International Journal of Managing Public Sector Information and Communication Technologies (IJMPICT)
Vol. 12, No.3, September 2021

CHALLENGES FOR PUBLIC SECTOR ORGANISATIONS IN CLOUD ADOPTION: A CASE STUDY OF SOUTH AUSTRALIAN PUBLIC SECTOR AGENCY

Dr.Yaser Mirza

Department of Information Technology & Mathematical Sciences, University of South Australia, Adelaide, Australia

ABSTRACT

This research explores critical aspects of procurement of ICT cloud services for South Australian public sector organisations with the case of South Australia Police (SAPOL) for evaluation. SAPOL as one of the state government agencies at the time is initiating this transition to the cloud environment. This exploratory research takes place when this public sector agency is doing its due diligence to ensure a successful implementation. In this study the researcher started off with surfacing the challenges in this journey for a public sector organisation before the actual journey commenced. SAPOL being a public sector organisation operates differently from private enterprises and has certain constraints and limitations that pose additional challenges for the organisation to transition towards the cloud. Interview with the CIO of the organisation responsible for the cloud migration initiative was organised. After detailed literature review, an interview questionnaire was prepared in accordance with the subject of interest. The information gathered in the interviews was recorded for detailed analysis. This paper contains a detailed report on the information analysed highlighting fourteen important challenges faced by the organisation in this cloud migration journey.

KEYWORDS

Technology in Government, Cloud Adoption, South Australia, Public Sector IT, Government Cloud, Cloud Challenges.

1. INTRODUCTION

Over the past couple of decades, organisations have used information technology to gain or sustain competitive advantage [1]. Many public sector organisations have been following the pattern implementing technology for survival in the constantly changing world. Thus, both public and private sector organisations have made massive investments into technology portfolios. With the rapidly changing work and business environment, the technology has gone through many folds of changes and thus become quite complex due to this organic growth in a responsive way to the demands of the business.

Currently with the tightening financial circumstances across the globe, especially in the public sector, there is a push to do more with less. Thus, some of the previous technology decisions and implementations must be retrospectively reviewed and rationalised. There is also another massive push in the public sector to move towards the cloud environment, driven by a policy decision by the federal and the state governments that public sector organisations must adhere to [2]. Thus,

currently the immediate challenge for many public sector organisations is to move towards the cloud environment and cut costs.

It is believed that moving towards the cloud environment will achieve more efficiency, scalability and cost savings for the government agencies [2]. Saying that, the process of transitioning towards the cloud environment is capital extensive and thereafter there is assumed to be operational savings. To achieve those operational savings, it is essential that the transition towards the cloud environment is done in a well thought mechanism that ensures the potential benefits in the future. To make this strategic move the technology managers only have policy guidelines available from the Office of the Chief Information Officer for State Government (OCIO) to their disposal. No detailed framework exists that allows organisations to follow and learn from other's experiences to have higher chances of success and cost savings.

It is also highlighted in the Auditor General Report's concluding remarks about cloud computing [3] that:

"The development of further cloud computing guidance is important in supporting agencies as they attempt to leverage on technical advancements. While traditional governance principles may exist around procurement, security and risk, there remains a need to develop and enhance guidance that reflects the current process, design, governance and contract management requirements for cloud services."

This research investigates SAPOL as one of the state government agencies that is initiating this transition to the cloud environment. This empirical research takes place when this public sector agency is doing its due diligence to ensure a successful implementation. In this study the researcher started off with exploring the challenges in this journey for a public sector organisation before the actual journey commenced.

- RQ. What are the challenges for SAPOL to transition towards the cloud environment?

The following instruments for data collection were used in this research:

- SAPOL Chief Information Officer (CIO) Interview: It was important to select the right target audience for the interview. For the topic under study, the SAPOL CIO at the time was the best suitable person to provide the researcher the detailed information on the topic.
- Electronic recording of the interviews was avoided to facilitate the comfort of the participants thus a probability of recording of the comments exists.
- Archival Records: Archived records were accessed through the existing electronic repositories for the organisation.
- Direct Observations: Direct observations have been very effective in the data collection as the span of direct observation has been extensive due to the access to the organisation for the researcher as a staff member.
- Documentation: I searched for the available documentation from academic and professional sources. This included the published information and some unpublished information to collect the data required for further analysis.

The learnings from this process will be vital for CIOs and managers of other public sector organisations, who will face similar challenges and obstacles in their way. The availability of a guideline to help them to overcome similar obstacles can simplify the transition.

2. ISSUE IDENTIFICATION AND ANALYSIS

Some challenges that lie in any cloud environment implementation are associated costs [4], the ambiguity in the process, the security compliance, legislative compliance, and data integrity. The changes in the legislation have not been up to the pace of the technological changes and currently it seems like specific legislations around data protection and privacy act need to be put into place relevant to the changing scenario of technology and cloud computing [5]. The definition of jurisdiction over the cloud environment is another challenge which comes in the way of transition [6]. There is a very big cultural change associated with the movement from an asset-based Information Technology system to a service-based Information Technology system [7]. Organisations need to change the way they operate due to this system. This is another barrier to the readiness. The way various financials operate specifically in the public sector, the shift will be from capital expense to operational expense. Thus, these are some of the challenges which have affected different organisations and in specific public sector organisations to move towards the cloud environment.

Although at the same time work is being done by different agencies to develop a roadmap and strategy for this transition, yet due to the exposure to certain elements of risks, organisations specifically public sector organisations are hesitant to the change. The private sector has been ahead of the public sector in the transition towards the cloud environment in the past but now public sector is also been giving more attention towards this paradigm [8]. Various solutions to mitigation of this risk is present as well as different mechanisms and offerings by the cloud service providers to enable the required level of security to the desires of the customer. To assist the transition, now organisations do not need to work on their own and they can leverage upon brokerage services that can support the transition process. Overall, this is the future direction and the gaps are being bridged very quickly.

2.1. Legal and Policy Aspects of Cloud Computing

2.1.1. Privacy Protections and the Stored Communication Act

There are implications on privacy with the implementation of cloud computing [5]. The current legal framework is not complete in regard to providing privacy protections to the users [5]. The US government has gone through some legislative changes over the years to keep up with the technological advancements and alignment of the legislation to ensure compliance of the technological implementations with the government legislations [9].

The fourth amendment provides the people protection of personal privacy from unreasonable searches and intrusions by the state. The dilemma with the internet users and cloud computing is that the boundaries have gone blur for private space due to the leveraging on the external cloud space. The protection of Fourth Amendment is much more limited to internet and cyber space [5].

In 1965, The Brooks Act came into existence being the first of its kind to be specifically focusing on IT management in Government. The legislative right of privacy in the light of fourth amendment of US constitution and explains how Stored Communications Act (SCA) was passed in 1986 as a part of Electronic Communications Privacy Act [5]. The Electronic Communications Privacy Act of 1986 which was passed by Congress and approved by President Reagan falls inadequate in its current state in the current environment [10]. The next to come was Information Technology management Reform Act (ITMRA) of 1996. This is now known as Clinger-Cohen Act. This act introduced the role of Agency CIO. [9]. Electronic Communications Privacy

Modernisation Act was referred to committee in 2012 but not advanced to the congress. The essence of this proposal was that any data production would require a search warrant [10].

The gaps in the SCA and recommendations that can help to cover the changing way that the consumers use technology these days with the protective legislations [5]. Some of the improvements that have been frequently advised have been noted [10] to comprise of the equal treatment of all data; application of suppression remedy where data acquired by unlawful means cannot be presented as evidence; authorization requirements for location data in the same way as government can access the data by the order of federal judge; similarly civilians and corporations should not be allowed to access personal and location data without the authorization an authority [10].

2.1.2. Government policy for cloud computing

In 2010 US Federal Data Centre Consolidation Initiative demonstrated the underutilization of the server infrastructure. In this evaluation the server utilization was found to be at the level of 7% [9]. In February 2011 the US federal government CIO Vivek Kundra presented the cloud computing strategy [9]. This strategy was included in a roadmap towards cloud environment implementation comprising of 25 points. This strategy also provided a framework for the other agencies to follow and make up their own decisions about cloud environment readiness. This strategy required agencies to have three cloud ready services to start off with the status of being cloud ready. The strategy emphasises on agencies to integrate cloud environment into existing Information Technology portfolio [9].

There was a direction to adopt “cloud-first” policy which required agencies to have cloud-ready services and the vendors to be government-ready in their offerings. These requirements were given to the vendors so that they can support the government’s strategic objectives [9].

A new era for the Australian public sector after the advent of the Obama Administration’s Cloud first policy [11]. Highlights some of the significant benefits of cloud computing and defines how agencies need to proceed towards the cloud environment transition while ensuring service delivery in parallel. A three-step guideline to assist government agencies to make this move to the cloud environment [11]. This includes secure data flow to the cloud environment, movement of Information Technology operations to the cloud environment and encouraging transparency to the cloud service providers CSPs. The benefits of the government cloud environment and a mechanism to go ahead with it involves analysis of the deployment and service models and selection methodologies [12].

2.2. Security and Resilience Challenges for Cloud Computing

The security implementation as one of the major challenges for the cloud environment and describes the trust factor in cloud environment in terms of security implementation and compliance as being critical to the future of cloud computing [13]. The European network and Information Security Agency (ENISA) produced a document called “Security and Resilience in Government Clouds” [14]. This demonstrated a decision-making model for government readiness for various cloud services provided by different Cloud Service Providers (CSPs) [14]. This report aims to support the European Union member to define the states cloud strategy with respect to resilience and security in government clouds.

Some of the organisations dealing with the sensitive data have not come across satisfactory legislative and security compliance for them to consider the movement towards the cloud

environment [4]. There are ways around the mentioned situations and the organisations should follow a complete analysis process to realise the possibility of cloud transition [4]. In favour of the cloud environment, the author suggests that it is not one size fit all but due to the variations of the adoptable solutions, different organisations can choose as per their requirements. The decision framework for cloud environment migration for federal agencies comprises of 3 steps: Selection, Provision and Management [14]. This allows different agencies to make the move slowly but surely, towards the cloud environment using the flexibility of the framework to work in accordance of their agency requirements and needs. The details advise various architectural solutions for organisations and evaluate their suitability for adoption, within the agencies based on their own requirements [14]. The decision framework looks at both public and private sectors in supporting the decision-making process.

Explains some of the impediments in the way of cloud computing for government agencies and small and medium enterprises. To find answer to the security impediment of cloud implementations, Cloud Data security project looks at the adherence of cloud services to government laws [15]. A 6-layer data security model along with a security assurance of three levels. These three levels are basic, advance, and premium which are offered to the clients of the cloud as a service [15]. Security management can be described as a service which means that the extent of security (with respect to the six layers and three levels) required on various data based on the security requirement against the sensitivity of data, can be purchased as a service on demand [15].

2.3. Challenges Associated with Cloud Jurisdictions

The personal jurisdictions and the challenges associated with it for the internet and cloud users [6]. This implies that the definition of private place where the privacy is to be protected needs to change as the internet users utilising cloud services can be potentially exposed and unprotected with data storage and sensitive information stored on the cloud environment. Study compares the choice of law as operated in the United States with the international laws for data protection in particularly the European Union [6]. Data protection and security laws applied by the European Union members protect the people and their information beyond the private arena [6].

The South Australian Industrial participation policy (IPP) requires all respondents of tenders to comply with the evaluation criteria set to measure the industrial participation by the supplier [16]. This is applicable to all contracts above a certain value. This is applicable to government procurements, public private partnership projects and private sector projects that are the beneficiaries of significant support of over $2.5 million from the Government of South Australia. Projects that are funded by the federal but managed by the state government are also covered by IPP.

The IPP favouring the local suppliers and may seem beneficial to state's economy in one way, at the same time, it has its draw backs. It makes it difficult for public sector organisations to realise the benefits of economy by scale provided by the large national and international suppliers of cloud environment.

The IPP dictates that all public sector contracts will need to include IPP evaluation scope in any contract evaluation. According to the SA State Procurement Board [16] all contracts valued between $22,000 and $220,000 will have to go through a mandatory Economic Contribution Test (ECT). In this range, there is no specified weighting and the ECT will be used to determine a winner, if more than one response represents good value. This is to the discretion of the evaluation panel to measure these criteria against the responses in line with the policy. For

$220,000 to $1 million in regional contracts and up to $4 million in metropolitan contracts ECT is mandatory and it has its quantitative weightage in the evaluation process. This is minimum 5% mandatory weightage but can be increases as deemed appropriate by the panel and the government agency [16].

2.4. Capability of Government organisations to transition to a cloud environment

Bellamy [17] talks about the exposure to increased risk by the public sector due to transition towards the cloud environment. Many of the government organisations cannot transition towards the cloud environment even though the risk can be managed by different mechanisms because of the lack of the capabilities required to support the transition and manage the cloud service after the transition [17]. The core investment into the pre-requisites for the cloud environment transition can on its own be a big enough hurdle for many of the government organisations under the current financial pressures. There are opportunities present by utilising the cloud brokerage services where vendors are providing services to manage this area for you and ensuring that the pre-requisite gaps a filled via this brokerage service [17].

This strategic change meant that there would be a change from asset management model to a service management model as well as from a financial point of view; the change would be from a Capital Expense (CAPEX) model to an Operational Expense (OPEX) model. This would mean that agencies would need to learn new ways to operate and this would be a significant cultural change as well [7].

2.5. Operational Challenges of Cloud Environment

Another threat associated with cloud computing is the potential of ripple effect of a problem spreading across the cloud environment can be a potential threat that would be introduced in the cloud environment [13]. There are a few examples to demonstrate this vulnerability in his book [13]. This problem is in particularly associated with the cloud environment due to the sharing of the large infrastructure which may be logically separated in most cases and physically separated in some. This is different from the conventional in-house dedicated infrastructure by the organisations for their own use. Some of the impediments to cloud computing may include the resistance to cultural change, liability and regulations, data portability, security concerns and privacy concerns, regulations and availability [7]. Some of the challenges associated with the cloud computing as integration of different cloud services, management of multiple cloud service providers and management of the cloud data [4].

The costs associated with the transition are being seen as a major bottleneck in the following of the latest trend [4]. The private sector has been ahead of the public sector in the transition towards the cloud environment in the past but now public sector has been giving more attention towards this paradigm [8]. More control and savings from Information Technology are expected as an outcome of the transition process. The switching cost of public sector organisations towards the cloud environment based on different scenarios [8]. The analysis is done between the switching cost (SC) scenario and public sector Information Technology procurement (PSITP). The analyses of the methodology used and presents an estimation model for public sector Information Technology procurements and recommends it in the current environment of change [8].

3. CHALLENGES FROM THE CIO'S PERSPECTIVE

This is highlighted in the Information Technology Management Committee Briefing paper (ITMC BP) for Cloud Computing at SAPOL [18] that applications and server numbers within SAPOL have increased dramatically over the last three years. This briefing paper stated that the steady increase in server numbers to support new SAPOL applications and the business decision to retire mainframe-based applications has resulted in server numbers rising from below 150 Windows servers three years ago to the current number of about 500 [18].

In order to understand the challenges for a public sector organisation to transition towards the cloud environment, an interview with SAPOL CIO resulted in the findings explained in this section.

This was a semi structured interview using a guided approach. The overall scope of the interview was controlled but the flow was natural that allowed more exploratory findings. Given below are the interpretations from the CIO's interview which have been documented as 14 challenges.

3.1. Lack of Maturity of the Cloud offerings

The cloud environment offering has been in place for quite a few years, but the maturity of organisations in acceptance of cloud environment has grown significantly in the last f years only. SAPOL CIO stated that "the acceptance of cloud environment is matched with the maturity of cloud offerings over the time". The term cloud has been taken in a lot of different directions by companies who are trying to brand their products or services and take the advantage of the euphoria of cloud.

The cloud offering has not matured to a complete extent for government organisations due to the difference operations from private sector. SAPOL must understand which of its functions along with data can be candidates for transition towards the cloud environment. This is not an easy task understanding the critical nature of the organisation.

3.2. Meeting the Government Cloud Directions

According to 2013 SA government's ICT strategy SA Connected [2], Agencies are required to invest more into services than hardware and software. The "cloud first" policy requires the government agencies to have cloud-ready services and similarly the vendors should be ready to provide the required services. The vendors have been made aware of these requirements so that government's strategic objective could be supported.

The issue for SAPOL for cloud adoption is to understand which one of its lines of business or back of house business is acceptable to be delivered through a cloud service. A true cloud service could be hosted anywhere and would be distinguished by the reliability, price, cost and flexibility of service. Several the cloud offerings are on the Australian shore because of the requirement of the government to hold their system of record data onshore. To ensure that record of data is preserved to comply with things like State Records Act, it eventually does not end up being true cloud service. They end up being a variation of a true cloud service, so some of the benefits of a true cloud service are not there.

3.3. Legislative Compliance & Data Governance Requirements

One of the major constraints in the movement towards the cloud environment can be the sensitivity of the data that lies on the infrastructure. Due to high level classification of the data, the cloud environment provider must be in many legal bindings with the state government and in some cases the federal government too.

Various options can be looked at to cater for this constraint as cloud environment can be public, private or hybrid. Different options may fit for different applications and infrastructure. The challenge here is that cost saving only comes with more sharing, so it can become difficult to manage this conflicting agenda between wishing to share to save cost and at the same time not wanting to share to implement security.
At the time of the research, the organisation was facing another challenge in terms of compliance with ISMF regarding following the government's security policy and framework. The compliance to this framework demanded that different classification of data must sit on different physical infrastructure. This implied that production and non-production data cannot sit on the same physical infrastructure. A lot of cloud provides rely highly upon virtual separation of the infrastructure rather than the physical separation. This allows better sharing and greater cost saving to the cloud provider and as a result to the clients of the cloud environment as well. The organisation needs to investigate the details of the ISMF and see that how much it can be stretched to meet the changing needs for movement towards the cloud environment. According to Privacy and cloud computing guideline [20] "where there are requirements for segregation of data, an agency should obtain all pertinent technical information from the service provider to ensure the proposed solution provides the required level of data segregation."

To cater for the above, this requires the classification of various data types to be appropriate candidates for different types of cloud options. In doing so, some applications/data will fall over in the category of being candidates of private cloud environments, but the attempt would be to manage security as well as to maximise the ROI. Private clouds may result in additional costs yet not deliver the desired efficiency all the times.

3.4. Jurisdictional Challenges, Inappropriate use, release, or loss of information

Remote Computing Service (RCS) Act dictates that the data must be carried or maintained by the service provider only for computer processing service and storage. SAPOL though being a public sector organisation is bound to protect its client's information and its own reputation in this regard. According to a cloud case study by Department of the Premier and Cabinet (2017d) information security implementation along with the fact where the data must be physically stored are major challenges.

For SAPOL, inappropriate release of information is one of the major risks. The loss of information or release of such information is a great risk for the organisation. According to Privacy and Cloud Computing guideline v1.2 [20].

"Agencies should also note that it may be possible for foreign governments to access information held in their jurisdiction or to access information held in Australia by any company with a presence in their jurisdiction. Some legislation of international jurisdictions contains provisions allowing that government to access information in specified circumstances, such as cases involving suspected terrorism or threats to national security, irrespective of the geographical location and without necessarily advising the South Australian Government. Risks arising from

foreign legislation should be considered in conjunction with all Australian legislative requirements."

Thus, the organisation believes that it must maintain all backups of information to cover the risk of loss of information. The release of information must be catered for in the contract struck with the vendors and service providers with legal consequences. To cover the release of information, with on-premises cloud model, there is a degree of confidence that the release of information is less likely. This was a challenge that the SAPOL security team must learn about and come up with the right solutions that can be implemented with the cloud environment offerings. SAPOL could take guidance from these laws implemented elsewhere in the world.

3.5. Reliability and Availability Requirements

As in case of some agencies may have records of violent crimes where someone has been murdered, agencies have to retain that record for at least 75 years. Although in theory, all stored in the cloud environment can be retrieved from the cloud environment, yet the matter of the fact is that the cloud providers are commercial entities. They may exist in the coming years or they may not as there is no guarantee for their sustainability and future. Government agencies cannot run records on a possible commercial organisation disappearing. One of the big challenges for organisations to meet is that can they trust the cloud provider.

Based on the USA government directions on transition towards cloud environment for its agencies, under the Obama administration, it was made clear that government organisations should use cloud environment but should also ensure that the backup of the data is kept on premises because of the risk associated with the records that runs the government. And the government must have its permanent records stored on a location where it is sure it exists. This is also a challenge for SAPOL. Possibly records which have short term necessity to retain could well be very well candidates for cloud service. Cloud services which are functional base that are joining people or helping in moving information from one place to another, are much stronger candidates than system of records.

The extent of adaptability of cloud environment also comes down to the nature of business of the government's agencies considering transition towards cloud environment. Cloud Services Planning guidelines [21] stated that "Expected levels of responsiveness, throughput, availability and reliability, and redundancy should all be part of the Service Level Agreement (SLA) with the cloud services vendor. You should confirm that the SLA addresses adequate system availability, downtimes, and scheduled outages, and that these are acceptable in terms of timing and duration to support business processes. The SLA should also consider the availability and flexibility of support arrangements." Some lines of business would attract and would be more suitable for this offering. Others based on the current maturity of the cloud offerings, may not be suitable for many years to come. It would be both a trust and a data retention issue.

3.6. Security requirements over Cloud environment

Cloud computing security guidelines [22] highlight that the alignment of cloud implementation with ISMF and ISO27002 is significant. This guideline states that government agencies will need to ensure that different policies, standards, and controls from ISMF are adhered to while implementing cloud environment due to the possibilities of security breaches [22]. Managing security over the cloud environment is a major challenge. This is a concern shared by many other in the industry.

According to ITMC BP [18], SAPOL is not fully compliant with government requirements to use mandated Government ICT contracts for server support. This position stems from 5 years ago (the original OCIO ICT Contracts) when new Govt server support contracts were rolled out that if fully adopted by IS&T would have; Introduced an unacceptable security risk through the server support Supplier having remote access to SAPOL data.

SAPOL would be responsible for the physical security of the assets in the current transition plan as the premises are owned by SAPOL.

According to Personal information data breaches guideline [23] "The collection, management and use of personal information by South Australian Government agencies, is governed by the SA Government's Information Privacy Principles Instruction – Premier and Cabinet Circular PC012 (PC012). The South Australian Data Sharing Act 2016 provides boundaries around specific uses of the personal information collected and held by agencies."

In the same way at a network security would be managed by the vendors and SAPOL's internal security teams in collaboration. SAPOL would be internally responsible for managing the security at the application level. Some of these things would become clearer when various cloud service providers respond to SAPOL's requirements and then SAPOL would look at the best solutions that work best with the organisation's requirements and constraints. The initial steps for SAPOL need to be very cautious to ensure that these challenges would be resolved early in the transition and contracting phase.

3.7. Establishing Security Service-Level Agreements

Many small and medium level enterprises need to understand and evaluate the security offerings by the cloud environment paradigm against their organisational and their customers' requirements.

According to Personal information data breaches guideline [23] "In delivering government services to the community, agencies collect and manage large amounts of information and data, including personal information, on behalf of citizens and other trusted partners. Where it has been identified that there has been a Personal Information Data Breach, agencies must take prompt action to deal with the breach and inform appropriate parties."

These organisations need to shift their approach towards appropriate risk management and choosing a variant of cloud environment appropriate to their reprioritised requirements. According to cloud computing security guidelines [24], "A risk management process should be used to balance the benefits of cloud computing with the security risks associated with the agency ceding management functions and a large proportion of oversight to a third party. A risk assessment should consider whether the agency is willing to entrust their reputation, business continuity, and information to an external entity that may erroneously transmit, store, and process the agency's data. The risk assessment must take into account the criticality and sensitivity of the data involved."

The organisations can define the security requirements in the service level agreements referred to as security SLAs. This approach is a solution where the customer defines the requirement and the vendor provides the appropriate level of security to the particular service at an agreed cost. The readiness of the vendor is only important at the time of delivery and postproduction when the security SLAs will be monitored and measured for contract performance management and continual service improvement. An effective transition mechanism is critical for postproduction

operational effectiveness as highlighted in a research also conducted in South Australian Public Sector agency IT Department [19].

3.8. ROI Rationalisation – Capitalising on existing investments

More control and savings from Information Technology are expected as an outcome of the transition process yet in the current scheme of things, SAPOL has already sunk investments in a couple of data centres along with its supporting infrastructure. Those investments cannot stop as they are supporting many of the different business functions and the organisation needs to capitalise on them till a point of time the economics of the situation guide SAPOL to move away from them.
ITMC BP [18] also states that a server support funding cost would not be justified which would have been magnified two-fold due to required savings that Treasury requested of SAPOL. These were on top of significant cost savings returned to Treasury that SAPOL contended.

As per the general principle of cloud computing, the shared usage of the infrastructure and the services can increase the efficiency and produce better ROI with minimal underutilised FTEs and infrastructure.

According to Cloud Services Policy Information Sheet [25] "Cloud services present many opportunities, including the potential to reduce electronic storage and internal ICT capital investment requirements."

SAPOL's immediate step would be on-premises cloud hosting but in future as the organisation's requirements change, hosting services could be considered and that will be an economic decision. At the time of the research it was considered that there is more value for money for SAPOL to utilise some of the existing infrastructure.

SAPOL was in the market using one of the SA government's hosted service panel contracts. The agency was using a tender to offer up on premises hosting of a server infrastructure and to transition the ownership or for the vendor to bring their own assets in and retire SAPOL's asset to provide that infrastructure as a service. It was not intended for all of SAPOL's assets, but the aim was to go for something like eighty percent of the server-based assets.

3.9. Cultural acceptance for the Cloud environment

Cultural acceptance of cloud environment in public sector organisations is one major challenge. SAPOL CIO in his interview states that "Cloud computing and the maturity of the organisations in its acceptance has come a long way in the recent past. Like any major change in public sector, the default culture unfortunately is to resist change." According to Cloud Case Study [26], "The excellent delivery of the staff training for the new mobile environment provided a positive experience, helping to alleviate resistance to change." Mainframe processing is one of those offering on cloud environment that SAPOL has embraced to a great deal. It was very good value for money for the organisation. It was a bit different from other cloud services as it was a part of managed services as it is been owned by government agencies but managed by outsourced service providers. It can be classified as an outsourced service management example that has been particularly useful for the agency.

SAPOL was leveraging of JTS (Justice Technology Services) to provide the mainframe infrastructure and application/environment management services. JTS was providing the same service to 4 government agencies as these agencies share information via JTS created interfaces.

In terms of ownership and management of some bits of infrastructure, applications and services, JTS was assisting SAPOL and in some respects this can be closely related to a private cloud environment.

Although this did not completely fall under the definition of Cloud environment in some ways as the costing mechanism with JTS was a CAPEX and OPEX model. This implied that SAPOL payed a percentage of all new infrastructures acquired by JTS to provide the services. Along with that SAPOL payed for the Operational costs for the services provided by JTS.

The sharing model implemented with JTS was only between 4 government agencies. This meant that even if one of the agencies required a service, JTS would provide the infrastructure and the service to fulfil the requirement. As the sharing capabilities were limited, and there was a commitment to respond to the service requests irrespective of the overall ROI, the efficiency of the infrastructure and the resources was not at maximum. The existing model helped SAPOL in the recent history and the model was working fine but there was a lot of opportunity for improvement and extension.

3.10. Political Issues

SAPOL CIO explained a potential political issue describing a scenario of jobs layoff in SAPOL as a result of cloud sourcing. CIO stated that as a state government department, SAPOL has a moral obligation in accordance to the state government's obligation to support the state government employees and their employment rights. In a decision for moving towards the cloud environment, there would be an underlying decision to cut down the FTE expense in the related infrastructure and the application management space which may justify the ROI. This would require a strategic direction where the organisation is moving towards OPEX model implying that the agreement for generation of redundant FTE positions will have to be accompanied with it. This may generate an ethical dilemma where many local resources are made redundant for which labour unions may come into play in the defence of the employees. Thus, any such transition plan has to be well sorted out in terms of catering for the ethical issues.

In terms of industrial participation policy (SA State Procurement Board, 2014), most cloud offering will have some form of local presence. The actual location where the data is physically hosted is another issue that must be managed within the requirements set out in the tender process and must be documented in the contracts. Some of the Whole of government purchasing agreements cover such sorts of things. Thus, in a true picture, IPP will not be a factor that would be influencing the final decision of vendor selection in such king of procurement.

3.11. Vendor Management & Contract Management

SAPOL is moving away from owning running and managing own risks to a contractual relationship so the important thing for the government agency is that the contractual relationship must be a strategic partnership. SAPOL is more interested in ensuring we have a strategic partnership where both parties will benefit from the engagement. That is one of the challenges, because it is not a very traditional method for government to deal with. It is a very long term viewed of strategic partnership where the success of both parties of the contractual agreement is mutually beneficial.

Cloud Services Planning Guideline from Department of the Premier and Cabinet (2017e) also highlights that cloud services would most likely require creation of new roles that have previously not existed. SAPOL would be looking at two separate functions for the management

of the cloud environment. One would be dealing with the pure contract management and ensuring that both parties bind to the agreed terms and conditions struck in the contract. At the other end there would be a function to manage the very day service levels and ensuring that the day to day work within the engagement proceeds. These functions will be both managing different areas and will require different skill sets for successful execution.

The way the contract is struck is the key to ensuring that operations go smoothly afterwards.
In terms of contractual arrangements with the Cloud Provider SAPOL CIO states that "In the traditional sense SAPOL being an outsourcer or SAPOL outsources its environment to a provider; SAPOL must negotiate capacity, breakpoints, investments and pricing changes for traditional cloud suppliers. As SAPOL is buying a pure service and is totally disconnected from the backend investment costs by the vendors which are effectively wrapped up by the vendor.
SAPOL CIO explains this phenomenon as:

"It is like when you go to a shop doesn't matter whether you buy one or fifty, you buy on the price that has been struck and agreed on the item. That is pretty much what you are doing when you are buying a cloud service."

SAPOL CIO emphasised on the formation of strategic partnership where there is something in the contract for both parties and it's a win-win situation. The terms of the contract must be realistic, and the focus must be on partnership as more can be delivered on good will rather than the terms and conditions of the contracts. The expectations must be realistic at both sides of the fence. There is a transitioning out option in the contract that binds the vendor to transition out of the contract in a few different ways which would be found suitable by SAPOL at the end of the contract.

SA Government's Cloud Services Planning Guideline state that "Ensure you have adequate contingency plans in case you, or other parties, need to terminate the service. For PaaS or IaaS models it should investigate the ability to move an application to another vendor or in-house." The vendor needs to be treated like a strategic partner and this is another challenge for SAPOL as in government agencies, this is not usually how operations take place. The collaborative partnership must be defined in the contract.

In an outsourcing technology environment, it is important to have a procurement function within the IS&T function that allows the technology people to focus on the technical details of the requirements to be put in the contracts, and they don't have to worry about the details of drafting the contracts and attaining the guidelines about the legal and government regulatory requirements. At SAPOL the procurement and contract functions look at those aspects of the contracts allowing the Information Technology managers to focus on the details. This sort of arrangement is definitely very helpful for the organisation for achieving the best results. This arrangement in cloud computing environment can help in providing agility to Information

3.12. Managing variations in IT Operations

According to SAPOL CIO "there are a lot of benefits for organisations who aim to move towards it. This phenomenon as a disrupter of technology to an extent which will change the way small and medium enterprises operate. Small and medium enterprises will not have to setup their own infrastructures and manage it rather they would be able to rely upon the services provided by the vendors and could focus on their core business instead of infrastructure." There would be a difference in the way Information Technology operates as SAPOL's focus would move away documenting, executing and managing the existing infrastructure to designing, specifying and

management. This would be a transition up the stack in the architecture where the focus of internal Information Technology function will be on the upper side of the technology stack. Infrastructure series and expertise would be cheaper for organisations to get from service providers who do it as their core business.

The Information Technology managers and CIO would need to understand the business part of the organisation to a much greater deal as their role would be more towards the upper end of the stack which deals with the business and the business requirements. SAPOL CIO highlights that, "The biggest benefit I see in cloud offering is the separation of consuming organisations to see or understand the underlying infrastructure and the effort involved to set it up. This will allow small and medium organisations to remain competitive." To understand the business requirements and being able to understand the vendor offerings and being able to differentiate between then and choosing the right set of services that meet the business objectives would be where the Information Technology managers would be required to fill the gap. The cloud offering can be of one size fit all, thus it the job of the organisations to ensure that they get the right variant of the cloud environment as per their requirements [4]. As the role of Information Technology will change thus the sort of resources that SAPOL would traditionally have in the business analysis system analysis area and solution design area will become much more key to engaging a provider and delivering the right products to the business. It is a different focus or emphasis of skills so SAPOL would use solution architects and technical leads in build context as well as in an analysis context. This would assist to understand the nature of the offering and how it should be configured to get the best outcome to the business.

There will be disruption to SAPOL's internal processes and procedures because of the vendor activity involved in process of providing a service. And there will be a change management process because the resource staffing roles will change from what they are today. And that is the traditional change management process that we will have to manage.

3.13. Funding for Cloud environment

SAPOL CIO said that, "For SAPOL, the sort of characteristic of cloud that are valuable are the separation of the consuming organisations needs to see or understand where or at what costs to the vendor, the service offering is happening". SAPOL will have to make arrangements for ongoing support for the cloud environment instead of buying assets. This is a major shift in the way SAPOL operates now. The core investment into the pre-requisites for the cloud environment transition can on its own be a big enough hurdle for many of the government organisations under the current financial pressures along with the switching costs.

This strategic change meant that there would be a change from asset management model to a service management model as well as from a financial point of view; the change would be from a Capital Expense (CAPEX) model to an Operational Expense (OPEX) model. This would mean that agencies would need to learn new ways to operate and this would be a significant cultural change as well. There are many benefits for the organisation in doing so, and one of the immediate benefits after the first stage of the implementation could be significant saving in the FTE expense. The complete ROI proposition associated with the cloud environment will be appreciated once the complete transition towards the off premises private cloud environment has been in the stage two. The infrastructure management will always stay within the organisation to manage the cloud environment and smaller subset of the local infrastructure and the resources.

3.14. Implementation Challenges

Many of the government organisations cannot transition towards the cloud environment even though the risk can be managed by different mechanisms because of the lack of the capabilities required to support the transition and manage the cloud service after the transition.

In response to a question, SAPOL does see the movement of enterprise service bus on to the cloud environment as a very tricky challenge and as an area that needs a lot of detailed analysis. There is some possibility that it may stay on premises and on SAPOL infrastructure. Along with that other high classified applications and data may stay within the organisation thus a complete transition towards the cloud environment is not seen as an option in the near future thus the organisation will always be following a hybrid approach.

Government or government agencies are not particularly well skilled or governed in the commercial reality to be able to provide a true cloud service. The government financing, budgets, et cetera influence weather or not an organisation inside government can operate as a true cloud service provider. Commercial entities will get venture capitals make investments will do loss leading will do a lot of things in order to grow business services. Private entities could well do loss leading in order to buy business. Governments on the other hand are dictated by their policy and cannot do such things. Governments are accountable for the public money. It would be a difficult thing as government, to try and set itself up for a cloud provider. Some of the public sector agencies have created an equivalent which is labelled G-cloud. It is not a cloud service rather shared infrastructure service.

If the south Australian government were a cloud provider to its agencies, then it would move a lot of the barriers that might exist for a commercial entity where data holding could be interstate or offshore. Government cloud environment could make things a lot easier in this matter but setting up a government cloud environment, but it would require a lot of resources and skill set that he believes would be very difficult to acquire and maintain on an ongoing basis. For private vendors as it is their core line of business, it is a lot easier for them to provide such services.

Cloud offerings exist in various shapes and forms. As also stated in the Cloud Services Information Sheet produced by SA Government, there are a few different service models and some implementations models e.g. IAAS, PAAS, SAAS [27] and then leads to XAAS. These are the service models and it is incremental obviously in the sequence from infrastructure to software. These are different levels of scalability ranging from server to network and platform scalability. There are the implementation models starting from on premises to off premises, private, public and hybrid [27]. Hybrid is a mix of private and public. The assumption is that everyone is going to the cloud environment is a mistake. People need to pick the right services for the cloud environment that actually match their business and delivery the best results for their business. This allows different agencies to slowly but surely make the move towards the cloud environment using the flexibility of the framework to work in accordance of their agency requirements and needs.

It has been recognised that not just the cloud environment, but various sorts of outsourcing offerings have been a part of the government landscape for some time now. SAPOL CIO elaborated by telling the researcher that, “Back in 1995 the EDS outsourcing of all ICT in government. The contract was worth 500 million dollars back then. That was the biggest government outsourcing deal that was done in the southern hemisphere.” SAPOL has learned from the outsourcing deals in the past and it is not a case for being mandated to move towards the cloud environment for SAPOL. SAPOL is evaluating cloud environment as one of the many

offering in the market to provide their required solutions. Currently SAPOL is looking into IAAS as the first candidate for the cloud environment with on-premises model of deployment. SAPOL is looking towards moving up to 80% of its infrastructure with this model where the vendor will be providing their expertise and managing SAPOL infrastructure on premises for SAPOL.

Cloud environment is one of the many offerings that organisations are considering looking at and every organisation needs to define whether a particular line of business or a particular solution is best fitted for a cloud environment, or on premises, or any other service. People need to pick the right services for the cloud environment that match their business and delivery the best results for their business.

SAPOL's transition will be looking IAAS and PAAS up to virtual machines and operating system level environments. Current transition plan is up to four or five years. Moving further up the stack as SAAS can be a little difficult for SAPOL at this point of time as the organisation does not deal with many generic software and applications that the vendors will be able to provide. There is a greater risk for the organisation for outsiders to be providing those applications as they are custom made for SAPOL specific services. It is possible, but it is not likely in the short term.

4. CONCLUSION

The European Network and Information Security Agency (ENISA) produced a document called "Security and Resilience in Government Clouds" [14]. This demonstrated a decision-making model for government readiness for various cloud services provided by different Cloud Service Providers (CSPs) [14]. This is a new era for the Australian public sector after the advent of the Obama Administration's Cloud first policy [11].

Cloud services in its various forms and implementation models have come a long way in terms of maturity and so has the acceptance of the organisations in moving towards it. The maturity of the cloud offering has increased in the recent years [4].

At SAPOL, the organisation is considering cloud services as one of the many solutions to its requirements to ensure higher service levels and improved efficiency for the organisation. As stated by SAPOL CIO, *"The reliability would be expected to be higher. Along with that the infrastructure related outages would be expected to be lower. There should be reduced lead times for projects for infrastructure setup."* In SAPOL's current environment support of new technology has required ongoing investment in training and specialist contractor skills to ensure the infrastructure and software performs to the expected level. The end to end process of provisioning a new service can take, in the worst case, 3 to 4 months, which is not acceptable.

SAPOL is currently considering the procurement of cloud services with a cautious approach. Some of the organisations dealing with the sensitive data have not come across satisfactory legislative and security compliance for them to consider the movement towards the cloud [4]. The current approach is to implement about eighty percent of its server-based infrastructure towards IAAS with a cloud service provider. A strategy of integrating and mixing cloud with the existing Information Technology portfolio is a good option [9].

The organisation has approached the market through Governments server hosting panel arrangement which has already gone through a list of pre-approved cloud service providers for this purpose and it covers the risk for the organisation to a certain degree. SAPOL's current transition plan is very cautious one and aims to make this transition over a period of next four to five years.

One of the challenges for SAPOL in the transition is ensuring the physical location of the cloud service providers. The current legal framework is not complete in regard to providing privacy protections to the users [5]. In Europe, data protection and security laws applied by the European Union members protect the people and their information beyond their private arena [6]. Personal jurisdictions and the challenges associated with it for the internet and cloud users [6]. This implies that the definition of private place where the privacy is to be protected needs to change as the internet users utilising cloud services can be potentially exposed and unprotected with data storage and sensitive information stored on the cloud.

Being a critical government organisation dealing with secure public information, SAPOL is bound to ensure that the reliability and security of information stays intact; this is critical for the organisation. Security concerns in the cloud as one of the main impediments for organisations to transition towards it [7]. The organisation is therefore currently evaluating an on-premise solution for server hosting by an external vendor.

The organisation is also focused on economic goals and wants to capitalise on the existing structure if it is economic feasibility allows the organisations. SAPOL's CIO believes that SAAS is an option but it is not likely to happen soon for the organisation due to the specific nature of the business functions and the Information Technology applications that support those functions.

For SAPOL the contract management must be focus on strategic partnership to make this venture successful. This would mean that the vendor is treated like a partner and there is benefit for both parties involved in the arrangement. The way the organisation would be operating in terms of business will not change much but the way in terms of Information Technology operations the focus would be more towards design and management rather than documenting and executing. As an organisation SAPOL is aiming to move up the stack with this arrangement.

Some of the potential benefits include reduced lead time to infrastructure setup and reduced down-times that are infrastructure related. One of the advantages of cloud to be supporting the business to be agile with respect to demand and scale up or down in as required without the requirement of extensive and long procurement processes [28]. SAPOL wants to cover the associated risks with respect to security and reliability and benefit from the offerings by the strategic partnership in the long term. A six-layer data security model along with a security assurance of three levels which are basic, advance, and premium which are offered to the clients of the cloud as a service [15]. Security management can also be looked as a service especially in public sector where the skills of managing security over cloud may not already exist. This means that the extent of security (with respect to the six layers and three levels) required on various data based on the security requirement against the sensitivity of data can be purchased as a service on demand.

The research identifies some of the possible ways to work around the challenges and defines a high-level road map to achieve the objectives of technological transition. The research also draws attention to potential ethical issues perceived to associate with the initiatives. This research can be used as the basis or the foundation of further study to explore more opportunities and discover the unknowns in this area and is not conclusive in its nature. It is recommended that further detailed study be conducted to help SAPOL achieve better business objectives with these technological initiatives.

Cloud Services has many benefits to organisations, yet it also poses implementation challenges. SAPOL being a public sector organisation has its own limitations, but it is moving towards cloud services as a solution to some of its business requirements.

This research will assist CIOs and IT executives to take better informed decisions about transitioning the technology portfolio to the cloud and rationalising the technology portfolio. The findings of this research specifically target the public sector organisations. Some of the specific research implications are listed below:

As highlighted by the Auditor General Report's [3] concluding remarks about cloud computing that there is a need to develop cloud computing guidelines for public sector organisations that focus on the process, design, governance and contract management aspects of cloud computing. It is evident that due to the lack of process and implementation guidance for transitioning towards cloud environment, agencies are unable to make the move. Thus, this research has bridged that gap by providing an evidence and experience-based guideline to SA Government agencies.

This research also provides empirical evidence elaborating the pros and cons of different implementation options available to public sector organisations for cloud environment adoption.

5. LIMITATIONS AND FUTURE RESEARCH

5.1. Limitations

Some of the limitations to this research include:

1. The size of the sample is small
2. Qualitative research has its limitations as the reader cannot easily reduce these descriptions to numbers.
3. Participants may be hesitant to give negative insight about their organisation.
4. All archived information may not be completely correct as documentation is one of the known weak links in the process.
5. The direct observations may have been false as human judgement has been involved in the process.
6. Possibility of introduction of bias due to longer duration spent in the organisation with vulnerability of being influenced by various factors to build up a perception.

6.2. Future Research

The research can be looked at as a first step towards the solution of the problem and further research within as well as beyond the organisation is encouraged. The units of analysis can also be further diversified to understand the cause and effect of the phenomena covered in this research. Quantitative analysis of the data if applied may help to enhance the findings and provide clearer relationships of interest.

REFERENCES

[1] Baporikar, N. 2014, "Information Strategy as Enabler of Competitive Advantage", *International Journal of Strategic Information Technology and Applications*, vol. 5, no. 1, pp. 30-41.

[2] South Australian Government 2013, *SA Connected ICT Strategy*, viewed on 12 January 2016, <https://digital.sa.gov.au/resources/topic/sa-connected>

[3] South Australian Government, Auditor-General Department 2015, *Supplementary Report for the year ended 30 June 2015: Information and communications technology report*. viewed on 1 July 2017, <https://www.audit.sa.gov.au/publications/2015>

[4] Avram, M. 2014, 'Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective', *Procedia Technology*, vol. 12, pp. 529-534.

[5] Nguyen, H.T.M. 2011, "CLOUD COVER: PRIVACY PROTECTIONS AND THE STORED COMMUNICATIONS ACT IN THE AGE OF CLOUD COMPUTING", *The Notre Dame Law Review*, vol. 86, no. 5, pp. 2189.

[6] Segall, S. 2013, "Jurisdictional Challenges in the United States Government's Move to Cloud Computing Technology", *Fordham Intellectual Property, Media & Entertainment Law Journal*, vol. 23, no. 3, pp. 1105-1441.

[7] Kumar, P., Assoc, R.K., Head, P. &, Kumar, G. 2013, "Technical Impediments to Cloud Computing: A Survey", *International Journal of Computer Applications*, vol. 47, no. 1, pp. 24-29.

[8] Nilsson, A. & Magnusson, J. 2011, Studying the Implications of Cloud-based delivery models on public Information Technology procurement: A switching cost perspective, eChallenges, viewed on November 2015 <http://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-68749>

[9] Metheny, M. 2017, *Federal cloud computing : the definitive guide for cloud service providers / Matthew Metheny ; technical editor, Waylon Kruch*, Second edition edn, .

[10] Martin, J. 2014, Proposed Legislative Changes and Future Laws, John Wiley & Sons, Inc. , Santa Clara, CA.

[11] Burton, D 2008, "What cloud computing means for government", *Government News*, vol. 32, no. 1, pp. 16-17.

[12] Liang, J. 2012, "Government Cloud: Enhancing Efficiency of E-Government and Providing Better Public Services", *Service Sciences (IJCSS), International Joint Conference*, Shanghai.

[13] Marinescu, D.C. 2013. *Cloud computing: theory and practice*, Waltham: Morgan Kaufmann.

[14] Catteddu, D. 2011, Security and Resilience in Governmental Clouds, The European Union Agency for Network and Information Security, viewed 20 August 2015, <http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds>

[15] Doelitzscher, F., Reich, C. & Sulistio, A. 2010, "Designing Cloud Services Adhering to Government Privacy Laws", *10th IEEE International Conference on Computer and Information Technology*, Bradford.

[16] SA State Procurement Board 2014, *RFQ Template*, viewed on 2 December 2015, <http://www.spb.sa.gov.au/content/policies-guides/simpleprocurementtemplates >

[17] Bellamy, M. 2013, "Adoption of Cloud Computing Services by Public Sector Organisations", *2013 IEEE Ninth World Congress on Services*, Santa Clara, CA.

[18] SAPOL 2015, *Financial Cost Analysis Model at SAPOL*, Internal SAPOL report. Unpublished

[19] Mirza, Y., Bhatti, B. 2018, "Transitioning IT Projects to Operations Effectively in Public Sector : A Case Study of Australian Government Agency", *International Journal of Managing Public Sector Information and Communication Technologies (IJMPICT)*, vol. 8, no. 1, March 2017, viewed 30 April 2017, *<http://airccse.org/journal/mpict/current2017.html>*

[20] Department of the Premier and Cabinet, Government of South Australia 2017c *Privacy and cloud computing guideline*, viewed on 1 July 2017, < https://digital.sa.gov.au/resources/topic/cloud>

[21] Department of the Premier and Cabinet, Government of South Australia 2017e, *Cloud Services Planning guidelines*, viewed on 7 July 2017, < https://digital.sa.gov.au/resources/topic/cloud>

[22] Department of the Premier and Cabinet, Government of South Australia 2017f, *Cloud computing security guidelines*, viewed on 16 July 2017, < https://digital.sa.gov.au/resources/topic/cloud>

[23] Department of the Premier and Cabinet, Government of South Australia 2017g, *Personal information data breaches guideline*, viewed on 21 July 2017, < https://digital.sa.gov.au/resources/topic/cloud>

[24] Department of the Premier and Cabinet, Government of South Australia 2017f, *Cloud computing security guidelines*, viewed on 16 July 2017, < https://digital.sa.gov.au/resources/topic/cloud>
[25] Department of the Premier and Cabinet, Government of South Australia 2017b, *Cloud Services Policy*, viewed on 14 Aug 2017, < https://digital.sa.gov.au/resources/topic/cloud>
[26] Department of the Premier and Cabinet, Government of South Australia 2017, *Cloud Case Study Remote Access*, viewed on 1 July 2017, < https://digital.sa.gov.au/resources/topic/cloud>
[27] Department of the Premier and Cabinet, Government of South Australia 2017b, *Cloud Services Policy*, viewed on 14 Aug 2017, < https://digital.sa.gov.au/resources/topic/cloud>
[28] Yuvraj, S.G. & Rathore, P.V. 2013, "Rebalancing the Information Technology Equation with Cloud Computing to drive Business Agility", *International Journal of Innovative Technology and Exploring Engineering*, vol. 2, no. 3, pp. 123.

APPENDIX 1: CLOUD INTERVIEW QUESTIONNAIRE

1. Please summarise SAPOL IS&T function and your role as a CIO.
2. Can you just tell us a bit about your role in IS&T and within SAPOL?
3. What are your thoughts about cloud computing and the benefits for the organisations who intended to move towards it?
4. We will step towards a bit more SAPOL specific questions, according to 2013 SA government's ICT strategy SA Connected, Agencies are required to invest more into services than hardware and software so cloud offering are pretty much things that are offered as a service, so what are some of the business benefits in short and long term in relation to procurement of cloud services specific to SAPOL. Does it add a lot of value if we had a south Australian government cloud instead of a vendor specific cloud?
5. That leads to the next question which is actually in sequence. Cloud offerings exist in various shapes and forms. There are a few different service models and some implementations models. So IAAS, PAAS, SAAS and then leads to XAAS. These are the service models and it is incremental obviously in the sequence from infrastructure to software. Then there are the implementation models starting from on premises to off premises, private, public hybrid, which obviously is a mix of private and public. So what would be SAPOL's transition approach towards the cloud so is there a step by step approach an agile sort of an approach?
6. So we have talked about slight transition towards infrastructure as a service, so the starting point of that would be on premise or off-premises.
7. While looking at IAAS, where are we at right now in that process?
8. Do we manage the security of those assets or that is also managed by the vendor?
9. You have already mentioned some challenges but are there other challenges. Or what would be the biggest challenge in our way to move forward in this direction?
10. What are some of the business changes required to this procurement? So how will we operate differently?
11. With the level of service that they expect from IS&T. Do we expect that to improve?
12. The way Information Technology would be operating on an ongoing basis after this transition. Would it be different from how we operate today?
13. We have talked about how Information Technology would be operating. In specific to Information Technology managers and CIOs, with the introduction of cloud, is there a difference in approach and is there a knowledge/practice gap which would have to be filled within IS&T.
14. Would they be managing the vendors and the cloud from here?
15. With the sorts of contracts we are looking at, is it right to say they would be tightly loosed in some sense where the contract management is looking after the contract in a tight way whereas the internal technical resources who are managing those partnership at the next level, they have got the flexibility to improve the service levels according to the changing needs.
16. At any point of time, if we have to move back from the cloud, although that should never come obviously, do you think our contracts should allow us that capacity?
17. Sounds like a plan. So now we have discussed a bit about procurement. A bit more procurement centric questions. According to SA Government's ICT policy statement 1, about Information Technology Governance agencies are required to conform to all legal statutory regulatory and industry and internal requirements. This would pretty much mean that agencies have to look after themselves. So we are given the direction but we have to make sure that the steps we take are right.

18. In specific to cloud, how does the industrial participation policy come in play, for organisations and state government?
19. What are some of the risk considerations for SAPOL while looking at cloud ad how we manage these risks?
20. Back to procurement centric questions. In a lot of organisations procurement sits in one corner and Information Technology in another one, so where do you see the right place for procurement in a procurement like this specifically which is very focused on Information Technology services. And secondly, are the goals of procurement team aligned with those of Information Technology.
21. Regarding your experience in procurements of ICT services and some bits about cloud services as well, can you please give us some considerations about that share your recommendations and experiences for agencies who want to go down this path.

AUTHOR

Dr. Yaser Mirza is an academic, researcher, technology professional and an entrepreneur with over seventeen years of experience working in public and private sector across different agencies in Asia, Middle East and Australia. He is recent experience has been with Government of Australia in various technology management roles, along with parallel academic affiliation with University of South Australia and Federation University Australia.