Ovum

TMT intelligence | informa

Victorian Government Cloud adoption study

A survey of managers and senior executives in the Victorian Government

Kevin Noonan, Chief analyst
kevin.noonan@ovum.com
November 2018

Commissioned by macquarie GOVERNMENT

Contents

Executive summary

Summary

Catalyst

This study takes a close look at cloud services in the Victorian State Government. The research is part of three related surveys commissioned by Macquarie Government, looking at the Australian federal government, the New South Wales government (NSW), and the Victorian government. All surveys were undertaken in 2018, and these build on an earlier federal government survey undertaken in 2015. The combination of these surveys provides a unique perspective that compares changing attitudes over time, and across government jurisdictions.

Ovum view

In 2015, government agencies were still grappling with lingering concerns about viability of cloud, especially relating to security and availability. The most common reason for transitioning to the cloud was “it’s government policy, so we’re doing it”. The survey picked up a strong sense of passive resistance, with an expectation that cloud would just be a passing fad and would disappear over time.

In 2018, it is now a very different market, and this is a consistent message across all three government surveys. Today, the government market is strongly committed to cloud, and has a more practical understanding about the challenges/benefits of cloud transition.

Victorian government responses were the most integrated in their approach to strategic vs tactical issues. For example, Victoria was the only jurisdiction to list functional business owners as the primary trigger for cloud investment, ahead of IT operations.

Key findings – Victorian Government Cloud Study - 2018

Strategy/Policy - A more balanced approach: strategic & tactical

- Key focus areas show a clear blend of strategic and tactical: (1) Improving business processes & agility, (2) responding to government policy direction, (3) supporting business growth & change, (4) applications modernization. Price is now only a middle order issue.
- Key differentiators for contemporary cloud vendors are (1) Customer experience, (2) Security, (3) Ease of procurement, (4) compliance.

Key challenges - Addressing operational realities of transition

- A greater focus is needed on skills and training to deal with a changing work environment
- Improved governance is needed to guide cloud strategy.
- Project complexity in dealing with the realities of cloud transition is turning out to be much more difficult than expected.

Key strengths - Cloud has been integrated into core priorities

- Most important drivers for cloud are (1) Return on investment, (2) My own agency's cloud strategy, (3) Government security compliance, (4) Applications modernization.
- There is a growing familiarity with cloud. Positive experiences in moving to cloud are typically "as expected" & "easier than expected"(65% responses).

Recommendations for government

- Skills shortages will continue to create both immediate and long term challenges. Skills development strategies will need to cater for an ongoing hybrid world, involving a combination of hosted workloads and more than one cloud provider.
- Practical architectural issues need to be addressed for managing existing legacy systems in a technology environment that is becoming increasingly hybrid.
- The development of cloud services in government has come a long way, but there is a shortage of insightful case studies to guide other government agencies.
- The value proposition for cloud is no longer just about cost. Procurement methods need to address cloud in a broader context of enabling organizational agility and flexibility, and driving government digital transformation.
- All of the surveyed agencies identified that some proportion of their existing data holdings require higher levels of secure storage. Cloud may be an option for these data holdings, as an alternative to the expense of increasing the security levels of the internally hosted environments.

Cloud strategy and direction

Management considerations most likely to drive future workloads into the cloud

Management considerations	Weighted score
Return on investment business case	80%
My own agency's cloud strategy	79%
Government security compliance (Australian Signals Directorate)	78%
Application modernization	75%
Government policy	72%
My own agency's assessment of cloud security	70%
Procurement guidelines, government contracts etc	70%
Equipment depreciation cycles	68%
Dealing with the challenges of "Shadow IT"	67%
Availability of OPEX	50%

Ovum Insights:

- Governments are focusing on very different issues, reflecting the status of their own cloud journey.
  - All governments put government policy as a middle order issue. Priorities are no longer about a forced march to cloud, but about a differentiated discussion driven by practical issues.
  - Victorian responses focus on strategic and business issues (ROI, Cloud strategy, Government security compliance)
  - NSW listed security as its top issue.
  - Federal government responses focus on availability of OPEX, Shadow IT and Application Modernization as its top three issues, whereas Victoria and NSW both put Shadow IT and availability of OPEX at the bottom

Which functional groups trigger cloud investment?

Functional groups	Weighted Score
Functional Business Owners	83%
IT Operations	76%
Development team	74%
External factors (e.g. policy change, Whole of Government Strategy)	67%
Cyber-security team	64%

Ovum Insights:

- Business owners lead cloud procurement decisions, followed by IT operations. This response differs significantly from both the NSW and federal government surveys, where IT operations still drive cloud investment. This is a significant step in the growing maturity of cloud investment.

In your own words, please provide some words or a phrase that best describes your cloud internal capability (Summary of responses)

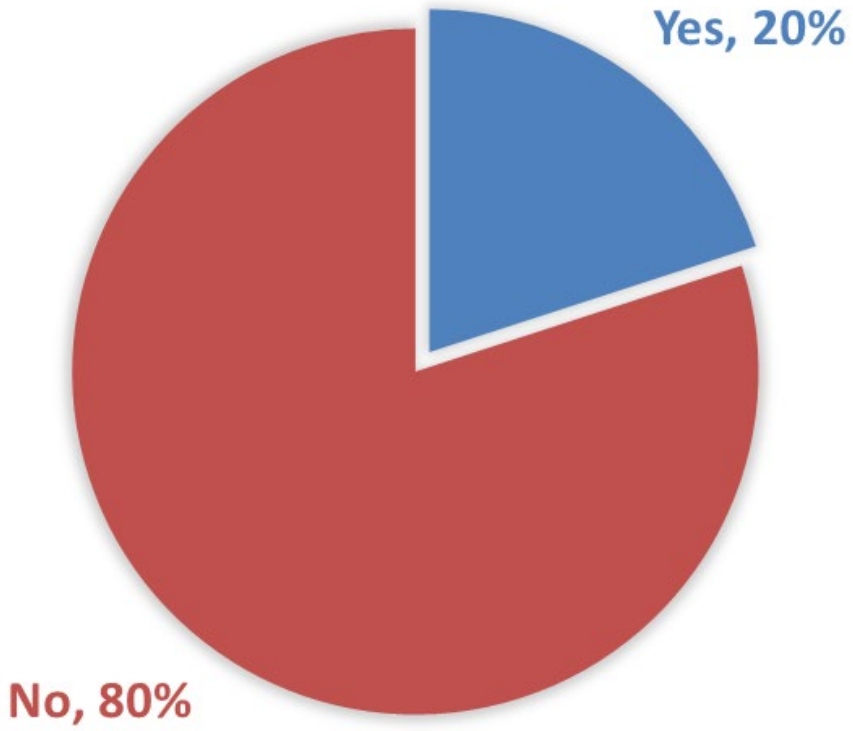
Ovum Insights:

- Cloud is seen as a better environment, not just a cheaper environment.
- Cost is seen as a lower order issue, and is seen more in the context of overall efficiency. This reflects an underlying growth in maturity about the government sector's understanding of cloud services.
- Similar to the NSW response, data management and security were rated as key considerations for the agency's cloud capability.

In your own words, please provide some words or a phrase that best describes your cloud internal capability (Detailed responses)

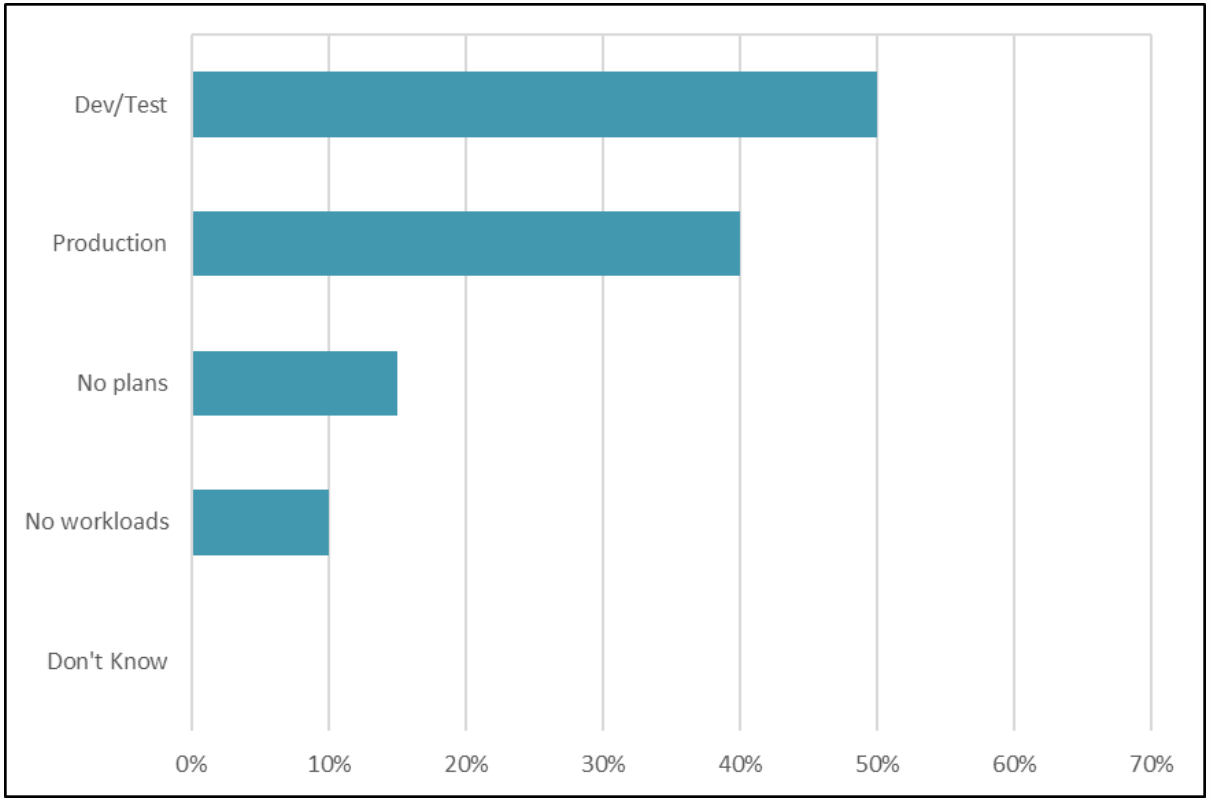
- Better access to data
- Controlling the influence from cloud service providers.
- Drops in the workloads can be well taken care of
- Expandable, flexible
- Flexible , resilient, agile
- Have observed reduced downtime
- Improvised innovation with increased efficiency
- It increased the work efficiency
- It offers latest security technology
- More reliable applications
- Offers enhanced security
- Protects data and systems as the storage is on cloud
- Quality of services has increased
- Reduces the chance of data loss and is very reliable
- The main mechanism works through virtualization
- They offer more flexibility as compared to traditional hosted services
- We are relying more for data storage and risk management
- We are saving money as we are just paying for the computing resources we use
- We can see reduction in the overall cost associated with IT
- With public cloud in place we don't need to worry about security

Are you using containers in production today?



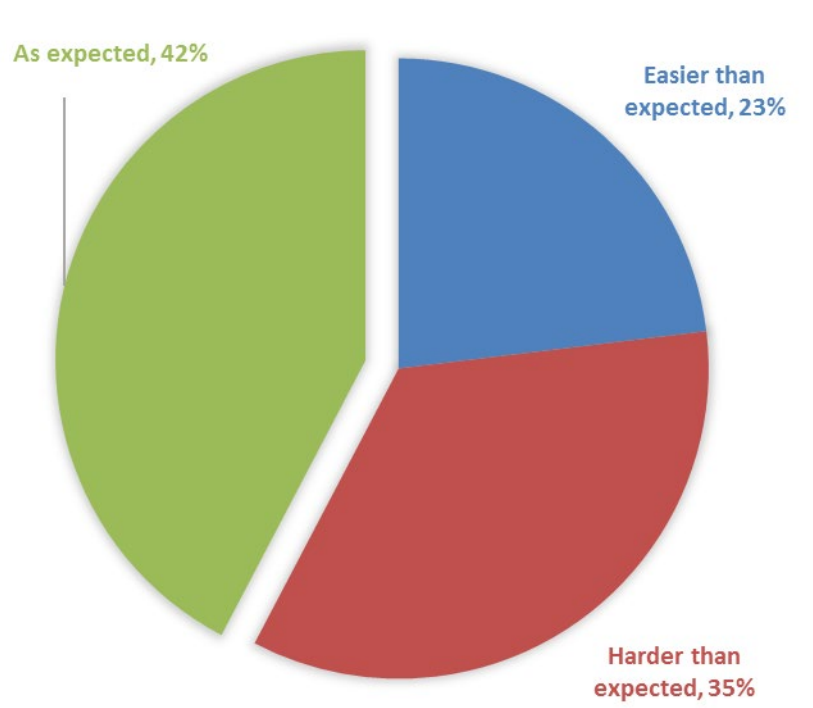
Ovum Insights:
The use of containers is still in early days of its evolution, with only 20% using containers in production today.

If you're planning to use containers in FY19, in which of the following environments?



Ovum Insights:
Of the agencies that are using containers, the majority still relates to systems development and testing.

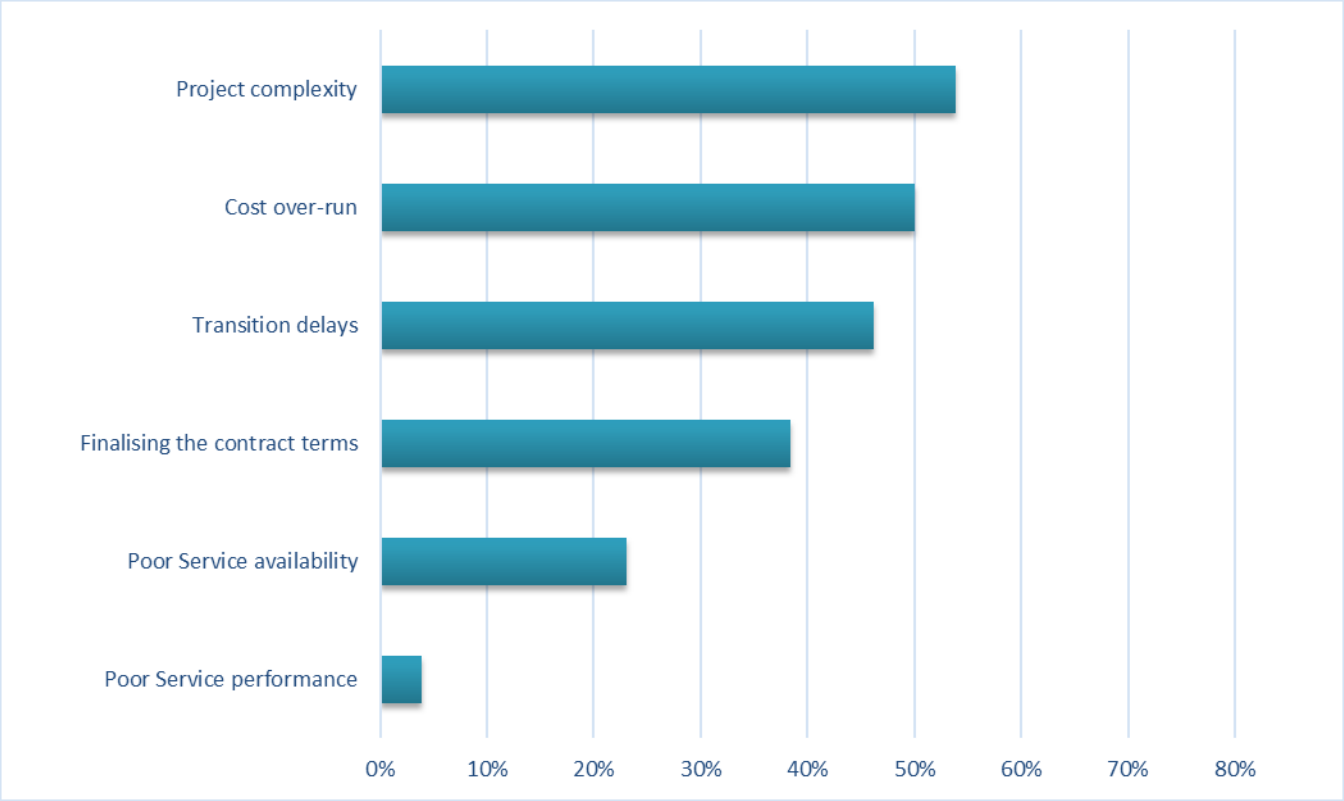
What was your most recent cloud migration experience?



Ovum Insights:

- While it is comforting to see 42% of agencies reported their cloud implementation went as expected, it is concerning that a significant 35% found the implementation was harder than expected.
- The next slide provides some clear insights into the underlying reasons.

Having migrated services to the cloud, which of the following difficulties (if any) were encountered?



Ovum Insights:

This question provides some important insights about the transition to cloud. Vendor performance is rarely the problem. Instead, the challenges tend to relate to an underestimation of the planning and effort that needs to be invested. Project complexity was influenced by the hidden challenges of transitioning legacy workloads, and interconnected system architectures.

Infrastructure as a Service

Please rate how much the following factors have influenced your decision to invest specifically in IaaS

Key factors	Weighted score
Improving business processes and agility	85%
Responding to Government policy direction	83%
Supporting business growth and change	81%
Driving application modernization	77%
Improving security	76%
Acting as a driver for data centre/IT consolidation	76%
Improving IT's responsiveness to the business	75%
Cutting costs	74%
Enabling IT to concentrate on more strategic "value-added" activities	73%
Supporting innovative new business activities	72%
Resolving capacity planning issues	67%
Delivering a better user experience	67%
Replacing legacy systems/infrastructure that are reaching end of life	64%

Ovum Insights:

- The clear message from Victorian government agencies is that IaaS is all about business improvement and modernization, occupying 1st, 3rd and 4th places.
- Government policy continues to be a strong driver for IaaS, coming in 2nd place.
- Security, datacentre consolidation and cutting costs are now middle order issues. In the early days of cloud, these were the hot issues, but the landscape is quite different today. Internal technical issues are giving way to broader business drivers.

In your own words, what are the main factors that influence your investment in IaaS? (Summary of responses)

Ovum Insights:

- This was a free text open-ended question, with no guidance given to the respondent. It was aimed at eliciting top-of-mind issues that could be presented in their own words.
- This time, issues around flexibility, security, data, and cost were most frequently mentioned

In your own words, what are the main factors that influence your investment in IaaS? (Detailed responses)

- Availability
- Better downtime expectation
- Can be deployed easily
- Capital expenditure
- Complexity and compatibility
- Cost and complexity
- Cost plays a major role
- Cost saving based
- Cost savings
- Data Security
- Focus or concern always revolves around security
- Improvised services
- Increased end-user productivity
- Managing expectations around change
- Migration cost
- No investment on capital
- No need to lay major focus on our own data center issues
- Reduced cost and increased recovery times
- Relative advantage
- Reliable network monitoring
- Require less time to get the desired results
- Scalability
- Security and more efficient work
- Security remains the top most concern
- Sense of increased safety
- Technological readiness

Biggest challenges/impediments to using IaaS

	Weighted score
Regulatory/compliance issues	83%
Lack of the necessary internal skills	82%
Lack of a cloud strategy and governance	80%
Availability of suitable offerings that meet our security requirements	78%
Complexity of procurement processes	74%
Difficulty in accurately measuring cost savings from cloud	73%
Lack of understanding of what business benefits cloud can deliver to my organization	72%
Concerns over reliability/availability (outages) of cloud services	72%
Predictability of consumption-based cloud pricing	71%
Migration risks outweigh the perceived business benefits	70%
Lack of the necessary leadership	69%
Practical difficulties in moving funds from CAPEX to OPEX	64%

Ovum Insights:

- Skills availability is seen as a key impediment for using IaaS in all jurisdictions.
- Federal responses were less concerned about compliance and governance, as both of these were mid-order issues. The Federal agencies were much more concerned with (1) CAPEX/OPEX, (2) Skills, (3) Reliability/Availability.
- The Vic survey was a closer match to NSW with primary focus on (1) Cloud strategy/governance, (2) Regulatory/Compliance (3) Skills.
- CAPEX/OPEX was promoted to a mid-order issue for Victoria.
- It appears that CAPEX/OPEX issues appear to grow as IaaS take-up increases. Funding becomes a greater issue.

In your own words, what are the biggest challenges/impediments to using IaaS in your organization? (Summary of responses)

Ovum Insights:

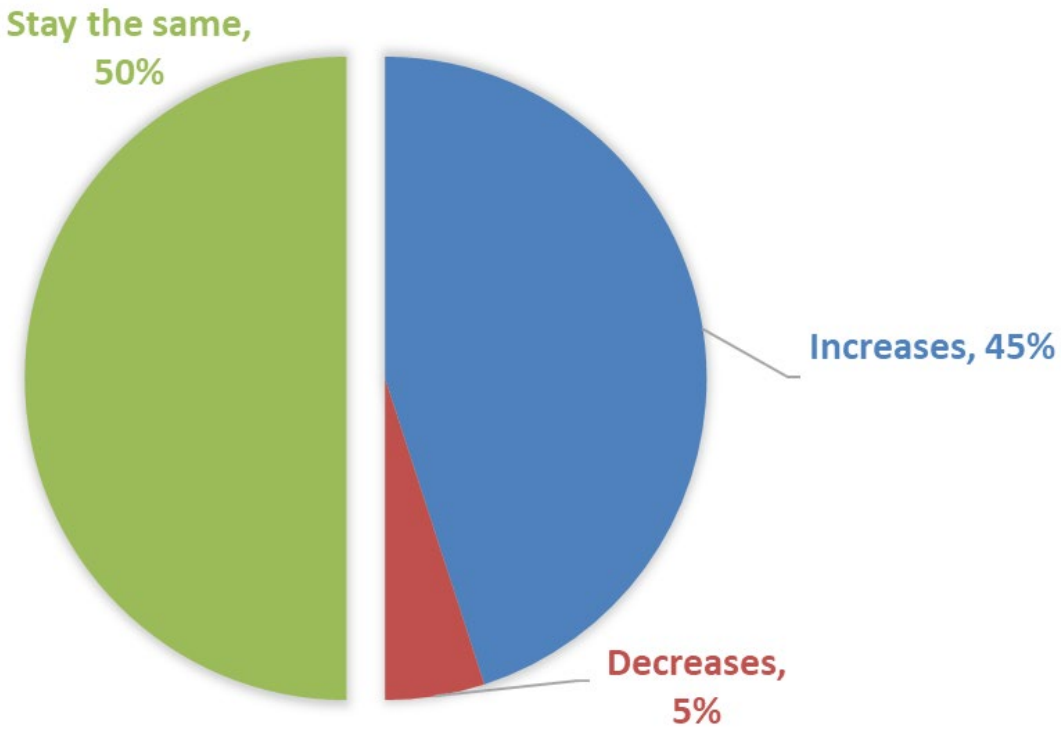
- This was a free text open-ended question, with no guidance given to the respondent
- Management challenges were a common theme throughout the survey, as managers grapple with the operational challenges of moving some of the more complex workloads into the cloud, and the challenges of transition
- Cost was raised as a significant issue. Cost challenges largely related to the overall cost-effectiveness of particular workloads, as well as transition costs

In your own words, what are the biggest challenges/impediments to using IaaS in your organization? (Detailed responses)

- Application , internet speed and cost
- Easy access to company's data
- Enables networking resources
- Energy efficiency
- Fast disaster recovery
- Flexibility related to time
- Flexibility to roll out updates
- I would say competitive pressure
- Improved business agility
- Integration aspects
- More reliable result and better performance
- Organizational context
- Perceived benefits
- Proof of concept
- Reduced latency counts
- Redundancy of the existing infrastructure
- Risk assessment
- Security and cost
- Security of our data
- To attain more output

Cloud security

Does cloud adoption increase or decrease your information security risk exposure?

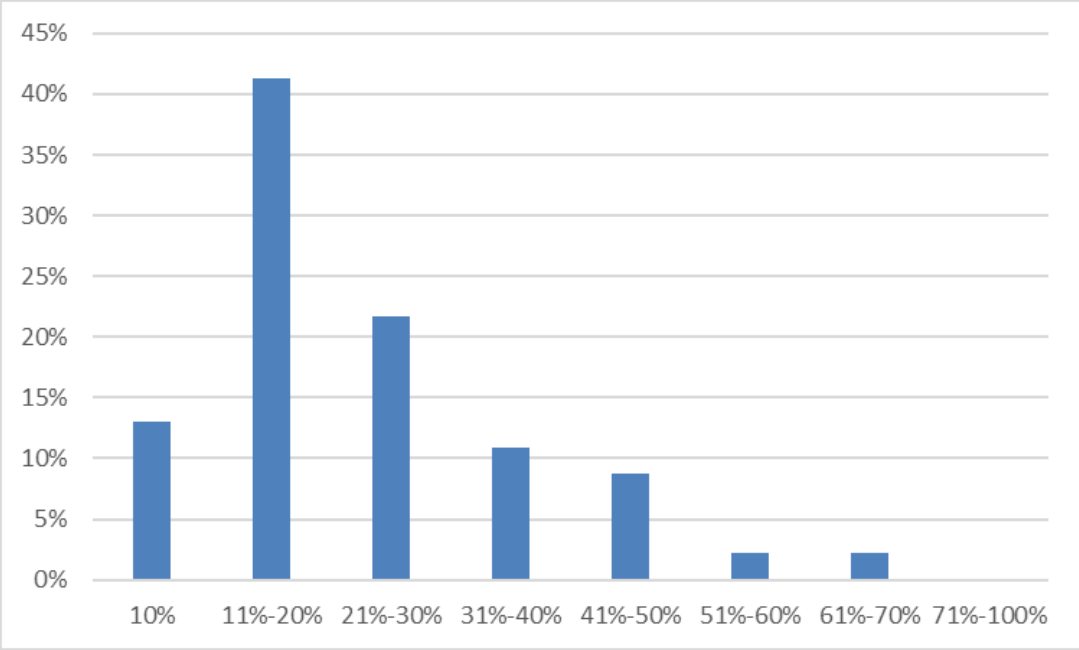


Ovum Insights:

- The Victorian response was marginally positive, with 55% indicating security exposure would either decrease or stay the same.
- It is nonetheless concerning that such a large number of responses (45%) still believe that cloud will increase their security risk exposure

What proportion of your data, if compromised, could cause substantial impact?

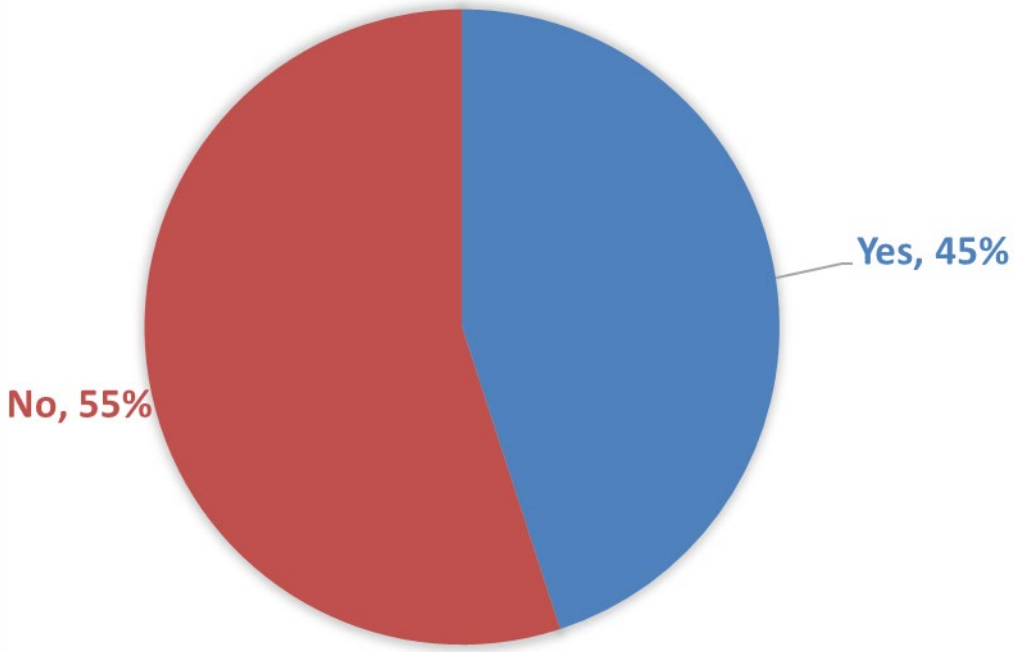
Definition of "Substantial Impact"
➢ Damage to national or state interests
➢ Lead to serious harm of individuals
➢ Undermine the agency's financial viability
➢ Seriously impede the development or operation of major government policy.



Ovum Insights:

- All surveyed Victorian agencies responded with at least some level of impact. The minimum was 10%.
- 63% of government agencies believe between 11% - 30% of their data would have "substantial impact" if compromised.
- The definition of "substantial impact" used in the survey question equates to the federal government's official definition of "Protected" security classification. The survey outcome raises some challenging questions about the treatment of a small but crucial part of each agency's data holdings that require higher levels of security.
- The "Protected" security classification comes with onerous architecture requirements, and these are not commonly addressed in state government systems. If a "Protected" classification is actually required, then this requirement may be better addressed by suitably accredited cloud providers.

Does your agency have any data that could be classified as 'Protected' as defined by Australian government guidelines?



Ovum Insights:

- This question builds on the earlier question, but this time explicitly references the “Protected” classification as defined by Australian government guidelines. Confirming the findings of the previous question, respondents again gave a solid confirmation (45%) of the need for “Protected” classification.
- While it would be unreasonable to suggest the survey is signalling for a widespread upgrade to security infrastructure, it does indicate an underlying concern that government infrastructure should have a strong focus on security.

In your own words, when you think of a "secure cloud" - what features and capabilities would you expect to be provided?

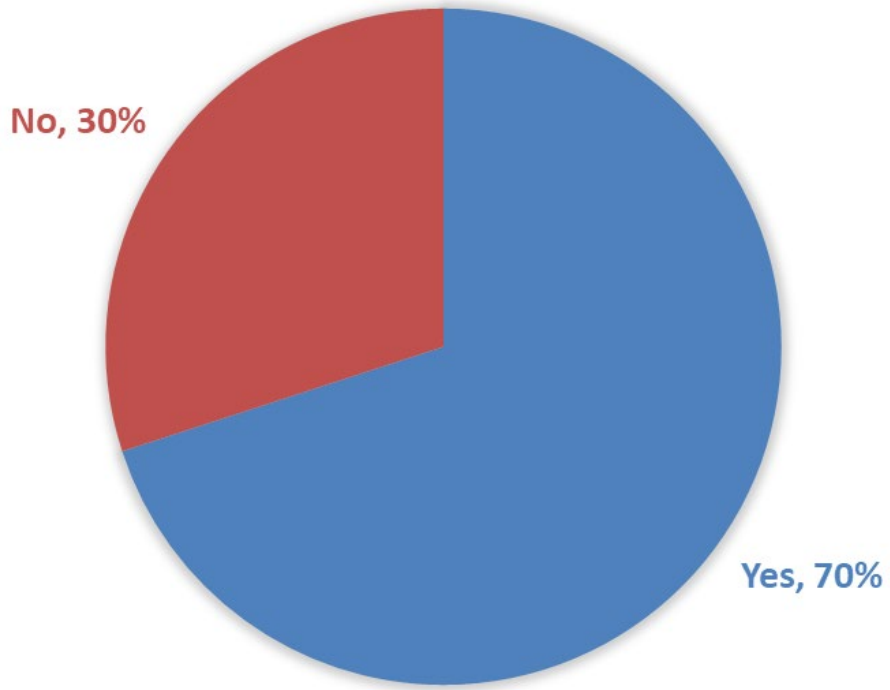
Ovum Insights:

- Security, Data and Risk are seen as the key capabilities that government agencies expect to be provided.
- A key capability of commercial cloud offerings is that security is “baked in” to the standard infrastructure offering.

In your own words, when you think of a "secure cloud" - what features and capabilities would you expect to be provided?

- Access to automatic updates
- Automatic synchronizing features
- Business Continuity and Disaster Recovery
- Data leakage prevention
- Data security
- Data security is the major feature
- Data should be accessed by authorized persons only
- Governance and reporting
- I would say risk management and data security
- Less human interaction
- Migrating workloads with secure connections
- Remote access, as it ensures high productivity and efficiency.
- Risk and compliance
- Risk management
- Risk mitigation
- Scalability and reduced IT cost
- Security , consultancy, costing
- Should be very flexible
- Technical expertise on hand 24/7 remotely
- We get Managed services

Has the introduction of the Certified Cloud Services List by Australian Signals Directorate, influenced your choice of cloud vendors?



Ovum Insights:

- The CCL received strong support from Victorian government agencies (70%).
- Additional interviews by Ovum with government agencies also supported this view. While accepting the limitations of the CCL, government agencies place value on having a government-oriented list that can be referenced in procurement decisions.

Perceptions of cloud service providers

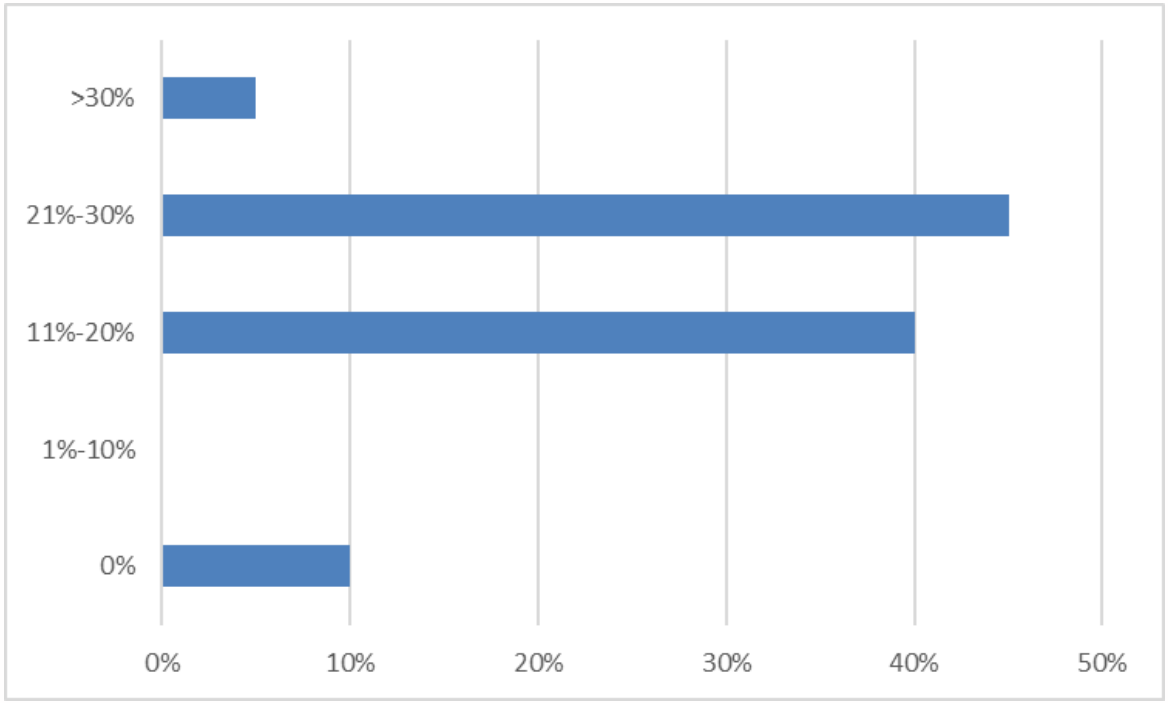
Factors that influence the selection of a cloud provider

Factors that influence selection	Weighted Score
Customer experience	89%
Security	87%
Ease of procurement	82%
Compliance	80%
Developer tooling & platforms	74%
Size / reputation of the cloud provider	73%
Data sensitivity classification	71%
Government policy	71%
Existing contractual relationships	69%
Geographical proximity	68%
Financial objectives	68%
Provider relationship	64%

Ovum Insights:

- Customer experience (#1 factor) reflects a shift in the market toward the pragmatics of delivering good cloud service.
- Issues relating to the importance of security (#2 factor) is a continuing theme underlining the importance of security as a core capability in the vendor cloud offering.
- Government policy is now a middle order issue for Victoria (same for Federal and NSW), reflecting a maturing market. It is no longer about a forced march driven only by overall government policy, but about the practical considerations of moving to cloud.

IaaS workloads: What proportion will be procured via a Managed Service Provider or System Integrator



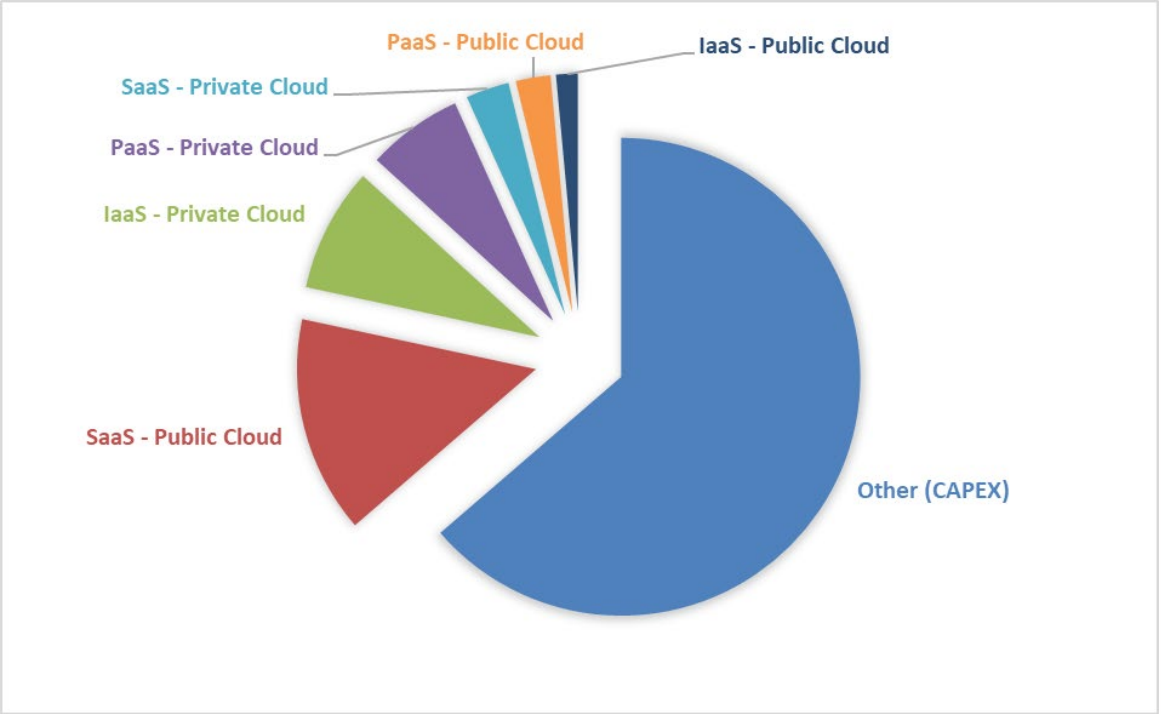
Ovum Insights:

- 85% of respondents put the involvement of third parties at between 11% and 30% of their cloud procurement.
- Managed service providers and system integrators are currently involved in only a minority of cloud procurement, with government agencies preferring instead to deal directly with cloud providers.

Cloud workloads

What percentage of current ICT systems is spent on cloud?

	% of IT spend
Other (CAPEX)	60.9
SaaS - Public Cloud	14.1
IaaS - Private Cloud	8.1
PaaS - Private Cloud	6.2
SaaS - Private Cloud	2.8
PaaS - Public Cloud	2.3
IaaS - Public Cloud	1.4



Ovum Insights:

- Spend on CAPEX is still high (60.9%).
- SaaS public cloud is expected to continue to grow as the major software vendors transition to cloud delivery models, and provide attractive offers to move into the cloud.
- IaaS private cloud sits in 3rd place. IaaS transition is an important part of a cloud transition strategy, as it sharpens focus on the challenges of data location and the management of legacy systems.

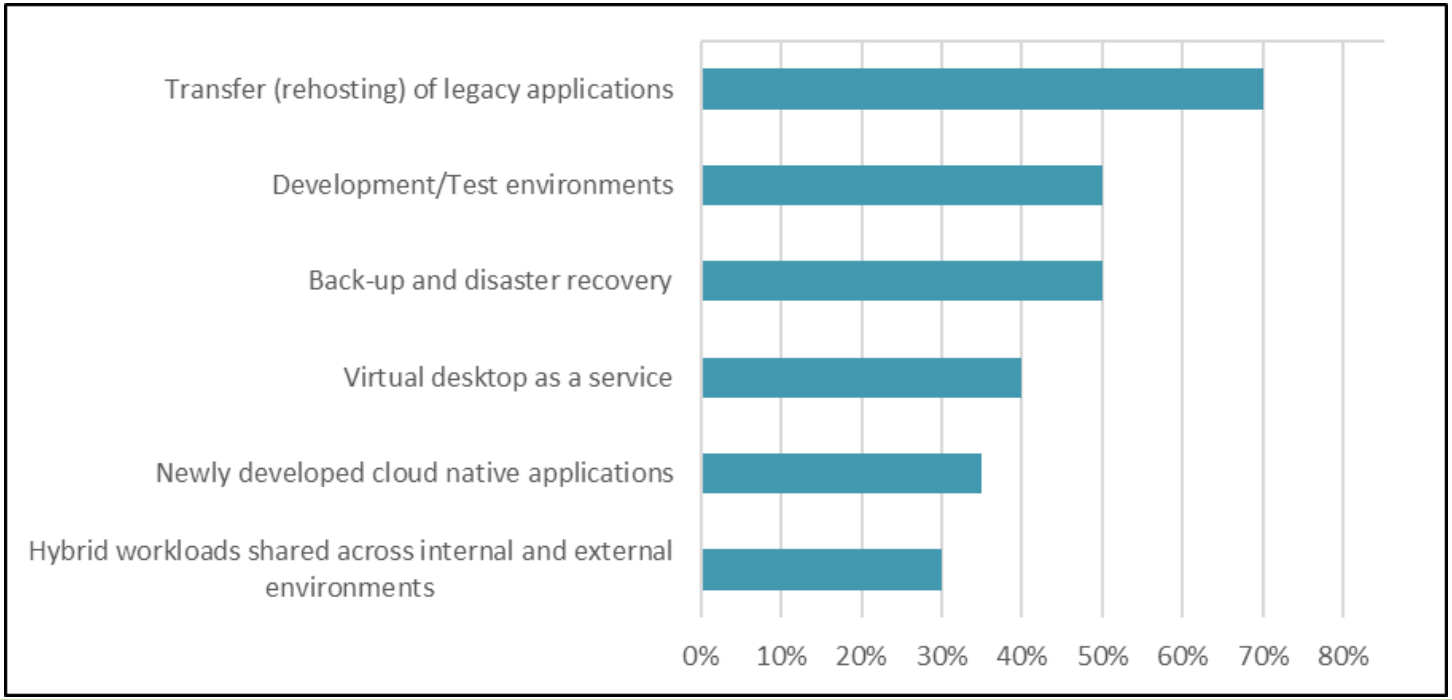
Expected cloud budget split in FY19

(Cloud budget allocation) →	1%-15%	16%-30%	31%-45%	46%-60%
Infrastructure hosting	5%	65%	25%	5%
SaaS/hosted applications	60%	35%	0%	5%
Managed services	2%	39%	59%	0%
Security services	90%	10%	0%	0%
Professional services	100%	0%	0%	0%

Ovum Insights:

- Similar to NSW, the Victorian FY19 cloud budget will be strongly weighted toward infrastructure hosting and managed services.
- 59% of respondents reported they will be allocating 31%-45% of their cloud budget to managed services.
- SaaS/hosted applications are now a clear emerging part of government cloud (35% reporting 16%-18% of their budget). The focus on SaaS/hosted applications is expected to grow as software vendors transition their services to cloud.
- Infrastructure hosting is expected to play an increasing role as government agencies transition legacy systems into the cloud.

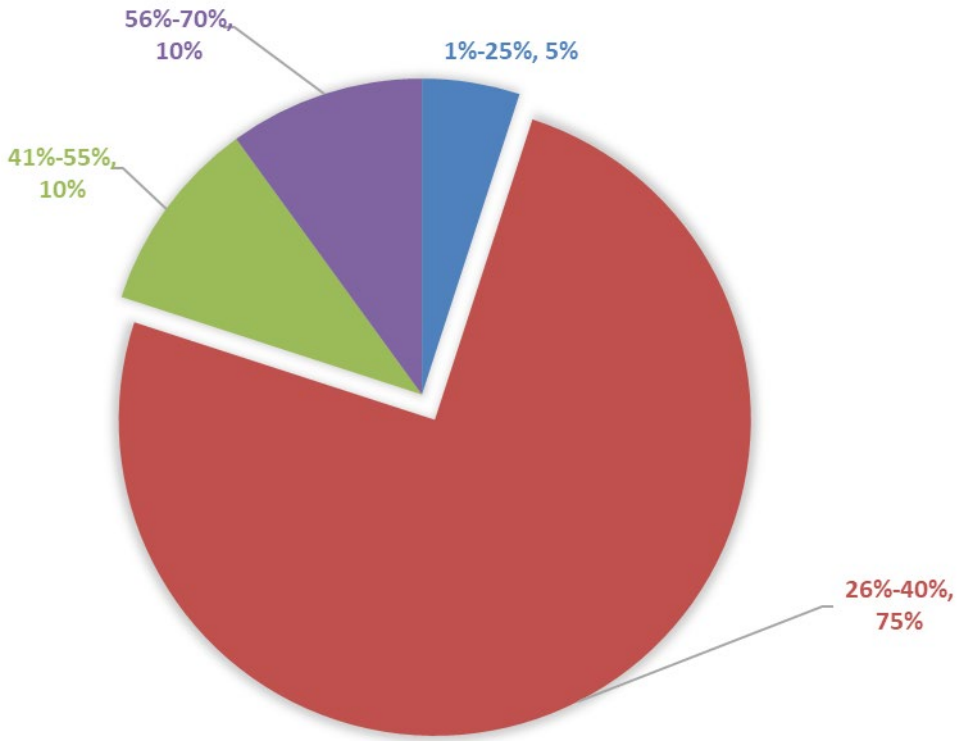
Which workloads do you plan to deploy in FY19 on IaaS?



Ovum Insights:

- It is noteworthy that a significant number of Victorian government agencies (70%) will be addressing the challenging issue of transferring (rehosting) legacy applications. This represents a significant step in the growing sophistication of the government's cloud journey. The most challenging issues, relating to hybrid workloads, are still to be addressed.
- It is unsurprising that traditional cloud workloads (development and test environments, and back-up and disaster recovery), continue to rate highly in agency IaaS plans, as this has been an ongoing focus for IaaS workloads in the past.

What proportion of your workloads will you never move to cloud?



Ovum Insights:

- Hybrid workloads will continue well into the foreseeable future. 75% of respondents reported that 26%-40% of their workload will never move to the cloud. This has significant implications for architecture and skills planning, as long-term strategies will need to cater for mixed workloads.
- The response also signals a growing sophistication in the market where cloud will dominate, but the strengths and weaknesses of cloud offerings are being critically assessed.

Appendix

Appendix

Further reading

"The emergency services sector is facing a disruptive future," IT0007-000876 (March 2016)

"Digital transformation needs to be built on a strong foundation," IT0007-000869 (February 2016)

"It is time to bid farewell to transaction processing," IT0007-000868 (February 2016)

Author

Kevin Noonan, Chief Analyst

kevin.noonan@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer