has provided consent.

Of the 47 cloud services that store data offshore, 29 hold data classified as OFFICIAL: Sensitive and the rest hold data classified as OFFICIAL. We were advised that no data was classified as PROTECTED.

Figure 4.11: Agency data stored in offshore location

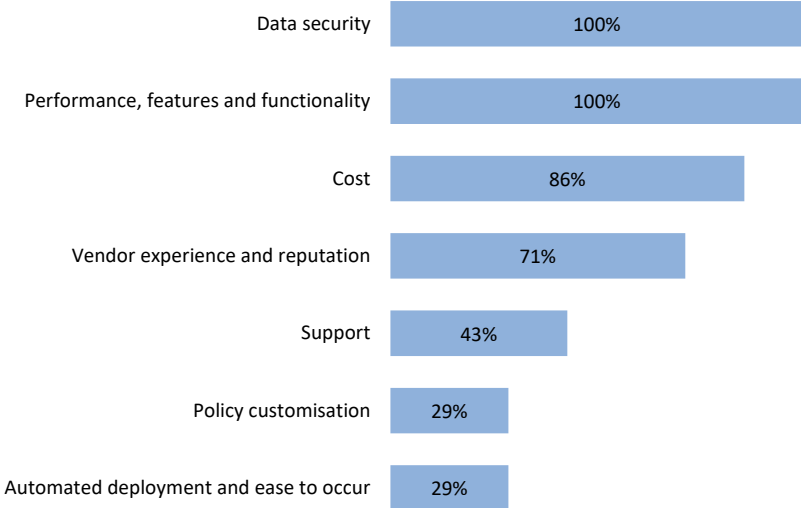


4.9 Most important consideration when evaluating cloud services

Agencies should consider their business needs and perform a full risk assessment before using cloud services.

When we asked agencies what they thought the most important consideration was when evaluating a cloud solution, all of them responded that data security (100%) and performance, features and functionality (100%) were the main priorities, followed by cost (86%), and vendor experience and reputation (71%).

Figure 4.12: Agency key considerations when evaluating cloud services

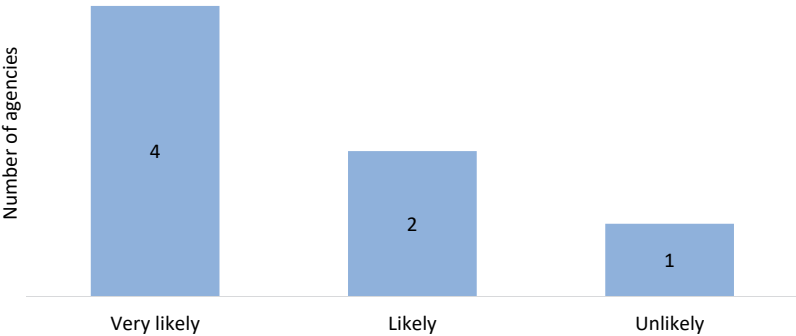


4.10 Agency adoption of new cloud services

The SA Government altered its strategy from ‘Cloud First’ to the ‘Cloud Right’ in November 2018.

Of the seven agencies we reviewed, most indicated that they are intending to increase the use of cloud computing services in the future. Figure 4.13 shows the likelihood of them deploying new cloud services over the next two years.

Figure 4.13: Likelihood agencies will increase the use of cloud services over the next two years



4.11 Major challenges or concerns faced by agencies

Agencies have significantly increased their adoption of cloud services in the last five years. Despite this, there are still some challenges when considering future cloud services for their business operations.

We asked agencies what ICT-related concerns and challenges they were currently experiencing when considering the future adoption of cloud services. They indicated:

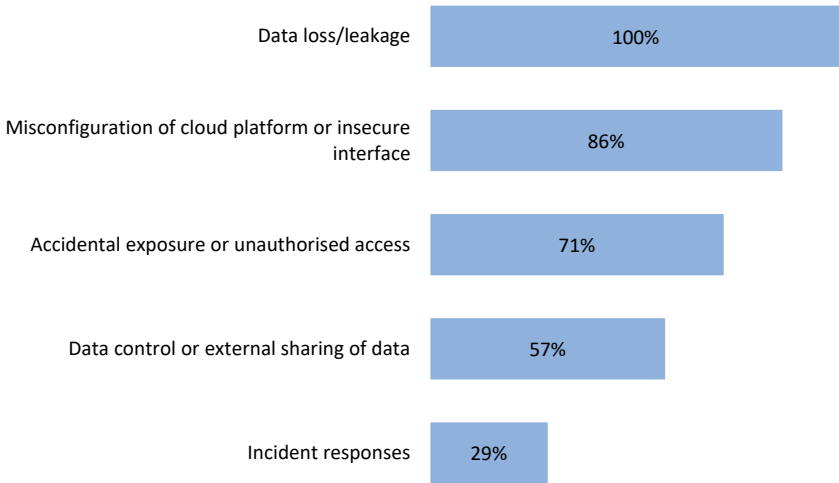
- ICT budget limitations
- loss of governance and data security
- lack of internal resourcing
- inability to attract and retain skilled ICT staff
- accidental exposure of information or unauthorised access
- poor performance and unavailability of services.

4.12 Agency key security risks and threats

As noted in section 4.9, data security within the cloud was identified as a key agency concern. We sought further details regarding agency data security risks and threats.

All of the agencies we reviewed advised us that they have experienced several security threats within their cloud environments with the potential to impact the completeness, integrity or availability of their data. Their key data security risks in a cloud environment were data loss or leakage (100%)⁵, security gaps within cloud system settings (86%) and accidental exposure or unauthorised access (71%).

Figure 4.14: Agency key security risks of cloud services



⁵ We were not advised of any actual instances of data loss or leakage for the agencies that we reviewed.

4.13 Agency cloud incident management

Of the seven agencies we reviewed, six advised us that they have a formal policy and procedures for incident management that is in line with the SACSF. The remaining agency has drafted a policy and procedure, but they are yet to be formalised.

When we asked whether agencies had any security incidents related to their cloud services, three agencies responded that a small number of minor incidents were experienced over the past three to four years. These incidents related to brief service disruption or outages across a small number of cloud service providers. These disruptions caused some impacts on agency business processes conducted through these services.

5 Cloud computing governance findings

5.1 Some agencies have not formally documented their policy and procedures for procuring and managing cloud services

What we recommend

Agencies should develop a cloud computing policy and procedure describing their procurement and ongoing control requirements for cloud services. Agencies should ensure that controls are aligned with established frameworks such as the SACSF and the ISO/IEC 27001.

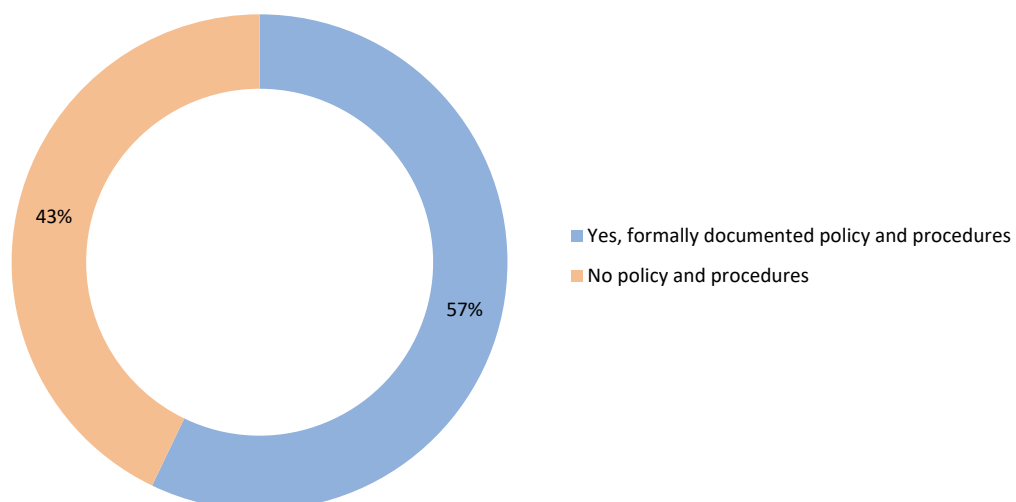
When defining the policy requirements for procuring and managing cloud services, the following aspects should be considered:

- clearly identify the business processes and data that management deems appropriate to be supported by cloud services
- establish a list of authorised approvers who can procure cloud services
- define requirements to identify and use approved cloud vendors
- engage with the ICT team to help define requirements and perform a detailed risk assessment
- communicate and define guidance on the management of cloud vendors
- define requirements to regularly conduct a risk assessment of cloud services.

Findings

We asked the agencies we reviewed whether they had a formally documented policy and procedure for procuring and managing cloud computing services. We found that three of the seven agencies did not.

Figure 5.1: Policy and procedures



Why this is important

A policy and procedure for procuring cloud services helps an agency’s decision-making process when determining the suitability of potential cloud services. In addition, establishing expected minimum ICT controls helps to protect the confidentiality, integrity and availability of the agency’s data.

5.2 Some agencies are not engaging their ICT team during the cloud evaluation process

What we recommend

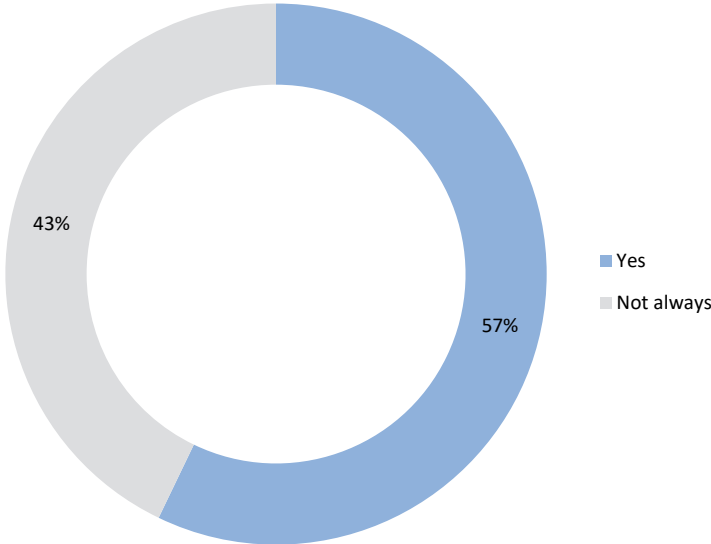
To ensure agency ICT security needs are met, cloud computing procurement processes should be updated so that business units actively engage their ICT team during the evaluation process.

Finding

We asked agencies whether their business units engaged their ICT team before procuring cloud computing services to support their business processes.

Of the seven agencies we reviewed, three advised us that they did not sufficiently engage their ICT team in the evaluation and implementation of their cloud service proposals.

Figure 5.2: Agency ICT security team involved in the cloud computing evaluation process



Why this is important

An agency’s ICT team can help in the early identification of ICT security gaps, determining cloud and network risks and providing advice for proposed corrective action. This can help agencies to make better risk-based decisions when evaluating cloud services.

5.3 One agency has not always performed a risk assessment before establishing a cloud service engagement

What we recommend

Agencies should perform a risk assessment before establishing of a formal engagement for any cloud service. This will help them to make informed decisions on whether to invest in a cloud service.

Finding

The relationship between an agency and a cloud computing service provider should be considered a partnership. The partnership should focus on improving the agency's service offering and implementing appropriate controls to protect the confidentiality, integrity and availability of the information asset.

In this partnership the risk is not transferred to the service provider. Ultimately information asset ownership remains with the agency, and it therefore needs to assess all associated risks and identify effective mitigating controls.

Section 2.11 of the SACSF states that a risk assessment must be performed by an agency before implementing any cloud computing service.

Of the seven agencies we reviewed, one agency responded that it did not always perform a risk assessment of their cloud services before implementing them.

Why this is important

An initial risk assessment helps the agency to better understand the risks and benefits of partnering with the service provider. It also helps determine minimum acceptable service offerings and security controls that must be established to ensure that any risks are appropriately addressed and that the provider can fulfil service quality expectations.

5.4 Some agencies are not performing an annual review of cloud provider independent assurance reports

What we recommend

Agencies should regularly review their cloud service provider's independent assurance reports. This will confirm the adequacy of any security controls applied, to understand where control risks exist and any mitigation activities that need to be applied.

Finding

Section 2.11 of the SACSF states that agencies rated at Tier 3 and above are expected to undertake:

A formal independent assurance report relating to the risk associated with cloud service is obtained on an annual basis where the cloud service is supporting:

- *Critical services*
- *Services with high availability or integrity requirements*
- *Services storing sensitive information or higher*
- *Services with a moderate or higher risk profile*

We confirmed that all seven of the agencies we reviewed are categorised as Tier 3. However, only one agency advised us that it annually reviews its cloud service providers' independent assurance reports for all their cloud environments.

The remaining six agencies advised us that they only review these reports at the initial implementation phase or after a major upgrade. These agencies therefore do not routinely seek or review these reports annually as required.

Why this is important

Reviewing independent assurance reports annually gives agencies better assurance that their cloud providers continue to implement appropriate controls to secure their data.

Examples of independent assurance reports include compliance with ISO/IEC 27001 and a Service Organization Control 2 (SOC 2) report. These reports include IT aspects such as security, availability, processing integrity, confidentiality or privacy.

5.5 Some agencies are not consistently establishing and documenting service level agreements in cloud contracts

What we recommend

Agencies should ensure that provisions for SLAs are included in contracts with cloud service providers. Agencies should regularly monitor these agreed performance and service quality targets.

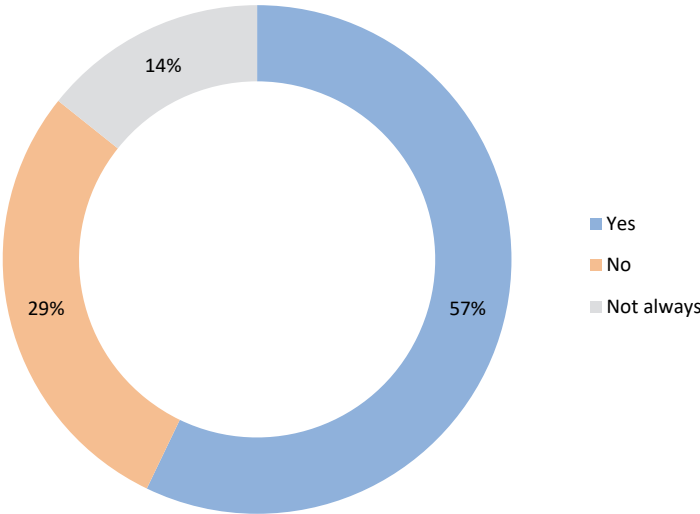
Finding

Before initiating any outsourced IT services, including cloud services, service requirements should be established. It is also important for agencies to consider how they will obtain assurance over the services they expect to receive. Best practice would be to include provisions for SLAs in the contract to set and measure agreed performance and service quality targets. They might also include agency and cloud provider responsibilities for key security controls. Agencies should regularly monitor these SLAs and other required responsibilities.

We found that three agencies that were not subject to their cloud providers' standard global SLA requirements had not always established and/or formally documented agreed SLAs and other related requirements for all their cloud computing services, including:

- a detailed list of all cloud services to be provided
- the expected level of availability (uptime)
- cloud platform performance or response time
- incident response and resolution times
- details highlighting redundancy for reducing the potential for single point of failure
- details of security compliance standards implemented.

Figure 5.3: Agency establishes formally documented SLAs for all cloud services



Why this is important

Failing to develop and agree an SLA may result in issues for the agency if the cloud computing service does not meet the needs and demands of its business. Areas for discussion between agencies and service providers as part of ongoing SLAs and contract management should include matters such as performance and availability.

5.6 Some agencies' user access management practices could be improved

What we recommend

Agencies should conduct regular reviews of user accounts across their cloud services to ensure access is appropriately managed.

Finding

The level of access within applications, operating systems and databases for agency users may vary depending on the cloud service model adopted.

Of the seven agencies we reviewed, two were not regularly reviewing their cloud application user accounts, including privileged users, to confirm their appropriateness for user job roles/ functions.

These two agencies were also not monitoring the activities performed by their privileged users (administrators).

Why this is important

Not regularly and thoroughly reviewing user access increases the risk of users retaining inappropriate access to systems and potentially performing unauthorised activities. This could lead to compromise of the confidentiality, integrity or availability of sensitive information within the system.

Not actively monitoring privileged user activities also reduces the likelihood of unauthorised or inappropriate access or system changes being promptly identified.

Appendix Explanation of terms used in this Report

Term	Description
Cloud computing	The delivery of IT services including servers, storage, databases, networking and software over private network connections or the internet (the cloud).
Cloud computing services	ICT services that are provisioned and accessed from a cloud service provider.
Cloud First	ICT operational strategy where an agency seeks to move all or most of its infrastructure to cloud-computing platforms over time, instead of maintaining on-premise locally resourced servers.
Cloud Right	ICT operational strategy used to focus on establishing a preferred option, which may incorporate a flexible cloud approach, that embraces the business needs of the agency.
Commonwealth Information Security Manual	The Commonwealth Government’s Australian cyber security centre has developed priorities strategies and guidance to help IT security professionals mitigate cyber security incidents caused by various external and/or internal treats.
Cyber security	Measures used to protect the confidentiality, integrity and availability of systems and data.
Information classification system	<p>The South Australian Information Classification System (ICS) is used to help agencies assess the confidentiality, integrity and availability of their information assets and ensure its appropriate protection. Information is classified into different categories including:</p> <ul style="list-style-type: none"> • OFFICIAL – as defined by the Commonwealth, this is information that was created or processed by the South Australian public sector with a low business impact. • OFFICIAL: Sensitive – as defined by the Commonwealth, compromise of this type of information may result in limited damage to an individual, organisation or government generally. • PROTECTED – as defined by the Commonwealth, compromise of this type of information may result in damage to state or national interests, organisations or individuals.
Information custodian	The information custodian is the individual or group assigned responsibility for managing a set of information (refer to SACSf Appendix B).

Term	Description
Infrastructure as a service (IaaS)	The National Institute of Standards and Technology defines IaaS as the ‘capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer 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 (eg host firewalls)’.
<i>ISO/IEC 27001 Information Security Management Standard</i>	ISO/IEC 27001 is an international specification detailing best practice requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS).
Key performance and availability indicators (KPIs)	KPIs indicate the progress achieved against an intended result and focus on strategic and operational improvement, on such matters as thresholds, uptime, system availability, response time, and problem resolution.
National Institute of Standards and Technology (NIST)	NIST is an international body that offers standards and technical guidelines to assist and provide a uniform cybersecurity direction/approach for the protection of data.
On-premises	The use of software and technology that is located within the physical confines of an enterprise.
Ownership arrangements	The SACSf requires formalisation of ownership arrangements. This includes identifying and recording the information assets according to the South Australian Information Classification System (ICS) and assessing and documenting all related cyber security risks.
Platform as a service (PaaS)	NIST defines PaaS as the ‘capability provided to the consumer 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 consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment’.

Term	Description
Scalability	The ability to increase and decrease demand within the cloud, through processing, networking, infrastructure, and software, to meet changing needs.
Service level agreement (SLA)	SLA is a technical service performance contract between a service provider and an agency that outlines minimum levels of expected services and associated responsibilities between parties.
Software as a service (SaaS)	The NIST defines SaaS as the ‘capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (eg 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’.
South Australian Cyber Security Framework (SACSF)	This is a risk-based framework developed by SA Government to assist agencies with preserving the confidentiality, integrity, and availability of information by applying appropriate management processes.
System and Organization Controls (SOC) Type 2 reports	System and Organization Controls (SOC) Type 2 reports are internal risk management controls reviews that assess the trust and transparency of service providers design and testing of established ICT security controls to safeguard customer data, over a specific period.
Tier level	Agency tier level is defined by the SACSF on their individual risk appetite, classification of information held, criticality of services provided, size and resourcing capability and perceived overall risk.

