Whole of Victorian Government Guideline
Information Security

Cloud Computing Security Considerations

Guideline

Departments and agencies can use this guideline to assist in performing the risk assessments required under Information Security standards SEC/STD/01 and SEC/STD/02 to make an informed decision as to whether cloud computing is currently suitable to meet their business goals with an acceptable level of risk.

Keywords:	Cloud, Information security, risk assessment, out source	
Identifier: SEC/GUIDE/06	**Version no.:** 1.0	**Status:** Final
Issue date: 1 December 2011	**Date of effect:** 01 January 2012	**Next review date:** 01 January 2014
Owner: Government Services Division Department of Treasury and Finance Victorian Government	**Issuing authority:** Government Services Division Department of Treasury and Finance Victorian Government	

Overview

Cloud computing offers potential benefits including cost savings, agility and improved business outcomes for Victorian government agencies, however there are a variety of information security risks that need to be carefully considered.

The Victorian Government requires that each department and agency develop an Information Security Management Framework (ISMF SEC/STD/01) and assess and manage the exposure risk of confidential information under its control (Data Classification and Management Standard SEC/STD/02).

This guideline identifies specific resources and illustrates an example approach that can assist agencies to perform the risk assessment and make an informed decision as to whether cloud computing is suitable to meet their business requirements with an acceptable level of risk.

Audience

The use of this guideline is recommended for all Victorian Government departments, four inner budget agencies (VicRoads, Victoria Police, Environment Protection Authority and State Revenue Office) and CenITex.

Context

Information Security guidelines provide advice and guidance to available resources and are to be used within the context of compliance with the WoVG Information Security Policy and Standards. This guideline provides advice only and can be modified or supplemented to suit the needs of the department or agency.

The Victorian Government's general approach to the development of Information Security guidelines is that:

- we do not intend to undertake original research on most information security topics;
- for most topic areas of a generic nature there are usually extensive existing resources available to provide guidance;
- the most relevant, available and maintained content should be identified for re-use by the Victorian Government;
- the information and publishing sources will include (but are not limited to):
    - Australian Government Information Management Office (AGIMO);
    - Commonwealth Government Defence Signals Directorate (DSD);
    - Information Security Forum (ISF);
    - Australian Government Attorney General's Department; and
    - Commonwealth and Victorian Information Privacy Commissioners;
- the selection of the subject matter for guidelines will be based upon an agreed schedule endorsed by the Information Security Advisory Group (ISAG).

The Victorian Government ISMF standard (SEC/STD/01) applies to the management of all aspects of the security of ICT and the Data Classification standard (SEC/STD/02) applies to the management of all information. This guideline supports these standards in relation to security considerations for Cloud Computing.

Resources

Commonwealth Government Australian Government Information Management Office (AGIMO)

General Introduction to Cloud Computing

The Department of Finance and Deregulation, through the Australian Government Information Management Office, has consulted with government agencies, industry and the public to develop an Australian Government Cloud Computing Strategic Direction paper to explore the opportunities and impacts of cloud computing.

http://www.finance.gov.au/e-government/strategy-and-governance/cloud-computing.html

Commonwealth Government Defence Signals Directorate (DSD)

Cloud Computing Security Considerations

The DSD discussion paper assists agencies to perform a risk assessment and make an informed decision as to whether cloud computing is currently suitable to meet their business goals with an acceptable level of risk.

http://www.dsd.gov.au/infosec/cloudsecurity.htm

Victorian Government Office of the Victorian Privacy commissioner (OVPC)

The Office of the Victorian Privacy Commissioner has published an ***Information Sheet*** that gives a brief overview of how the Information Privacy Act 2000 (Vic) applies to cloud computing technologies.

Particular attention should be given to the sections documenting 'questions to consider'.

http://www.privacy.vic.gov.au/privacy/web2.nsf/files/cloud-computing/$file/info_sheet_03_11.pdf

Victorian Government Solicitor's Office (VGSO)

Client Newsletter August 2011 - Head in the Cloud, Feet Firmly Planted

http://www.vgso.vic.gov.au

Information Security Forum (ISF)

Securing Cloud Computing: Addressing the Seven Deadly Sins

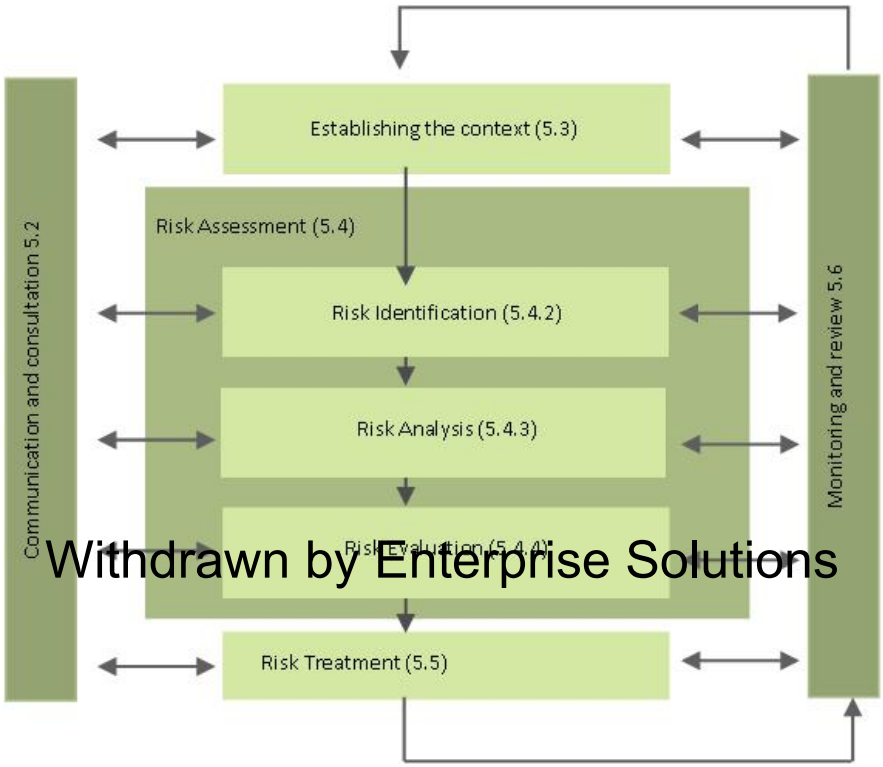
Commercial and Not for Profit Source, Published January 2011. Available to ISF members at:

https://www.securityforum.org/?page=publicdownloadcloud

Example Approach

An approach to managing risk is outlined in the Victorian Government Risk Management Framework (VGRMF), issued by the Department of Treasury and Finance, that provides for a minimum risk management standard across public sector agencies. The VGRMF is consistent with the Australian/New Zealand Risk Management Standard: *AS/NZS ISO 31000:2009* or its successor, and DTF's Information Security SEC STD 02 – Data Classification.

VGRMF Risk management process



The key elements of the risk management process are as follows:

- **Communication and consultation** – communication and consultation with external and internal stakeholders should take place during all stages of the risk management process. This ensures that those accountable for implementing the risk management process and stakeholders understand the basis on which decisions are made, and the reasons why particular actions are required.
- **Establishing the context** – establish the external, internal, and risk management context in which the rest of the risk management process will take place. By establishing the context, the organisation articulates its objectives, defines the external and internal parameters to be taken into account when managing risk, and sets the scope and risk criteria for the remaining process.
- **Risk assessment** – risk assessment is the overall process of risk identification, risk analysis and risk evaluation. *IEC/ISO 31010:2009 Risk Management - Risk Assessment Techniques* provides further guidance on risk assessment techniques.
- **Risk identification** – the aim is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives.
- **Risk analysis** – risk is analysed by determining consequences and their likelihood, and other attributes of the risk. It provides an input to risk evaluation, decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods.

- **Risk evaluation** – involves comparing the level of risk with risk criteria and making decisions about which risks need treatment and the priority for treatment implementation.
- **Risk treatment** – risk treatment involves selecting one or more options for modifying risks, and implementing those options. When implemented, treatments provide or modify the controls.
- **Monitoring and review** – risks and the effectiveness of controls and risk treatments need to be monitored, reviewed and reported to ensure changing context and circumstances do not alter priorities.

Additional resources

- **National Institute of Standards and Technology - *Cloud Computing***
  http://csrc.nist.gov/groups/SNS/cloud-computing
- **European Network and Information Security Agency**
  Cloud Computing Security Risk Assessment
  http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment
  Security and Resilience in Governmental Clouds
  http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds
- **Cloud Security Alliance**
  Security Guidance
  http://www.cloudsecurityalliance.org/guidance
  Top Threats to Cloud Computing
  http://www.cloudsecurityalliance.org/topthreats.html
  Governance, Risk Management and Compliance Stack
  http://www.cloudsecurityalliance.org/grcstack.html
- **Delimiter - *The Australian Private Cloud: Who Sells It?***
  http://delimiter.com.au/2010/10/26/the-australian-private-cloud-who-sells-it
- **Torry Harris - *Comparison of Cloud Providers***
  http://www.thbs.com/pdfs/Comparison%20of%20Cloud%20computing%20services.pdf
- **CloudHarmony - *Cloud Speed Test***
  http://www.cloudharmony.com/speedtest
- **Web Hosting Talk**
  http://www.webhostingtalk.com
  http://www.webhostingtalk.com.au

Further information

For further information regarding this guideline please contact the Government Services Division, Department of Treasury and Finance, at info.cio@dtf.vic.gov.au.

Glossary

Terms as defined by the Australian Government Information Management Office (AGIMO) in Cloud Computing Strategic Direction paper
http://www.finance.gov.au/e-government/strategy-and-governance/docs/final_cloud_computing_strategy_version_1.pdf

Term	Meaning
Cloud	A metaphor for a global network, first used in reference to the telephone network and now commonly used to represent the Internet.
Cloud computing	Refers to style of computing in which various resources – servers, applications, data, and other often virtualised resources – are integrated and provided as a service over the Internet. Cloud computing isn't a new technology nor a new architecture .. it's a new delivery model.

Version history

Version	Date	GSD TRIM ref	Details
0.1	1 September 2011	D11/192132	Initial Draft
0.2	28 September 2011	D11/192132	Internal review
0.3	1 October 2011	D11/192132	ISAG review
0.4	3 November 2011	D11/192132	To ISAG for endorsement. Was endorsed subject to inclusion of reference to the VGRMF
1.0	24 November 2011	D11/192132	To CIO Council for noting. Was noted, with request for next version to include summary checklist of key elements to consider as identified in resources.

Withdrawn by Enterprise Solutions