Victorian Government Cloud Security Guidance

Contents

Document management

Document		Date
Name	Victorian Government Cloud Security Guidance	4 July 2018
Reference	VG-CISO Guidance 01	4 July 2018
Approved	Geoff Beggs Executive Director Enterprise Services Branch Department of Premier and Cabinet	4 July 2018
Issued	John O'Driscoll Victorian Government Chief Information Security Officer, Enterprise Solutions Branch Department of Premier and Cabinet	4 July 2018
Authority	Victorian Government Cyber Security Strategy	August 2017
Contact for updates	vicgov.ciso@dpc.vic.gov.au	
Registration	Version 1.1 D18/51419	

Cloud security guidance

Summary

The Victorian government's preferred order of consideration for ICT investment is to first share solutions across government, where suitable, and second to access cloud services where no existing suitable shared services exist[1].

All systems including cloud systems will have a level of residual risk that must be understood and considered acceptable by the agency. The purpose of this guideline is to assist agencies understand the risk and help determine if it is acceptable.

Cloud services will often be considered in replacement of existing services. When assessing the risk of a cloud system, it is important to consider this in comparison to the existing system. In some circumstances the cloud service may not have all desirable controls but represent an improvement over the current environment. In these circumstances it may be appropriate to accept a less than perfect system if it results in an overall reduction in risk.

Cloud services can provide a powerful, low cost delivery mechanism to deliver services and provide a significant enhancement to the security of IT systems when implemented well.

Agencies should:

- Implement appropriate governance
- Understand the nature of information being handled by the service
- Understand the security capability of the service
- Secure aspects of the service that are the client's responsibility.

Cloud services that have been certified by the Australian Signals Directorate (ASD) are preferred, as they provide a high level of assurance to security capability. Other vendors should be assessed against the risk profile established for the proposed system and associated information.

Scope

In scope

The term 'agency' within this document refers to any VPS entity.

This guidance applies to all Victorian Public Service (VPS) departments and agencies. It is also the recommended guidance for all service delivery partners of VPS entities that use cloud services to deliver government services.

Out of scope

Compliance with legislative requirements such as the Public Records Act.

[1] *Victorian Government IT Strategy 2016-2020*

Procurement obligations.

This guidance document does not address the full lifecycle of cloud usage. For a comprehensive cloud assessment methodology, please refer to:

- *Digital Transformation Agency and the Secure Cloud Strategy* [2]
- *The Open Management Group, Cloud Standards Customer Council (CSCC), Security for Cloud Computing: Ten Steps to Ensure Success*.[3]

Audience

This guideline is targeted at general management, cyber security and IT security practitioners and assumes a basic knowledge of cloud computing and enterprise security architectures.

Guidance

Governance

1. Single agency – if the service is to be used by a single agency, the client agency is responsible for all governance and risk management activities of the service.
2. If an instance of the service is to be used by multiple Victorian government agencies, the following model is recommended:

    2.1. Lead agency – an agreed agency is given responsibility to oversee the security evaluation and management planning process. This will involve co-operating with participating agencies to ensure visibility of risk and possibly access resources to undertake the process. The lead agency takes responsibility for ongoing management of the system security plan.

    2.2. Participating agency – all agencies that will place information on the service remain accountable for information security and should be satisfied that risk is appropriately managed. This will involve co-operation with the lead agency to ensure risks are clearly understood and possibly provide resources in assessment, planning and ongoing management.

    2.3. Advisory agency – for projects of high significance, the Victorian Cyber Security Unit within Enterprise Solutions Branch in DPC may be invited to provide specialist support in the selection and planning governance.

Understand the nature of information being handled by the service

3. Understand the nature of the information that the service will be handling in transit and at rest. The value of this information should be rated using the Victorian Protective Data Security Framework (VPDSF) Business Impact Levels[4] (BIL's).

4. Identify whether information is subject to any specific legislative obligations such as those relating to privacy or health records.

[2] www.dta.gov.au/files/cloud-strategy/secure-cloud-strategy.pdf

[3] www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf.

[4] https://www.cpdp.vic.gov.au/images/content/pdf/data_security/20170504%20VPDSF%20Ch2-AppB%20BIL%20Table%20V1.1.pdf

4.1. If information has specific legislative requirements, develop a plan to meet these requirements in addition to the steps in this document.

Understand the security capability of the service

5. If information has a confidentiality rating greater than zero, preference should be given to cloud providers that have been certified by ASD.
   https://www.asd.gov.au/infosec/irap/certified_clouds.htm

   5.1. It remains the responsibility of agencies to understand whether the security capability of the service is appropriate to the risk. If an ASD-certified cloud service is chosen, the agency should obtain a copy of the Information Security Registered Assessors Program (IRAP) assessment to make a more informed risk assessment.

   5.2. In other cases, an informed risk decision should be made through gaining insight into the security capability of the service. This can be achieved through alternate certifications such as ISO 27001 or assessment tools such as the Cloud Security Alliance (CSA) control matrix[5].

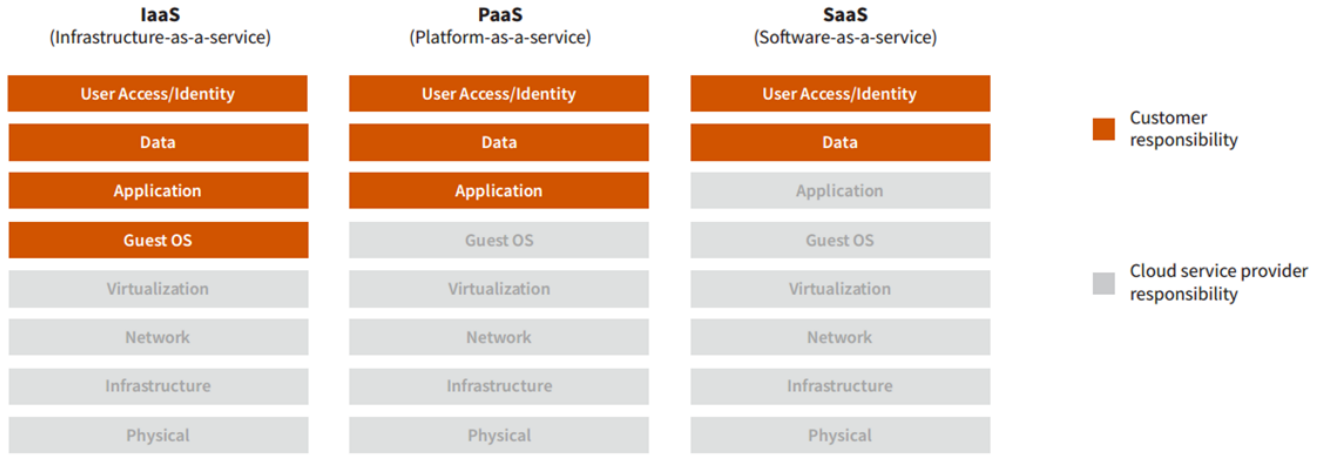
6. The security functionality of cloud services varies greatly. Agencies should understand the security configuration options of the service.

Ensure the agency has secured aspects of the service that are the client's responsibility

7. Cloud service offerings generally follow one of three models:

   - Infrastructure as a Service (IaaS)
   - Platform as a Service (PaaS)
   - Software as a Service (SaaS)

With all of these models, some security responsibility remains with the customer. At a high level, customer responsibilities and service provider responsibilities follow the model below. Agencies should have a plan in place to address the security responsibilities of the customer.



Note 6

[5] https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/

[6] Cloud security models - Oracle and KPMG cloud threat report, 2018

Agencies should document a System Security Plan. Examples of possible security controls include:

8. Ensure access to appropriately skilled resources to secure the service. This may involve training in-house staff or procuring specialist support.
9. Incorporate appropriate Identity and Access Management (IdAM) from the outset, ideally based on roles, especially for administration duties.
10. Ensure secure communications between client and the service. This may include use of Transport Layer Security (TLS) or Virtual Private Networks (VPN) protected access. For IaaS, segment and contain network traffic using the Cloud Service Providers (CSPs) virtual network.
11. Establish a security control regime using third-party tools (Cloud Access Security Broker) to achieve better visibility, data security, threat protection and compliance, as well as to automate security configurations where possible.
12. Take full accountability for application and data security in production, staging, development and test (non-production) environments and ensure roles and responsibilities are clear.
13. Standardise all cloud deployments on 'hardened' images such as those available from Centre for Internet Security (CIS).
14. Ensure that contracts support the ability to revert from the cloud. Clarify data sovereignty and the location of online and offline backups.
15. Agencies should leverage existing security assessments where available for each contract. An example using the cloud security assessment table published by the Cloud Standards Customer Council (CSCC) is provided in the table below[7].
16. Ensure mechanisms are in place for the service provider to notify the client agency of cyber incidents and data breaches.
17. Ensure regular independent security auditing of the service. This will often be achieved under existing certification and accreditations such as ASD cloud or ISO27001 certification.
18. Agencies should determine if any further controls are required.

[7] http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf

Sample executive cloud security assessment

Question	Assessment	Notes
What is the nature of the information being handled by the service?	VPDSF Confidentiality Rating: 0-4 VPDSF Integrity Rating: 0-4 VPDSF Availability Rating:0-4 Subject to legislative obligations such as privacy: Yes/No	
Is a detailed risk assessment required and has this been undertaken?	Yes/No	
Preferred - Is the service certified by Australian Signals Directorate (ASD) to the confidentiality level of the information being handled?	Yes/No	
• If Yes, has the IRAP report been assessed and found to be acceptable	Yes/No	
If the service has not been ASD certified, is the service certified to a recognised security standards such as ISO27001?	Yes/No	
• If Yes, has the certification report and Statement of Applicability (SoA) or equivalent been assessed and found to be acceptable	Yes/No	
Are legal terms and conditions clearly understood and acceptable?	Yes/Partially/No	
Are the responsibilities of the service provider and the consumer clearly understood by all parties?	Yes/No	
Have security capabilities of the service been clearly articulated and verified by independent audit?	Yes/Partially/No	
Does the agency have the capability and knowledge to securely undertake activities that are the responsibility of the agency?	Yes/Partially/No	
Has the agency documented the System Security Plan (SSP) including Identity and Access Management?	Yes/Partially/No	

Detailed assessment

If the service has not been certified by ASD, a detailed risk assessment should be undertaken when the information is rated ‘1’ or higher on the VPDSF information business impact levels or is subject to other legislative obligations. The agency should determine if is a detailed risk assessment is required for services that have been ASD certified.

Agencies should use an industry standard risk assessment framework to guide this assessment. At the time of publication, the following control assessment methodology is recommended:

- https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/

Background

The Victorian government Chief Information Security Officer (CISO) issues cyber security guidance as part of WOVG responsibilities defined in the Victorian Government Cyber Security Strategy (cyber security strategy) approved by Cabinet and launched in August 2017.

As part of the cyber security strategy the CISO has undertaken an assessment of current cloud security models and issues this guidance in relation to the government's obligations as a customer when consuming cloud services in a shared security model (cyber security strategy action 20).

Successful and secure cloud service consumption requires that the roles and responsibilities relating to information security are clearly defined and understood. While agencies retain accountability, security responsibilities are split between the cloud service consumer and the CSP. Global CSPs are typically less flexible in meeting government specific requirements, so agencies face having to manage security models that vary between different CSPs and between different cloud service deployment models.[8]

Key challenges

- A number of high profile cyber incidents (data breaches) in 2017 were caused by sensitive or confidential data being loaded into unsecure development, testing or staging cloud instances. This reconfirms Gartner's forecast from 2015, in which it estimated that by 2020, 95 per cent of cloud security failures will be due to customer activity[9].
  - Challenge: How do you manage agency and service provider staff behaviour to implement 'security by design' when consuming cloud services.
- CSP security responsibilities differ between IaaS-, PaaS- and SaaS-based service models.
  - Challenge: What security architectures and assurance regimes are required for each different cloud service model and provider?
- Regardless of the 'as a service' model being used, IdAM and data security are always customer accountabilities.
  - Challenge: How do you maintain consistency and best practice IdAM, especially privileged access management (PAM) for all administrators and users, whether CSP or agency?
- Moving workloads to a secure cloud platform doesn't automatically make the system more secure. In June 2017 the "Petya" cyber-attack compromised CSPs.
  - Challenge: What end-to-end security assurance is required to support service delivery reliability?

[8] *Cloud Customer Architecture for Securing Workloads on Cloud Services*. page 7 (www.cloud-council.org/deliverables/CSCC-Cloud-Customer-Architecture-for-Securing-Workloads-on-Cloud-Services.pdf)
[9] https://www.gartner.com/newsroom/id/3143718

- CSP isolation keeps tenants separated.
  - Challenge: What additional application, logical, network or storage segregation is required as a result of the system's sensitivity, classification, risk profile and compliance requirement?
- For workloads that require compliance certification/accreditation
  - Challenge: What application-level audits and certifications are required and how is assurance reporting coordinated with the CSP?

References and resources

Cloud ICT services and security capabilities continue to evolve. It is important for consumers to continue to update understanding of risks and improving security capabilities provided in the cloud market place.

The following table provides a list of resources available to agencies to support their respective cloud shared responsibility security arrangements. It also includes resources to support full lifecycle cloud decision making.

The table comprises three groups of references:

- General advice on cloud security
- Cloud shared security specific advice
- Cloud vendor reference information on cloud shared security models

General advice on cloud security

Source	Reference	Advice
Office of Victorian Information Commissioner	*Cloud Computing in the Victorian Public Sector* www.cpdp.vic.gov.au/menu-resources/resources-data-security/cloud-services	A detailed discussion paper exploring issues such as legislative requirements including privacy and public records act, issued in 2015 by the Commissioner for Privacy and Data Protection.
Australian Signals Directorate (ASD)	*Cloud Computing Security for Tenants.* This document, developed by ASD, is designed to assist a tenant organisation's cyber security team, cloud architects and business representatives to work together to perform a risk assessment and use cloud services securely. www.asd.gov.au/publications/protect/Cloud_Computing_Security_for_Tenants.pdf	ASD Certified Cloud Services: ASD has awarded ASD Certification to the listed cloud service providers for specified cloud services. Agencies should review the ASD Cloud Computing Security documents, which describe security risk mitigations associated with cloud computing. Australian Government agencies should also perform due diligence reviews of the legal, financial and privacy risks associated with procuring cloud services (which this certification does not include). The cloud computing security for tenants document includes advice in relation to customer responsibilities

Source	Reference	Advice
Cloud Standards Customer Council (CSCC)	The CSCC is managed by the Object Management Group (OMG). The CSCC™ is an end user advocacy group dedicated to accelerating cloud's successful adoption and drilling down into the standards, security and interoperability issues surrounding the transition to the cloud.	Excellent in-depth guides to inform cloud shared responsibility security arrangements. *Security for Cloud Computing: 10 steps to ensure success V3.0* A practical reference to help enterprise information technology (IT) and business decision-makers analyse the security implications of cloud computing on their business. This guide includes a list of steps, along with guidance and strategies, designed to help decision-makers evaluate and compare the security and privacy elements of cloud service offerings from different cloud providers in key areas. *Practical Guide to Cloud Computing V3.0* The cyber security strategy's seminal deliverable outlines key definitions, characteristics and benefits of cloud computing. A ten-step roadmap for cloud computing contains guidance and strategies for the successful migration and deployment of cloud computing applications.
Cloud Security Alliance (CSA)	The CSA is described itself as "the world's leading organisation dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment."	*The Treacherous 12 Top Threats and Industry Insights* is a comprehensive document that addresses customer responsibilities. https://downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.pdf

Source	Reference	Advice
Center for Internet Security (CIS)	The Victorian government has a subscription to the CIS and has complete access to all the hardened images for cloud builds and for Amazon Web Services Foundations (*CIS Amazon Web Services Foundations Benchmark version 1.1.0*). https://www.cisecurity.org/hardened-images/	Government cloud consumers should always use the available CIS hardened images for all their cloud workloads. CIS offers dozens of hardened images via major cloud computing vendors. CIS Hardened Images are securely configured according to applicable CIS Benchmarks.
Information Security Forum (ISF)	The Victorian government has a subscription to the ISF. The ISF has a number of resources available to support agencies to develop their respective cloud shared responsibility security arrangements.	The ISF *Standard of Good Practice* (SoGP) has a cloud computing policy and a cloud service contracts section.

Cloud shared security specific advice

Source	Content	Description
Gartner	*Clouds Are Secure: Are You Using Them Securely?* Published: 22 September 2015	Gartner advice for CISOs and security leaders on the scope of their responsibilities for security in the cloud.
Gartner	*Staying Secure in the Cloud Is a Shared Responsibility* Refreshed: 08 May 2017 | Published: 07 April 2016	Gartner latest advice is that CISOs and security leaders should understand the scope of their responsibilities for security in the cloud.
ISF Briefing Paper	*Securing Collaboration Platforms*	This briefing paper addresses the five major risks and mitigation options when using a collaboration platform incorrectly secured. This applies directly to cloud collaboration platforms.
ISF Member Content	Member Presentation 09 - David Frith - The use of cloud brokers and their use in cloud migration, assessment and portability.pdf https://www.isflive.org/docs/DOC-22180	What cloud brokers are, why they're used, and what controls they can provide - he also described how they can help with cloud readiness assessments, workload governance, cloud management and portability.
Securosis	https://securosis.com/blog/wrangling-backoffice-security-in-the-age-of-cloud https://securosis.com/blog/wrangling-backoffice-security-in-the-cloud-age-part-2	Security blog site.

Taxonomy

Term	Definition
ASD	Australian Signals Directorate
Agency	Any legal entity within the Victorian public sector (VPS).
Client	Agency consuming the service
Cloud	See NIST Special Publication 800-145[10]
Instance of the service	Commonly a service with shared access.
IRAP	Information Security Registered Assessors Program managed by ASD.[11]
ISO27001	ISO/IEC 27001:2013 is the international standard that describes better practice for an ISMS (information security management system)

[10] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
[11] https://www.asd.gov.au/infosec/irap/irap_assessments.htm