Contents

PART 1  EXECUTIVE SUMMARY .................................................................................................................... 3
PART 2  INTRODUCTION ............................................................................................................................... 4
PART 3  CONTEXT ......................................................................................................................................... 5
   3.1 NSW Government and cloud ........................................................................................................... 5
   3.2 The cloud market ............................................................................................................................ 6
PART 4  CLOUD-ENABLED BUSINESS TRANSFORMATION ............................................................................. 7
PART 5  PROJECT IMPLEMENTATION KEY CONSIDERATIONS ........................................................................ 9
   5.1 Organisational assessment .............................................................................................................. 9
      5.1.1 Business objective and business need ..................................................................................... 9
      5.1.2 Organisational readiness ....................................................................................................... 10
      5.1.3 Economic and financial appraisal ........................................................................................... 11
      Total cost of ownership ................................................................................................................... 12
      Cost considerations ......................................................................................................................... 12
      Economies of scale ......................................................................................................................... 14
      Shifting from capex to opex ............................................................................................................ 14
   5.2 Market assessment ........................................................................................................................ 15
      5.2.1 Understanding the cloud market ........................................................................................... 15
      5.2.2 Ensuring appropriate procurement processes ........................................................................ 16
   5.3 Change implication ........................................................................................................................ 17
      5.3.1 Organisational change ............................................................................................................ 17
      5.3.2 Skills, capability and cultural change ....................................................................................... 18
   5.4 Data ............................................................................................................................................. 19
      5.4.1 Security, privacy and data location .......................................................................................... 19
      5.4.2 Access to data and business continuity .................................................................................. 21
   5.5 Regulation and compliance ......................................................................................................... 22
      5.5.1 Public access to government information .............................................................................. 22
      5.5.2 Record keeping obligations .................................................................................................... 22
   5.6 Technical considerations ............................................................................................................. 23
      5.6.1 Bandwidth, WAN and LAN requirements .............................................................................. 23
      5.6.2 Data and systems integration ................................................................................................. 24
      5.6.3 Mobility ................................................................................................................................ 25
   5.7 Transition ...................................................................................................................................... 25
      5.7.1 Licensing arrangements .......................................................................................................... 25
      5.7.2 Migration in ............................................................................................................................ 26
      5.7.3 Migration out .......................................................................................................................... 27
      5.7.4 Avoiding vendor lock-in ......................................................................................................... 28
PART 6  KEY FINDINGS ............................................................................................................................... 29
PART 7  DOCUMENT CONTROL .................................................................................................................. 30
PART 1 EXECUTIVE SUMMARY

Cloud-based as-a-service offerings present significant opportunities for government to benefit from scalable multi-tenanted environments, lower costs per-user, improved business processes and better value for money.

The NSW Government ICT Strategy recognises that improved government service delivery and better value ICT investment will be underpinned by a new, strategic approach to the sourcing and management of public sector ICT. This includes the adoption of cloud-based services where it is appropriate for agency business needs. The NSW Government Cloud Services Policy and Guidelines gives guidance to NSW Government agencies to assist in determining which cloud delivery model is best suited for their business needs.

The Cloud Pilot Project Final Report presents an analysis of cloud implementations by five NSW Government agencies (Cloud Pilot agencies), which were monitored over the course of a ten month period, from January to October 2013.

This report is based on observations captured at project team meetings and by conducting interviews with key project team members, stakeholders and vendors. The results of the Cloud Pilot Project are presented as lessons learned throughout the report. There are also seven key findings for the consideration of the NSW Government ICT Leadership Group and the ICT Board.

The objective of the Cloud Pilot Project was to test and understand the implications for the NSW public sector of transitioning to cloud-based as-a-service solutions. As such, observation of five Cloud Pilot agencies has demonstrated that as-a-service sourcing has the potential to deliver the following benefits:

- **Cost** – moving from customising and operating in-house ICT, to using the best available ‘off the shelf’ commodity solutions will reduce the total cost of ownership.
- **Agility** – on-demand, scalable and flexible services that can be implemented quickly provide agencies with the ability to respond to changing requirements and peak periods.
- **Efficiency** – improving the efficiency of internal business processes has long term benefits for the business, offers long term savings opportunities and enables uptake of other cloud-based service more easily.
- **Innovation** – innovation will be facilitated by economies of scale, as well as rapid and continuous system development and improvement.
- **Resilience** – a highly resilient environment reduces the potential for system failure.

Overall, certain factors that contributed to the successful implementation of cloud-based services by the Cloud Pilot agencies are:

- organisational readiness, including collaboration with divisions across the whole agency
- understanding and a clear articulation of the business objective(s)
- willingness to transform the business if required, supported by consistent senior executive leadership
- change management planning
- due diligence of the agency’s technical and business requirements.
PART 2  INTRODUCTION

The NSW Government ICT Strategy recognises that improved government service delivery and better value ICT investment will be underpinned by a new, strategic approach to the sourcing and management of public sector ICT. This includes the adoption of cloud-based services where it is appropriate for agency business needs. The objective of the Cloud Pilot Project was to test and understand the implications for the NSW public sector of transitioning to cloud-based as-a-service solutions. The Cloud Pilot Project Final Report presents an analysis of cloud implementations by five NSW Government agencies (Cloud Pilot agencies), which were monitored over the course of a ten month period, from January to October 2013.

This report is based on observations captured at project team meetings and by conducting interviews with key project team members, stakeholders and vendors. The results of the Cloud Pilot Project are presented as lessons learned throughout the report. There are also seven key findings for the consideration of the NSW Government ICT Leadership Group and the ICT Board.

The five Cloud Pilot agency projects were as follows:

1. **Fire and Rescue NSW – email as-a-service**

   Fire and Rescue NSW (FRNSW) trialled the migration of 7,500 staff (at the time of writing 600 staff had been migrated, with the remaining staff migrated by Christmas) from Groupwise email managed in-house, to the Microsoft 365 email component hosted in the cloud. An archive of all emails continued to be managed in-house. The business objectives were to lower costs and improve internal service delivery of email to end-users.

2. **NSW Department of Trade and Investment, Regional Infrastructure and Services (DTIRIS) – ERP as-a-service**

   DTIRIS partnered with SAP to consolidate its multiple existing finance, payroll and enterprise resource planning (ERP) systems into a single cloud-based platform. SAP provided DTIRIS the ERP system as-a-service, with data stored offshore with the exception of payroll data, which is stored in a data centre located in NSW. The key objective of the ERP project was to replace a number of existing, poorly functioning and high risk systems with a single solution, enabling all entities within the agency to deliver core finance, procurement, project management, human resources and payroll processes. DTIRIS approached this project as a business transformation project. It was led and overseen by key senior executives.

3. **Businesslink – email as-a-service**

   Businesslink initiated a project to replace an internally built and managed email system, with cloud-based Microsoft 365 email. Businesslink is a shared service provider, and the plan was to use the software internally with Businesslink staff and then roll it out to its customers (other agencies within the family and community services cluster). The vendor’s assessment of the remediation work required to integrate the offering increased significantly, and the project has not yet been implemented.

4. **The WorkCover Independent Review Office (WIRO) – infrastructure as-a-service**

   WIRO implemented cloud-based infrastructure as-a-service to host its case management software. As an office established to review decisions of its parent WorkCover, WIRO’s main business objective was to ensure independence from WorkCover, experience rapid implementation of the solution and minimise cost.

5. **ServiceFirst Proof of Concept – messaging as-a-service (two projects) and desktop as-a-service**

   ServiceFirst trialled three separate proof of concept (POC) projects – Fronde (Google-based solution) and Unisys (Microsoft Exchange-based solution) provided messaging as-a-service solutions and HP provided a desktop as-a-service solution to a limited number of users over a period of three months.
PART 3  CONTEXT

3.1 NSW Government and cloud

Government ICT investment is increasingly influenced by budget constraints, rapidly ageing technology and higher community expectations in relation to service delivery. Adopting commercially available cloud-based services has the potential to generate savings with scalable, pay-as-you-go solutions. They also provide an opportunity for the government to improve business processes and efficiency in order to take advantage of new technologies, which provide the flexibility and agility to respond to changing service delivery requirements.

The NSW Government released the Cloud Services Policy and Guidelines in August 2013, gives guidance to NSW Government agencies when evaluating cloud-based services for ICT procurements in order to determine the ICT delivery model that provides the best value sustainable investment, taking account of the full range of cost-benefit considerations. The document is intended to provide guidance to agencies to assist in determining which cloud delivery model is best suited for their business needs. The Policy was informed by the work undertaken to develop standard contractual arrangements for procuring ICT ‘as a service’ under the Procure IT Framework and will be further informed by the key findings of this report.

Cloud-based as-a-service offerings present significant opportunities for government to benefit from scalable multi-tenanted environments, lower costs per-user, improved business processes and better value for money.

NSW Government has traditionally sourced its information and communications technology (ICT) through either in-house (custom buy and build) solutions, or managed services hosted on internal servers by externally skilled technical staff.

Generally, agencies customised products to suit their differing internal technical environments. This has resulted in a NSW public sector environment where agencies may have different integration architecture even though they may be using the same ICT solutions. This means that it is more complex (and more costly) to share solutions between agencies, increase or decrease the number of users, and in some cases move to different vendors.

Cloud-based services offer government a third as-a-service (cloud-based) ICT sourcing option. As-a-service provides opportunities for agencies to achieve better value, flexibility and reliability, and make sustainable service delivery improvements. It should be emphasised that most of the considerations required when deciding to move to cloud-based services are the same as deciding whether to source in-house or managed services.

The Cloud Pilot Project has demonstrated that as-a-service sourcing has the potential to deliver the following benefits:

- **Cost** – moving from customising and operating in-house ICT, to using the best available ‘off the shelf’ commodity solutions reduces the total cost of ownership.
- **Agility** – on-demand, scalable and flexible services that can be implemented quickly provide agencies with the ability to respond to changing requirements and peak periods.
- **Efficiency** – improving the efficiency of internal business processes has long term benefits for the business, offers long term savings opportunities and enables uptake of other cloud-based service more easily.
- **Innovation** – innovation is facilitated by economies of scale, as well as rapid and continuous system development and improvement.
- **Resilience** – a highly resilient environment reduces the potential for system failure.
3.2 The cloud market

The different nature of each of the projects implemented by the five Cloud Pilot agencies highlighted that there are many different market players offering cloud-based products and services. Of the five projects observed, there were three market players identified: platform owners, service providers and niche consultants. The level of support required by the agency, internal capability level, budget and technical environment varied between the agencies, therefore Cloud Pilot agencies chose different market players to contract with. Each of these players offers different levels of service.

The market players identified by Cloud Pilot agencies are as follows:

- **Platform Owners** – offering a licence to use the product on a per-user basis.
- **Service Providers** – offering cloud-based products as well as a suite of services around that product. Product price would usually be more than the price for the platform owners as they offer additional services (and consequently additional service fees) on top.
- **Niche Consultants** – specialise in integration architecture (systems or application integration), web applications (plug-and-play applications), data migration process, and other areas of specialisation. It is considered that there may be a potential role for existing corporate and shared service providers to assist agencies to adapt their internal technical environment to for the use of cloud services (thereby becoming niche consultants to agencies).

Based on the findings of this pilot, the maturity of the agency (rather than the maturity of the market or offerings available) and the agency’s business objectives are the main driver for selecting a vendor. An initial organisational readiness assessment, a thorough understanding by the agency of what would be required to adjust their internal technical environment, and a plan for managing the change to the cloud-based services, were all factors that contributed to the successful implementation of projects by the Cloud Pilot agencies.
PART 4 CLOUD-ENABLED BUSINESS TRANSFORMATION

As well as immediate benefits associated with cloud implementations, transitioning to an as-a-service model has broader benefits. It has been observed through the Cloud Pilot Project that as-a-service offerings provide an opportunity for agencies to reconsider their business process design and enterprise architecture, as well as organisational and cultural change initiatives. This will in turn improve efficiency, increase service capability and place greater emphasis on strategic business objectives.

One way in which cloud-based services offer savings opportunities is by encouraging a review of business practices and prompting agencies to improve them. Simply put, the main difference with cloud-based services, where the cost is determined by how much you need to use, is that a move to the cloud requires a more thorough review of internal business processes which might otherwise not have been triggered by traditional sourcing options.

Cloud-based services are pay per usage, that is, the more services required (such as data storage, customisation, additional services such as end-user support, user-administration and domain administration) the higher the cost of the service.

The full benefits (including cost savings) offered by cloud-based services and as-a-service solutions will be realised if agencies redesign their internal business processes to suit the offering, rather than customising offerings to suit their existing environments or internal business processes. However, improving business efficiencies would be required regardless of whichever of the three sourcing options was selected. While cloud-based services do not require internal business processes to be transformed, the service would come at a higher cost if these efficiencies are not thought through before the service is implemented.

In the case of three Cloud Pilot agencies (DTIRIS, FRNSW and Businesslink) the move to cloud-based services was a catalyst for transforming business processes, which led to greater business efficiencies (including lower costs and savings opportunities) and a greater ability to meet business objectives. DTIRIS, FRNSW and WIRO noted that they expect to realise future benefits and savings that they are not yet able to quantify. Agencies that recognised the whole-of-business implications of moving to an as-a-service model and engaged early across a range of internal business units were best placed to take advantage of these opportunities.

Recognising that a move to cloud-based services is more than just a move to a new IT platform, and wide internal consultation across the agency (such as record-keeping, policy, finance, HR and IT) will stand agencies in good stead when addressing organisational change.

FRNSW initially approached their email migration project as a traditional IT project. However as the remediation work was being conducted a number of business process questions arose including email retention periods, document management systems, communication with employees and other change management issues. The project team realised that the business transformation aspects of the migration required a different project management approach so the project scope was expanded to include change management, a review of internal business processes, extensive employee communications and staff training in records management.

Several Cloud Pilot agencies noted the need for senior executive level support and project sponsorship (DTIRIS, FRNSW, ServiceFirst) to ensure successful implementation. Agencies noted that it was easier to transform business processes when assisted by senior executive engagement.

DTIRIS has advised that a number of factors led to successful project implementation, most significantly because it was a major organisational priority and because there was buy in from and active engagement of the senior executive. The same executive team was involved from start to finish - from building the business case to implementation.
The project team was appropriately resourced and had the authority to make prompt decisions, taking a pragmatic approach to risk. The in-house approach meant that the team maintained ownership of the project. DTIRIS commented that there was significant organisational resistance to change, which highlighted the importance of early communication and the allocation of flexible and appropriate resources.

Cloud Pilot agencies have all commented that cloud services enabled their agency to access cost-effective services that were flexible to their changing future needs. For the Cloud Pilot agencies where timely implementation was a key factor (WIRO starting up their operation and to DTIRIS in having lack of transparency of their existing operation), the cloud service offered an opportunity to quickly implement a solution.

All Cloud Pilot agencies that implemented a messaging as-a-service solution (FRNSW, Businesslink, ServiceFirst) noted that implementation prompted a re-evaluation of the purpose of email, that is, as a temporal messaging system rather than a document management system. This required agencies to change how they structured their business processes for keeping records, maintaining access to records, and storing personal data.
PART 5  PROJECT IMPLEMENTATION KEY CONSIDERATIONS

5.1 Organisational assessment

5.1.1 Business objective and business need

Lessons learned

- The decision to implement a cloud-based solution should be based on the ability of the solution to realise key business objectives.
- In order to derive the full benefits of implementing the cloud based solutions, agencies need to clearly understand and articulate their business needs to the market.

Traditionally, when sourcing in-house or via managed services, a procurement process may have consisted of identifying a suitable solution from a range of tenders. All five Cloud Pilot agencies noted that the clear articulation of the agency’s business objective(s) to the market was imperative in order to identify the most suitable solution.

Further, Cloud Pilot agencies noted that their business objective(s) and an assessment of their organisational readiness guided their decision in determining which market player was the most suitable for their business need(s).

When a clear business objective(s) was the driver of the project, the project was more likely to be successfully implemented. Cloud Pilot agencies that based their move to the cloud on meeting a business objective(s) reported smoother transition to a cloud environment and faster benefits realisation.

The primary business objective(s) Cloud Pilot agencies sought to achieve by adopting cloud-based services varied and were not necessarily based on cost alone. Overall, cost was not the primary driver for any of the Cloud Pilot agencies in transitioning to a cloud environment (cost-drivers are discussed further at section 5.1.3). Likewise, overall benefits were realised when agencies conceptualised their projects as business transformation projects, rather than traditional IT projects.

FRNSW initially approached its migration to a messaging as-a-service platform as a traditional IT project. The project was planned as if it were a straightforward IT implementation; the project team consisted of technical staff, and the scope of the project was to migrate from one platform to another. The business needs were not articulated first, rather, the project was viewed as a transition from legacy messaging solution to an up-to-date messaging (cloud-based) solution. The business objectives were originally framed as technical (the specification of works was highly detailed about what the email service should provide).

When FRNSW understood the extent of change required to their business processes to implement the email service, the project’s objective was amended to that of a business transformation project. The project team was expanded to include a change manager and discussions with a range of divisions within the agency were held regularly. FRNSW were mindful that the remediation of business processes was something that would only need to be done once, and that this would facilitate future uptake of other cloud-based services.

DTIRIS had a clearly defined business objective from the outset, which was to provide visibility of financial, human resources and payroll systems across a complex agency. Their business need was to rationalise five legacy finance and HR reporting structures into one, creating a “single source of truth”.

WIRO also had a clearly defined business objective from the beginning of the project - a speedy implementation and to maintain independence from WorkCover - and chose vendors accordingly.
It is considered that the articulation to the market by agencies of the business objective when seeking tenders will have an effect on the solutions that are available and therefore on the ability of the benefits to be realised.

ServiceFirst initiated its procurement tender process for identifying suitable vendors for its proof of concept project by releasing request for tender (RFT) documents. The ServiceFirst project team noted that vendors experienced issues in implementing an appropriate solution as they lacked a clear understanding of the business objective.

Vendors of the desktop as-a-service solution were required to spend the first month conducting a gap-analysis to determine the most appropriate solution. A limitation of a “proof of concept” (as opposed to an implementation), was that there was no actual business need identified. Rather, the purpose of the project was to learn about the maturity and capabilities of the market and test whether hypothetically an implementation could be done. The request for tender process consisted of putting out detailed specifications, as would be done in a procurement process to seek a traditionally sourced solution. However, this meant that cloud service providers did not have information on the business need they were being asked to address, and when they went to commence the project did not have sufficient information. This, in turn, highlighted that a clearly articulated business objective is imperative to successfully implement a cloud-based as-a-service solution.

5.1.2 Organisational readiness

Lessons learned

- Technical remediation is often required to implement a new ICT solution, regardless of the delivery model. However, the technical remediation required to move to a cloud-based solution may differ from that required to move to a new internal solution.

- Early assessment of required remediation will reduce the effort, time and cost involved in transitioning to a cloud-based solution.

- Internal remediation is an exercise that may only need to be performed once, after which agencies will be able to source additional cloud-based services more easily.

- Strong enterprise architecture capabilities and other technical skills are required to successfully migrate from the existing internal technical environment to cloud-based services.

Transitioning to a cloud environment can be technically challenging, particularly where it involves legacy or non-standard data, software and systems. In some cases, significant remediation may be required to enable integration or migration to a cloud environment. It is noted, however, that similar remediation would be required to implement a new internally built and managed ICT solution.

An assessment of internal technical cloud readiness as well as organisational readiness can assist agencies to accurately ascertain the effort, time and cost associated with adopting an as-a-service model.

An assessment of organisational readiness involves a greater scope than just technical readiness and may include analysis of senior executive buy-in, staff capabilities, document management processes, adherence to privacy requirements, time constraints, and budget (including implications of a move to operational expenditure).

Cloud Pilot agencies that undertook a thorough review of their internal technical environment prior to implementation reported a smoother migration, fewer unexpected costs and a more timely delivery against project timeframes (DTIRIS, FRNSW). Agencies noted that while the effort, time and cost associated with remediating the internal technical environment needs to be considered, it is an exercise that may only need to be performed once, after which the agency should be able to source additional cloud-based services more easily and potentially reducing transition costs.
Cloud Pilot agencies reported that experienced private sector organisations could be leveraged and were often better placed to assess the internal technical environment and prepare a remediation plan (for example Businesslink). Agencies commented that this assessment need not form part of the agreement to procure a cloud-based service. Rather, any agreement to carry out this assessment can be separate to an agreement to procure the solution, which may in turn be separate from an agreement to migrate the agency to a cloud environment.

The ServiceFirst POC shared the experience of other Cloud Pilot agencies that remediation of the internal technical environment must be done beforehand to enable the uptake of as-a-service solutions. A limitation of the POC was that only a production environment was available.

Procurement probity issues may arise where separate agreements are entered into (such as for the technical assessment and preparation of a remediation plan), and the provision of a related cloud service. Cloud Pilot agencies reported that a sound understanding of internal technical readiness can assist agencies to articulate requirements during the tender process (Businesslink, DTIRIS, FRNSW).

5.1.3 Economic and financial appraisal

<table>
<thead>
<tr>
<th>Lessons learned</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Undertaking a traditional cost/benefit analysis of implementing a cloud-based solution can be unhelpful as it may not be able to factor in the potential savings opportunities; the scope of savings of benefits of improving business processes; skills and capability requirements; and difficulties in quantifying of a move to the cloud-based service. There may also be difficulty associated with defining the scope of expenditure, which is likely to be organisation-wide, and which may only become apparent beyond the forward estimates.</td>
</tr>
<tr>
<td>• Further work could be undertaken to provide guidance to agencies on what factors to consider when calculating whole-of-life or total cost of ownership of as-a-service solutions.</td>
</tr>
<tr>
<td>• The adoption of as-a-service solutions may require upfront capital investment in setup and migration costs, but in the longer term will be maintained through recurrent funding.</td>
</tr>
<tr>
<td>• The funding and budget implications of shifting from capital to operating expenditure are largely unclear.</td>
</tr>
<tr>
<td>• Agencies must ensure that appropriate consultation has been conducted with relevant business units and with NSW Treasury.</td>
</tr>
</tbody>
</table>

When procuring goods and services, including cloud-based services, all NSW Government agencies are required to demonstrate value for money. Both the ICT Investment Principles endorsed by the ICT Board and the NSW Procurement Board’s statement on value for money recognise that benefits, costs and risks across the expected period of use of the good or service needs to be identified and assessed when determining value for money.

By considering all costs, benefits and risks associated with ICT investments, including acquisition, installation, operation, maintenance, refurbishment and disposal costs, agencies will be well positioned to deliver informed investment decisions. Value for money includes an evaluation of both price and non-price factors.

As-a-service solutions are priced on a pay-as-you-go model, which means costs are directly aligned with usage. All cloud-based as-a-service solutions are scalable, meaning that notionally the number of users can be increased or decreased easily and quickly by the vendor. This gives flexibility in the cost of the service and allows agencies to only pay for what they use. They enable access to services on demand without the financial commitments associated with directly purchasing, operating, maintaining and upgrading IT infrastructure.
By paying only for services consumed, the per-user cost of cloud-based services can be significantly lower than those associated with internally built and managed solutions. However, initial investment may be required to remediate an agency’s internal technical environment to enable the transition to cloud-based services. The term of the contract or agreement may also play a part in determining what is possible. For example, in a 12 month agreement, all vendors generally allow scaling the number of users up (with an increase in costs), but not all vendors allow number of users to be scaled down.

**Total cost of ownership**

For agencies to assess the viability of a cloud-based offering, they must understand how the cost differs from a traditional software solution. A traditional cost/benefit analysis of cloud implementations in the Cloud Pilot Project was not possible as it was difficult to evaluate costs and savings. For example, it was not clear whether benefits should include savings derived from productivity gains, and if so, how these could be quantified or estimated, particularly in advance. Further guidance is required from NSW Treasury on the factors that should be considered when assessing the long-term costs of as-a-service solutions.

Financial expenditure can be compared for the as-a-service solution against the estimated expenditure on the existing solution (if applicable), but should be based on a long term assessment, not just of the first year as this is not truly representative of total expenditure.

In order to measure the savings benefits of adopting an as-a-service model, the total cost of ownership (TCO) and whole-of-life costs need to be taken into account. Where possible, this should where possible include an assessment of the potential costs of the as-a-service solutions into the future compared to what the cost would have been if the agency had continued to implement a traditionally sourced ICT solution. Guidance needs to be given to agencies to determine a consistent method to determine what factors to include in such an assessment.

FRNSW has noted that a like for like on-premise implementation has been scoped at approximately $800,000 (without software assurance) and more than $1 million (with software assurance). TCO projections to three years including the cost of employing additional staff to support an on-premise Microsoft Exchange solution had the potential to double each of the above options.

DTIRIS has noted that it forecasts savings of $12.5 million per annum through implementing and using the cloud-based solution. This saving is comprised of discontinuing some legacy enterprise systems and support systems; not having to spend money on assets and software that would otherwise be deployed; and savings in project costs associated with cloud systems.

As indicated earlier in this report, it should be emphasised that the observed cloud implementations have all been characterised by their project teams as business transformation projects, rather than IT projects, and this is reflected in the way each Cloud Pilot agency gathered financial information on the cost of their projects.

Potential cost savings were an important consideration for agencies, particularly where the cost was compared to an internally built and managed solution. However, it is noted that cost is not always the primary driver of the adoption of a cloud-based service. In four of the five Cloud Pilot agencies, software as-a-service (SaaS) solutions were chosen primarily to realise a business objective. In these instances, the cloud-based solution represented a more efficient and effective means of achieving strategic business outcomes.

**Cost considerations**

A number of factors affect the cost of implementing a cloud-based solution. In the SaaS model, costs are directly aligned with usage. That is, the more users, the higher the cost of the project. The mobility and scalability of the solution will also impact on cost. Further, when moving to as-a-service, agencies do not
actually “own” anything except the right to use that service, and therefore the traditional cost assessment models are not applicable as both whole-of-life and intangible costs need to be included.

It is noted that organisations may have different requirements when moving to a cloud-based solution to facilitate their business transformation, driven by differing cost considerations:

- **End-user requirements**

  End-users are most concerned with the ease of use of software applications. Ease of use requirements may include: how intuitive the applications are, how quickly end-users can master the application; and how does the application simplify the day-to-day tasks of the end-user. The end-user is not concerned with how the application is delivered (traditional software or SaaS) as long as it is user friendly and is available whenever and wherever the end user needs access to it.

- **Business requirements**

  Business requirements are all about solving business problems. Does the application solve the needs for the business unit? Does it fit into the critical business process? How quickly can it be deployed, how are team members trained and supported and does the cost fit into the budget? Just like end-users, business units are unconcerned about the method by which the application is delivered as long as it solves the business problems, becomes a dependable part in the business process and fits within the budget.

- **Corporate/Agency requirements**

  Corporate requirements are either driven by a need to increase revenue or to reduce or contain costs. These requirements trump both the end-user and the business unit requirements. If the sponsor for an application cannot build a business case that shows the impact to revenue and cost, most likely there will be no approval at the corporate level. Just like end-users and business units, the organisation is often unconcerned about how the application is delivered, as long as the application contributes to the top and bottom line.

- **Operational / IT requirements**

  When organisations buy software applications, they traditionally look to the IT department to support and maintain the application. For this reason, IT departments may tend to prefer traditional software applications over a SaaS model because of their responsibility to the end-user for delivery of the solution.

  Generally speaking, the costs between each Cloud Pilot agency were significantly different because:

  - differing starting points of each agency (their existing infrastructure, skills, budget, capabilities, business need and business objective, etc)
  - differing types of implementations involved (desktop, infrastructure, messaging, etc)
  - differing costs involved whether agencies contracted with a platform provider, service provider, integrator or migration consultant.

  Significant remediation costs may be involved in moving to an as-a-service model. This is particularly the case where an agency has large or complex legacy and non-standard data, software and systems. This being the case, savings generated by cloud-based solutions may only become apparent beyond the usual forward estimates. Cloud Pilot agencies commented that the initial investment associated with remediating the internal technical environment should not necessarily be associated with one

---

implementation. Because the internal technical environment will only need to be remediated once, agencies should be able to source additional as-a-service solutions more easily and cost effectively.

On a per-user basis, the Cloud Pilot agency implementations did not always guarantee up-front agency cost savings, particularly where it was an agency’s first adoption of an as-a-service solution (factoring in the costs associated with changing the internal business processes or remediating the internal technical environment).

However, the primary business objectives varied and were not necessarily based on cost alone. Cloud Pilot agencies all started from a different baseline of technical capability, their internal technical environments differed (some required less remediation than others to integrate the cloud-based service) and had differing business objectives.

Agencies also differed in the types of factors included in their cost estimates. For example, with the email as-a-service implementations the cost of changing the document management system or training staff in the use of a document management database were included in the implementation costs but such costs were included by other agencies.

Agencies that have implemented their solutions have reported significant cost savings compared to their previous solution(s) (DTIRIS, FRNSW). Medium to long term savings will also be favourable as a result of their cloud implementations, factoring in opportunity savings and benefits of more effective business processes.

**Economies of scale**

Benefits of cloud-based solutions include the opportunity to leverage economies of scale through scalable offerings and multi-tenanted architecture.

Multi-tenanted architecture refers to a SaaS vendor with a number of customers subscribing to a single, centrally-hosted software service. This enables the vendor to serve all of its customers in a consolidated environment. A similar application installed locally might require each customer to dedicate an entire server to the application, perhaps more than one if load balancing and high availability are concerns.

This represents a substantial potential saving over traditional software models. For SaaS applications that are built to scale, the operating cost for each user will continue to drop as more users are added. It is considered the provider will then develop multi-tenancy as a core competency, leading to higher-quality offerings at a lower cost.

Scalability of cloud refers to the ability of a vendor to increase the number of users of the product. The general perception is that cloud will be easily scalable, but vendors may limit the true scalability of the product through incremental pricing steps based on user numbers and other thresholds.

**Shifting from capex to opex**

The *NSW Government ICT Strategy* and the *Procurement Board’s Strategic Directions Statement 2013-14* both highlight the need for a new and more flexible approach to the procurement of goods and services to meet current and emerging business needs. ICT investments traditionally involve substantial capital investment followed by maintenance and upgrade costs. The adoption of as-a-service solutions may require upfront investment in setup and migration costs, but in the longer term may be better managed through ongoing recurrent funding that enables flexibility.

The procurement of as-a-service ICT necessitates moving away from the traditional approach of funding being sourced from capital expenditure (Capex), towards ICT being increasingly funded from operating expenditure (Opex).

Where an agency’s Opex budget does not allow for additional expenditure on as-a-service solutions, current practices encourage agencies to seek additional funding from Treasury for Capex, even though this may not represent the best value for money.
Agencies may currently be unaware of existing mechanisms that enable procurement of ICT through operating expenditure. DFS is currently working on providing guidance for agencies on the known issues associated with funding ICT expenditure from Capex and Opex, to ensure that Capex and Opex operate on a ‘level playing field’ with a focus on achieving value for money. DFS plan to follow this up with guidance on how agencies evaluate both funding options equally when considering an ICT project.

5.2 Market assessment

5.2.1 Understanding the cloud market

Lessons learned

- A sophisticated understanding of the cloud market is necessary to ensure that agencies engage the most appropriate vendor to meet their needs. This understanding includes differentiating between platform owners, service providers and niche consultants.

- Agencies must be able to adequately define their requirements in order to select the appropriate vendor(s) to meet their business objectives.

Depending on which vendor agencies contract with, there may be implications for skills and capability requirements within an agency. That is, if an agency has significant internal capability, it may be appropriate to contract directly with the platform owners. If no there is limited capability, it may be more suitable to contract with a third party service provider (further discussion at section 5.3.2). Of the Cloud Pilot agencies observed, three contracted directly with a platform owner (DTIRIS, FRNSW, Businesslink) and the remaining two contracted with a third party service provider (WIRO, ServiceFirst).

Platform owners

Platform owners are generally large multi-national corporations that own the base software platforms and will generally be the body who issues product licences. Little else will be offered in the contract with the platform owner other than the licence to use the product (usually on a per-user basis), the commitment to safe data storage, access to that data by the client and deletion of data off the servers at the end of the contract term. Generally, additional services such as disaster back-up and recovery, ongoing support and migration assistance would be offered, but as an additional service with an additional fee on top of the base cost.

Platform owners may also issue licences to a third party service provider (which in turn passes the rights to use the licence onto a client).

Generally, cloud-based products offered by the platform owners have a better price point than those offered by third party service providers for the product. If platform owners offer services (often offered through a subsidiary company or competing division within the company), these are charged on top of or in addition to the base product price.

Service providers

Service providers offer a range of services on top of the base cost of a licence to use a product and generally their overall cost may be higher per-user, however the client benefits from a wider range of services. Service providers will take up the administration, maintenance and support functions (for a price) that platform owners may not. It is important to establish the scope and level of support that will be provided by the vendor during and immediately following implementation, and the cost of that support.

Benefits of contracting with service providers are that they take on most of the maintenance and administrative burden as part of the service cost, as well as cater for agencies that lack the capabilities or infrastructure to implement or manage a platform themselves.
Niche Consultants

A growing area of the cloud services industry is that of niche consultants. Specialising in integration architecture (systems or application integration), web applications (plug-and-play applications), data migration process, and other areas of specialisation, consultants may be a subsidiary of a larger company or an independent company.

5.2.2 Ensuring appropriate procurement processes

<table>
<thead>
<tr>
<th>Lessons learned</th>
</tr>
</thead>
<tbody>
<tr>
<td>• It is essential that agencies clearly articulate their business objective requirements to the market when procuring cloud services.</td>
</tr>
<tr>
<td>• Agencies need to be mindful to ensure probity of the procurement process, especially when engaging a niche consultant to undertake an assessment of remediation or amendments to the internal architecture that may be required, who may be a subsidiary division of a platform owner or service provider company that may be bidding for the tender.</td>
</tr>
<tr>
<td>• Agencies need to understand the different market players that offer cloud services in order to identify the most appropriate vendor to suit their business needs.</td>
</tr>
</tbody>
</table>

Agencies need to be aware that large platform owners have internal business areas that may quote for different aspects of the process including architecture design, integration, migration, managing the service, initial and on-going support, backup and disaster recovery. Platform owners may also have service providers as company subsidiaries. This offers a challenge for agencies in maintaining probity in the procurement process. Agencies need to be aware of these complexities.

With such a diverse market of cloud-based services, agencies may find themselves contracting with many players for the provision of the one service. For example, they may engage a platform provider to provide the service, but engage a migration consultant to execute the migration. Again, it is important that agencies are mindful of this in maintaining probity in the procurement process.

As one example, FRNSW was in initial discussions with a platform provider and was enquiring about the remediation work required to implement the offering. The vendor (Vendor X) offered a consultation through a subsidiary company, “free-of-charge”, with an assessment team which would determine the current internal technical environment and identify what might be involved in implementing a cloud-based offering.

Vendor X accepted that they would then step back into general pool of vendors that would have to tender a bid for the work. The probity issue that arose was that the definition of the internal technical environment would ultimately shape the technical specifications of the business problem, thereby giving Vendor X an unfair advantage against other tendering companies who were all asked to define a possible solution in order to be selected as the successful tenderer.

Therefore, it is important that agencies have a clear understanding of their internal technical environment (that is their business needs) and be able to articulate this to the market when seeking possible cloud-based solutions.

ServiceFirst identified that an accurately drafted request for tender document is essential in obtaining the most appropriate as-a-service solution. In order to have an accurate request for tender document, it is therefore essential for the agency to understand their business needs, the business objectives to be achieved, internal technical environment and level of resourcing available. If an agency is able to articulate to the market their business requirements and objectives, then the market player is more likely to be able to provide a service that meets those needs.
If the business objectives are not clearly articulated, agencies leave themselves vulnerable to vendors who over-promise and under-deliver. Providing as-a-service to government agencies is relatively new, and vendors may not yet be familiar with specific government requirements as-a-service. ServiceFirst commented that it experienced a clear disconnect between the vendor’s sales and operational teams.

### 5.3 Change implication

#### 5.3.1 Organisational change

**Lessons learned**

- A thorough assessment of the organisational change implications of transitioning to an as-a-service model, particularly impacts on business processes and capability requirements, should be undertaken prior to implementing a cloud-based solution.
- Change management planning should be one of the first considerations of any cloud implementation.
- Taking full advantage of moving to an as-a-service model requires agencies to reconsider business process design, which can improve efficiency, increase service capability and place greater emphasis on strategic business objectives.
- Recognising that a move to cloud-based services is more than just a move to a new IT platform, and wide internal consultation across the agency (such as record-keeping, policy, finance, HR and IT) will stand agencies in good stead when addressing organisational change.

The pilot findings indicate that moving to a cloud environment will require more emphasis on business design where cloud services will interface with and impact upon business systems. As noted earlier in this report, as-a-service Cloud Pilot agencies commented that the transition to an as-a-service model has had organisational change implications.

Cloud Pilot agencies noted that a holistic adoption of cloud service should be viewed as part of a larger business re-engineering project, rather than as an IT project (FRNSW, DTIRIS). Early engagement across the agency on the organisational change implications of transitioning to an as-a-service model allowed agencies to more easily take advantage of associated opportunities to improve business efficiency.

However it is important to note that this work would need to be done regardless of whether a cloud-based service or a traditionally sourced platform (managed service or in-house) was being implemented.

In some instances, if the remediation work is not done it may not be possible for the cloud-based service to be integrated (Businesslink, Service First DaaS POC).

Traditional sourcing options mask the need to generate efficiencies within an agency. Inefficient business practices such as poor document management systems may go unchecked if IT platforms (traditionally sourced) are rolled over from one solution to the next. However with cloud-based services, where the agency pays per usage, these inefficiencies are translated to data storage or require customisation of the solution (which comes for an additional fee).

FRNSW experienced this in the case of their email migration project, which required amendment to the way documents within the agency are stored. As a result, a spin off project will be conducted to look at the agency’s document management system. The project manager noted that this work has been masked over the years as the licences for the email system were renewed and further document management inefficiencies were hidden.

Once business inefficiencies are resolved, the process to uptake cloud based services becomes more streamlined. Therefore agencies may only need to amend their business processes once to realise the
longer term savings and other benefits cloud-based services have to offer (further discussion on savings is at section 4.1.3). The business transformation itself will also result in savings due to the efficiencies it generates.

Managing the organisational change associated with the transition requires comprehensive internal communications and education strategies, along with staff training and a phased implementation. Agencies that implemented projects commented that they underestimated the change management implications and have adopted strategies to manage organisational changes (DTIRIS, ServiceFirst, FRNSW).

In this respect a move to the cloud will almost certainly have training or skills implications. Implementing as-a-service solutions will enable greater mobility across the public sector, in terms of syncing services to mobile devices, as well as promoting a working environment where employees have shared knowledge of common software and therefore transferrable skills (further discussion as-a-service is at 4.6.2).

However change is not restricted to employment of technically skilled staff. A move to cloud-based services may also bring change to business processes; the way divisions within an agency collaborate with each other on ICT projects; the way documents and emails are stored and managed; how the services are paid for (operational expenditure rather than capital); how services are procured (and contracted); how staff manage their daily tasks, and workforce mobility.

5.3.2 Skills, capability and cultural change

Lessons learned

- Contract and vendor management capabilities will be required to manage solutions after migration.
- A thorough understanding of future skills and capability requirements is essential to realising the full benefits of adopting an as-a-service solution.

The adoption of certain cloud-based services may have significant impacts on skills and capabilities. Implementing a cloud-based service may also require end-user training, particularly where the service differs significantly from previous solutions.

Internal resources may be required to support staff during and immediately following implementation. More broadly, transitioning to a cloud environment will result in less demand for hardware and system management and product-specific software skills, and more demand for business analysts, architects, portfolio and program managers, change managers, and vendor and contract managers. These shifts will have cultural change implications for agencies.

Agencies need to understand their own internal technical abilities when choosing cloud-based products, services and vendors. Different vendors offer different levels of support both in implementing and managing the cloud environment. Agencies that do not address the capability and cultural change implications of the transition to an as-a-service model may experience a high level of internal cultural resistance during and immediately following implementation, with slower uptake of services and a poor useability rating.

ServiceFirst noted that a move to cloud services can be perceived by the operational team implementing the service in the agency as a threat to their tenure as an employee within the agency. The move to cloud-based services and outsourcing of the management of systems will have implications on the organisational structure of agencies, if they currently manage their services in-house. How an agency chooses to approach this issue and manage the transition will be guided by a number of factors including resourcing, alternative options for deployment, individual needs and the agency’s ability to re-train.
DTIRIS noted that it underestimated the internal resistance to changing the ways things have always been done. Cloud based solutions require such a far more holistic shift in an organisation so the inertia within the agency will be more apparent than with a shift to traditional IT-platforms.

FRNSW commented that implementing the messaging as-a-service solution required the agency to re-evaluate the perception of email from a document management system, to a temporal messaging system. Some parts of the organisations were keen to adopt the newer technologies, while some business units preferred to stick with tried and tested email systems. This signifies the need for a cultural change in the agency regarding how staff undertakes their record keeping and collaboration.

Further, FRNSW noted that the cloud service it implemented can align with current or future mobile devices, thereby enabling the agency to support future government direction on mobility solutions.

Businesslink noted that cultural changes have slowly been accepted over time. The agency undertook a change management process to manage the transition of the business away from building and maintaining infrastructure to integrating as-a-service solutions. This process has involved communication sessions between senior executives and staff.

5.4 Data

5.4.1 Security, privacy and data location

<table>
<thead>
<tr>
<th>Lesson learned</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Commercial cloud service providers with certified information security systems have robust security measures in place, which help to ensure the security of agency data.</td>
</tr>
<tr>
<td>• Agencies can enter into contractual arrangements with cloud service providers that specify data storage location.</td>
</tr>
<tr>
<td>• An assessment of the risk associated with data location should form part of an agency’s selection of solution and vendor.</td>
</tr>
</tbody>
</table>

The protection of personal information is a key consideration for agencies moving to a cloud environment. Agencies have an obligation to ensure the privacy of personal information and, where it is in the public interest, government information must remain confidential. The risk of third party access to information stored in the cloud is a common concern, particularly in relation to co-located customers and when data is in transit.

In general, agencies commented that data security controls implemented by cloud service providers are rigorous and provide a high level of compliance with international information security standards and best practice capability. This can help ensure that agencies maintain compliance with the requirements of the NSW Government Digital Information Security Policy.

In all cases, contractual arrangements restrict the vendor’s access to agency data and provide assurances regarding access by co-located customers and external third parties. All Cloud Pilot agencies agreed that the vendor’s adherence to security measures and controls (including international ISO protocols and standards) were sufficient to give them confidence that agency data would be protected in order to enable the agency to comply with privacy and data security requirements (WIRO, FRNSW, DTIRIS).

It is noted that standard contract terms often include provisions obliging vendors to report security incidents to customers and provide for customer visibility over the vendor’s security procedures. This was a feature of a number of contracts negotiated by agencies. Agencies selected vendors that operate in compliance with international standards and industry best practice in relation to information security and privacy.
DTIRIS has expressed confidence in the data security offered by the vendor of their ERP system. The system requires users who seek to access the business data to authenticate themselves and verify their identity. The ERP solution also offers restricted physical access with data centres logically separated and staffed around the clock, 365 days a year. The ERP provider relies on encryption technology, based on security protocols. Multilayered, partitioned, proprietary network architecture permits only authorized access to the data centres that supports the solution. After a risk assessment of its business needs, DTIRIS decided to store payroll and privacy related data in a local data centre rather than store it offshore, engaging a platform as-a-service located within NSW. The local data centre is also certified according to ISO security standards ensuring privacy requirements are met.

This separate location (and providers) of data storage highlights a new way of looking at business processes, broken down into components of a whole. Each component of a business process, depending on an assessment of business needs, can be serviced by a different vendor, data centre, or service as required. Depending on the different requirements of a business, data may be stored in a public cloud, while other data may be stored in a private cloud. Agencies are able to pick and choose services, data location and levels of security based on business needs and legislative requirements.

**Data location**

In general, the nature of cloud services may result in uncertainty as to data location at any given point in time. The legislative and regulatory frameworks of jurisdictions in which data is stored (or through which it transitions) may have implications for data control and access. Data centre location and jurisdiction-specific legislation are considerations for agencies transitioning to a cloud environment.

All Cloud Pilot agencies considered data location as part of the implementation, and some selected a cloud service provider on the basis of data location alone. Other agencies were able to select from several data centre locations offered by the vendor. All Cloud Pilot agencies undertook a risk assessment when making a decision about the location of data storage. This included an audit of jurisdiction-specific legislation and whether data location would impact the agency’s ability to deliver its core business objectives while also meeting obligations under the NSW regulatory framework.

It is noted that, under contractual arrangements, Cloud Pilot agencies were satisfied that they had sufficient certainty as to data storage location to ensure that their privacy and data access obligations were met. Agencies that have data stored either offshore or within Australia are confident that its location and the security controls and procedures implemented by the vendor provide sufficient data protection. This is because they did a due diligence and risk assessment before contracting with the vendor.

Depending on the business needs of each agency, different Cloud Pilot agencies implemented different data location options. One agency elected to implement a hybrid cloud solution in which the majority of data is stored offshore, while small amounts of sensitive data remain on infrastructure located on agency premises in NSW (DTIRIS). One agency maintained an in-house server that kept an archive of all data migrated into the cloud, which was slightly higher in cost than total out-sourcing the data storage, but also deemed suitable for their business need (FRNSW). One agency has data stored only in NSW (WIRO).

DTIRIS’ business data is stored securely in SAP data centres; with physical hardware and data separated into tenants (data is isolated for each customer’s business information). Duplicated and redundant hardware storage systems are maintained for backup.
5.4.2 Access to data and business continuity

Lessons learned

- Assurances regarding access to data are essential in maintaining business continuity.
- Contractual provisions should guarantee access to data in accordance with industry uptime standards and provide for regular reports on system outages, maintenance and downtime.

A number of factors can affect access to data stored in a commercial cloud environment. These include the quality and continuity of the services provided by the cloud service provider, the quality and continuity of the customer’s access to internet technologies, and the customer’s internal technical environment. Guarantees regarding the quality and continuity of services provided by the cloud service provider are an important part of ensuring customer access to data and thereby maintaining business continuity. It is also important that backup and disaster recovery plans are implemented that adequately account for agency business needs. These may be set out contractually.

All Cloud Pilot agencies included contractual provisions that guarantee access to data in accordance with industry uptime standards (FRNSW, DTIRIS, ServiceFirst). Additionally, contracts often required the vendor to provide regular reports regarding system outages, maintenance and downtime. Some agencies commented that the reputation of the vendor contributed to their confidence that service levels and access would be maintained (DTIRIS, FRNSW).

Agencies noted that the vendor’s obligation to provide access to data ends immediately beyond the vendor’s own firewall, after which access is determined by the agencies’ internet services and internal network operation.

A number of Cloud Pilot agencies included explicit contractual provisions for data backup and disaster recovery (FRNSW). Some agencies chose to address backup and disaster recovery in a separate agreement, in one instance with a separate vendor. Some agencies expressed frustration that the cost of backup and disaster recovery was not included in the initial quotation for the service (WIRO).

DTIRIS has been assured that the data centres that host its data have multiple connections to power, along with a short-term uninterrupted power supply and diesel generators as power back up. In the first week after migrating its data to the cloud service, the CIO was advised after the fact that there had been a power outage at the data centre. There had been no noticeable disruption to business continuity.

WIRO experienced a disruption to their business continuity due to a slowing down of the service caused by the agency having reached its data limit within the billing period. This was an issue that could be remedied by either increasing the price cap limit, or reviewing the amount of data used within each billing period. A more significant issue experienced by WIRO was that at least once or twice a week on average, the system slowed down to the point where it needed rebooting. During this time staff were unable to work for periods of 1-5 hours.
5.5 Regulation and compliance

5.5.1 Public access to government information

Lesson learned

- Retention policies, access guarantees and interoperability between cloud solutions and internal software and systems help to ensure that agencies can continue to meet legislative public access obligations.

Agencies need to be sure that transitioning to an as-a-service model will not compromise their ability to comply with obligations imposed by legislation or government policy in relation to public access to government information. The Government Information (Public Access) Act 2009 (GIPA) imposes a legislative obligation on agencies to ensure that, upon request, they can access information in order to make it available to the public.

This will be particularly important if agencies implement email or case management systems (or the like), with an option to retain data for only a prescribed period of time and parallel document management systems (that satisfy an agency’s GIPA obligations) are not in place.

Most agencies identified GIPA obligations as a consideration during a risk assessment and legislative compliance audit undertaken as part of their project implementation. However, after conducting their respective risk assessment processes, all Cloud Pilot agencies were confident that transitioning to an as-a-service model would not compromise their ability to comply with obligations imposed by legislation or government policy in relation to public access to government information and proactive release (FRNSW, DTIRIS, WIRO).

In the case of DTIRIS, the cloud service actually improved public access to government information. The ERP platform enables the agency’s data to be in the one place, which enables better access to the data and a greater visibility of the agency’s payroll system, financial reporting information, purchasing processes and human resources.

5.5.2 Record keeping obligations

Lesson learned

- Moving to an as-a-service model will not affect an agency’s ability to comply with legislative record keeping obligations provided robust information management practices are in place, including a document management system and related policies.

State records legislation regulates the creation, management, destruction and protection of the records of public offices, and provides for public access to those records. Agencies are required to conduct their own risk assessment to determine whether document management systems and policies ensure compliance with state records obligations, as requirements vary between agencies according to the type of business they conduct and the type of records they create. This risk assessment is required regardless of the type of ICT sourcing.

If agencies implement cloud-based email or case management systems they will usually be given the option to retain data for a prescribed period of time (according to the cost structure), after which it will be deleted. This means agencies need to ensure that they have document management systems in place that satisfy an agency’s record keeping obligations.

In the context of cloud-based email services, the interaction between the cloud service and the agency’s document management system, and policies relating to the retention and disposal of emails, are particularly important. The State Records Authority has published information on cloud computing on its
website in this regard to assist agencies understand some of the implications of record keeping and cloud services².

It is noted that some agencies are of the view that State Records obligations are barriers to the adoption of cloud-based services. However, State Records has amended its disposal authority to include transfer and storage of digital records with service providers whose data management facilities or servers are based outside of NSW (thereby including cloud service providers)³. In practice, Cloud Pilot agencies found that their ability to comply was not affected provided the agency had robust information management practices in place, including document management systems and related policies.

Cloud Pilot agencies reported that early assessment of the implications for agency information and records management mitigated the risk of project delays (FRNSW). Agencies reported that the transition to an as-a-service model provided an opportunity to improve internal information management and record keeping practices (FRNSW, DTIRIS, WIRO).

5.6 Technical considerations

5.6.1 Bandwidth, WAN and LAN requirements

<table>
<thead>
<tr>
<th>Lesson learned</th>
</tr>
</thead>
<tbody>
<tr>
<td>• To maintain business continuity and ensure optimal service quality and performance, bandwidth, WAN and LAN requirements must be assessed prior to implementing a cloud-based solution.</td>
</tr>
</tbody>
</table>

It was noted that the performance of cloud-based solutions depends on the quality of internet technologies, and that performance can be compromised where services are scaled up without taking account of network requirements.

To ensure optimal service quality and performance, cloud vendors identified agency bandwidth, WAN and LAN requirements and conducted in-house and remote testing prior to implementation to ensure service continuity. The number of users and the type and complexity of the solution were key factors in determining agency requirements.

Cloud Pilot agencies were able to make network adjustments prior to implementation, thereby mitigating the risk associated with interruptions to services and business continuity. Agencies that undertook this work as part of their internal remediation reported fewer issues during implementation (FRNSW, DTIRIS).

It is noted that, while cloud-based services are easily scalable, network configuration is generally not so easily varied. For this reason, networks must be configured for peak anticipated usage, which may lead to excess network allocation if the service is scaled down.

---
5.6.2 Data and systems integration

Lessons learned

- Moving to a cloud environment requires an increasing emphasis on business design and architecture, particularly where cloud services will interface with or impact on existing business systems.
- Prior to adopting a cloud-based solution, the impact on business processes should be considered, and the ability to integrate the cloud-based solution into existing enterprise infrastructure should be evaluated to ensure continuity of service and operations.

Moving to a cloud environment requires an increasing emphasis on business design and architecture, particularly where cloud services will interface with or impact on existing business systems.

Sophisticated enterprise architecture capabilities are required to ensure seamless data, software and system integration in a cloud environment. Particular care must be exercised when considering the integration of cloud-based services with internal, business-critical legacy or non-standard data, software and systems. In some cases, data, software and systems must be redesigned, upgraded or replaced.

Therefore it is important to identify all potential points of failure prior to implementing a cloud-based solution and to have mitigation and disaster response plans in place. Points of failure may differ from traditional internal IT solutions and generally cloud-based solutions will have three points of failure: device, site and carrier. One Cloud Pilot agency commented that any point of integration is a potential point of failure (FRNSW). An understanding of the extent to which this is required assisted agencies to accurately evaluate the effort, time and cost associated with adopting an as-a-service model.

Agencies recognise that implementing commercial off the shelf as-a-service solutions better enable information sharing and access to cost savings through multi-tenanted environments. Using a multi-tenanted environment is to store data on the same server in the same location, thereby allowing the user to avoid the additional costs imposed by vendors for customising products. When agencies engage the same vendor for the same offering (albeit with differing levels of services on top) they can leverage economies of scale, thereby experiencing lower costs per-user to enjoy the service. Further, by not customising products, agencies shift the onus of maintenance and service continuity from the agency to the vendor. Further discussion on implementing as-a-service and the organisational impact is at 4.3.1.

There is a significant opportunity for agencies to benefit from accessing services that are already in operation and working well, for many reasons. DTIRIS noted that it was able to quickly implement the ERP solution (two weeks tender evaluation, six weeks contract negotiations, five months from project commenced to the go-live date) because the vendor had a product that was ready to go. DTIRIS has commented that the rapid implementation was due to a number of factors. For example, DTIRIS focussed on adopting the solution with minimal customisation and it used the standard contract.

WIRO expressed the same sentiment – that it was able to switch on the solution within a matter of days, rather than weeks or months, because they chose an out-of-the-box, standard solution and adopted the standard contract.

ServiceFirst noted that the most complex part of its POC was the integration with existing systems. A large effort was required by internal resources to integrate the cloud service with their existing systems, the cost of the project increased significantly, which led to that aspect of the project being suspended and a test environment used instead. This raises the point that while as-a-service products may ultimately result in agency savings, business efficiencies and other benefits longer term, it may require capital investment in the short term.
5.6.3 Mobility

**Lessons learned**

- The flexibility, mobility and high availability of services is often a key driver of the adoption of cloud-based services.
- Agencies need to be mindful of ensuring that these benefits are not limited to a particular technology or platform.

The flexibility and high availability of services is often a key driver of the adoption of cloud-based services. Increasingly, consumers and employees are accessing applications and services remotely using smartphones and tablets. Citizens and businesses now expect convenient, real-time services anywhere at any time, via the internet and mobile devices. The NSW Government has endorsed a mobility framework that provides technical guidance to agencies when procuring mobility solution services. It details the issues that need to be considered so each agency can identify the available options that best suit their business requirements as they define their agency specific strategy and approach - for example a mobility or bring your own device strategy and policy (BYOD).

Mobility was a key consideration for all Cloud Pilot agencies in migrating to an as-a-service model. They all considered whether particular services were limited in their compatibility with mobile devices, for example by manufacturer or model or whether they complied with their BYOD.

Cloud Pilot agencies were also mindful of compatibility with emerging technologies and future developments in mobile device hardware. As noted in section 3.3.2, cloud-based data, software and systems are dependent on internet technologies. Therefore, where a cloud-based service is optimised for mobility, service quality and performance is conditional on the quality and performance of the mobile internet connection.

5.7 Transition

5.7.1 Licensing arrangements

**Lessons learned**

- Agencies need to give careful consideration to the licensing implications of transitioning to an as-a-service model.
- Software licences and agreements often have limited or no mobility and cannot be transferred easily from one type to another or between holders. This may result in a situation where agencies are liable to maintain expensive legacy licences even after migrating to a cloud-based solution.

Licensing may be a factor when making the decision of whether to move to the cloud. In some cases, Cloud Pilot agencies were motivated to source cloud-based services because they had legacy licences that were due to expire (FRNSW, Businesslink).

While licensing may not be determinative of the most suitable solution, it may have implications for the timing of the transition to cloud-based services.

Agencies will have different levels of knowledge about their licensing needs, so will need to engage closely with their current and prospective vendors about what options they have regarding transitioning to new licensing. Sometimes vendors offer arrangements to bridge the transition, but agencies will need to ensure they have a sound understanding of their business objective and seek guidance from vendors about which licensing arrangement will support that objective.
Businesslink noted that it would have benefited from engaging with vendors more closely to obtain thorough and specific information about the possible licence structures that would have suited its needs.

5.7.2 Migration in

Lessons learned

- Migrating data from an internal environment to a cloud environment via the internet can be a time consuming process and may put significant strain on an agency’s network infrastructure and internet bandwidth.
- Additional challenges may arise as a result of coexistence of the existing and new solutions during the migration phase of a cloud implementation.
- A comprehensive understanding of migration challenges will help agencies minimise disruptions to services.
- Agencies need to be prepared for surprises, to learn from experience and adapt accordingly.

Scalability is one of the primary benefits of cloud-based services, which can easily be expanded or contracted to meet the changing needs of agencies. In this way, it is often said that cloud services can be ‘switched on’ and ‘switched off’. However, the migration process may be managed in a number of different ways depending on the requirements of the agency and the requirements of the vendor.

Migrating to a cloud-based service is usually not simply a matter of switching the service on. In most cases a large amount of data must be migrated to the cloud in order for the service to have the functionality of an internal solution. Migrating data from an internal environment to a cloud environment via the internet can be time consuming and may put significant strain on an agency’s network infrastructure and internet bandwidth. A comprehensive understanding of the challenges associated with migrating to a cloud-based solution can help agencies minimise any disruption to services.

Establishing the ongoing operational network requirements for using cloud-based services is integral to ensuring optimal performance after implementation. It is equally important to take account of the network requirements for the migration phase of implementing a cloud-based solution.

FRNSW determined that migrating data to the cloud would put significant strain on internal network infrastructure and internet bandwidth. It was determined that a staggered migration should occur in the evenings and on weekends to minimise disruption to services (or sluggish services), though FRNSW also identified that this is when internal servers would be running BAU backup processes, which would slow migration.

FRNSW managed their own migration process in cooperation with a third party consultant, mainly because FRNSW is maintaining an on-premise archive of all emails. Data was migrated in stages, broken down into small groups of users to minimise the load on the network, determined by how the agency collaborated internally.

For example, from the first batch FRNSW learned that it should migrate calendar and contacts first and then migrate email. The senior executive, executive support staff, out-posted fire fighters and head office staff were migrated in separate groups. The migration of each group was carried out in two stages - from the existing platform to a new internal Exchange environment, and then to the cloud environment (‘swing migration’ as opposed to ‘direct migration’). This helped to minimise disruption caused by excessive data traffic on network infrastructure and through the internet. Moving to the internal environment and then to the cloud environment allowed for the reconfiguration of data from the existing platform to make it suitable for the new platform, which streamlined the process of moving the data to the cloud environment.
Some issues, particularly relating to functionality and usability, may become apparent during the migration phase of a cloud implementation as a result of co-existence of the existing platform and the new cloud-based service. This is particularly the case during the implementation of large cloud projects where all data cannot be migrated to the cloud-based solution at once. It is important to recognise the potential challenges and implications of co-existence. Employees must be appropriately informed and/or trained to ensure no data is lost. FRNSW included co-existence issues as part of its communications plan (some issues included difficulties syncing calendars and booking meeting rooms.)

In some instances agencies are able to migrate a limited amount of data to the cloud first in order to ‘go live’ (the essential, business critical data) and migrate legacy data over a longer period. This can speed up the implementation process (as experienced by DTIRIS).

5.7.3 Migration out

Lesson learned

- On termination of an agreement for cloud-based services, agencies must be able to ensure that data will be migrated securely to a new solution while maintaining business continuity, and that data will be removed entirely and permanently from the provider’s infrastructure.

On termination of an agreement for cloud-based services, an important consideration is that agencies can migrate data securely to a new solution while maintaining business continuity. On transition-out, agencies need to consider what data will need to be archived, where it will be archived, how it will be transferred and, where necessary, how the service provider can verify that it has been destroyed.

The destruction of data by the vendor on transition-out can be addressed contractually. It was noted that specific provisions outlining how data will be destroyed help to ensure that government information cannot be accessed by the cloud service provider, co-located customers or external third parties.

A number of Cloud Pilot agencies commented that accepted industry practice and commercial imperatives mean that service providers would incur considerable damage to their reputation if they were not to destroy data after transition-out. Additionally, commercial necessity makes it likely that the vendor’s servers will be ‘written over’ multiple times in the period following transition-out.

Cloud Pilot agencies commented that these realities help to re-assure them that the vendor would undertake an appropriate destruction of agency data at the end of the contract period (FRNSW, DTIRIS). As such, FRNSW, DTIRIS and WIRO felt it unnecessary to include a specific “transition-out” clause in the contract with the vendor. FRNSW’s contract allowed for a period of time for the agency to take their data out, (the vendor provided tools to facilitate this) but there is no onus on the vendor to transition the agency data out.

The ServiceFirst POC was the only agency to include a specific transition-out clause in its scope of works and contract. This was in part because the service was implemented for only three months and the data was operating in a real production environment, rather than a test environment. Therefore it was essential for ServiceFirst to ensure a clear process for migrating any data back to the original service. The vendors successfully migrated the data back to the original service without any complications experienced by end-users.
5.7.4 Avoiding vendor lock-in

**Lessons learned**

- Agencies should be cognisant of avoiding vendor lock-in at the point of engagement with cloud service providers.
- Industry interoperability and data portability standards will help to minimise the risk of vendor lock-in.
- Additionally, government data and information standards will facilitate the adoption of cloud-based services and increase collaboration and information sharing between agencies.

Transitioning between cloud-based solutions must take account of the functionality delivered by a new provider, and that this process can be costly and time consuming. Open standards, interoperability and data portability, and the use of commercial-off-the-shelf products, can reduce the risk of vendor lock-in and make transitioning between providers easier. Vendor guarantees in relation to technological parity and obsolescence can also mitigate associated risks. Matching internal business processes to those expected by a cloud service provider decreases complexity and removes the need for customisation, which may hinder transition.

Where the decision to transition to a new provider is predicated on a breach of contract on the part of the original provider, or where the provider significantly alters the service, stops offering the service or ceases business altogether, it may not be appropriate that the customer bear the costs associated with transitioning to a new provider.

Cloud Pilot agencies identified several issues that would hinder their movement to a new provider including the termination of cloud contracts, transitioning to a new cloud service provider (specifically migrating data from one provider to another) and remedies for breach of contract (FRNSW). Generally however, agencies viewed these as minor considerations compared to other issues, such as data location and security, access and cost.

A number of agencies commented that accepted industry practice and the commercial realities of the cloud market are such that providers are unlikely to engage in practices that would result in vendor lock-in, and that they were confident of being protected from excessive transition costs (DTIRIS, FRNSW, WIRO).

Agencies commented that risks associated with technological obsolescence are mitigated by transitioning to cloud-based services, particular software-as-a-service, as offerings are constantly improved and updated to keep pace with technological change.
PART 6  KEY FINDINGS

1. Guidance is needed on the change management implications of transitioning to an as-a-service model, including skills and capability requirements and cultural change dimensions.

2. Guidance is needed on the implications of cloud-based services for agency information and records management.

3. Standard terms for contracting for as-a-service would assist inexperienced or smaller agencies and guidance is needed on the associated procurement processes.

4. Recognising that implementing commercial off the shelf products better enable information sharing and access to cost savings from multi-tenanted environments, a mechanism for limiting vendors from providing customised solutions would assist agencies to realise the benefits of cloud-services.

5. Guidance is needed on undertaking a total cost of ownership and whole of life analysis of cloud-based services as well as what “value for money” is for as-a-service solutions.

6. Guidance is needed to assist agencies to understand the implications of the shift from capital to operating expenditure associated with the adoption of an as-a-service model.

7. A mechanism for sharing agency experiences in procuring and using cloud services would assist agencies to navigate through the process of implementing cloud services.
PART 7      DOCUMENT CONTROL

Document history
Status:       Draft
Version:     2.0
Approved by: John Thomas
Approved on: 21 October 2013
Issued by:   Katarina Ruszczyk
Contact:     John Thomas, Director, ICT Services, ICT Policy, Department of Finance and Services
Email:       John.Thomas@services.nsw.gov.au
Telephone:   (02) 9372 8286