20.1. Cloud Computing

Objective

20.1.1. Cloud systems risks are identified and managed and that Official Information and agency information systems are protected in accordance with Cabinet Directives, the PSR, the New Zealand Government Security Classification System, the NZISM and with other government security requirements and guidance.

Context

Terminology

20.1.2. Terminology and definitions of cloud models and services used in this section are consistent with NIST Special Publication 800-145, The NIST Definition of Cloud Computing, dated September 2011 (see table of References below).

20.1.3. A fundamental construct in the management of risk in cloud environment is that of Trust Zones and Trust Boundaries. A Trust Zone is a zoning construct based on levels of trust, classification, information asset value and essential information security. A Trust Boundary is the interface between two or more Trust Zones. Trust Zones use the principles of separation and segregation to manage sensitive information assets and ensure security policies are consistently applied to all assets in a particular trust Zone. Refer also to Section 22.2 – Virtualisation.

Separation and Segregation

20.1.4. Separation and Segregation is determined by system function and the sensitivity of the data the system stores, processes and transmits. One common example is placing systems that require a connection to the Internet into a demilitarized zone (DMZ) that is separated and segregated (isolated) from more sensitive systems.

20.1.5. Separation and Segregation limits the ability of an intruder to exploit a vulnerability with the intent of elevating privileges to gain access to more sensitive systems on the internal network. VLANs may be used to further separate systems by controlling access and providing segregation thus giving additional protection.

Mandates and Requirements

20.1.6. In August 2013, the Government introduced their approach to cloud computing, establishing a 'cloud first' policy and an All-of-Government direction to cloud services development and deployment. This is enabled by the Cabinet Minute [CAB Min (13) 37/6B].

20.1.7. Under the 'cloud first' policy state service agencies are expected to adopt approved cloud services either when faced with new procurements, or an upcoming contract extension decision.

20.1.8. In October 2013 the Government approved the GCIO risk and assurance framework for cloud computing, which agencies must follow when they are considering using cloud services [CAB Min (13) 37/6B]. It also directs that no data classified above RESTRICTED should be held in a *public* cloud, whether it is hosted onshore or offshore.

20.1.9. It is important to note that although agencies can outsource **responsibility** to a service provider for implementing, managing and maintaining security controls, they cannot outsource their **accountability** for ensuring their data is appropriately protected.

Background

20.1.10. The adoption of cloud technologies and services, the hosting of critical data in the cloud and the risk environment requires that agencies exercise caution. Many cloud users are driven by the need for performance, scalability, resource sharing and cost saving so a comprehensive risk assessment is essential in identifying and managing jurisdictional, sovereignty, governance, technical and security risks.

20.1.11. Typically agencies and other organisations start with a small, private cloud, allowing technical and security architectures, management processes and security controls to be developed and tested and gain some familiarity with cloud technologies and processes. These organisations then progress by using non-critical data, for example email, and other similar applications, in a hybrid, private or public cloud environment.

20.1.12. There are a number of technical risks associated with cloud computing, in addition to the existing risks inherent in organisational systems. Attention

must also be paid to the strategic, governance and management risks of cloud computing. Security architecture and security controls also require careful risk assessment and consideration.

20.1.13. Cloud service providers will invariably seek to limit services, liability, compensation or penalties through carefully worded service contracts, which may present particular risks.

20.1.14. Much has been made of the operational cost savings related to cloud technologies, particularly a lower cost of operating. Less obvious are the risks and related cost of managing risk to an acceptable level. It is important to note that short term overall cost increases may, in some cases, be attributed to the adoption of cloud technologies and architectures.

20.1.15. Some valuable work in mapping the cloud risk landscape has been undertaken by such organisations as the Cloud Security Alliance, the US National Institute of Standards and Technology (NIST), the UK's Cloud Industry Forum and the European Network and Information Security Agency (ENISA). It is important to note that the extent of the risk landscape continues to evolve and expand.

Scope

20.1.16. This section provides information and some guidance on the risks associated with cloud computing, its implementation and ongoing use. Some controls are specified but agencies will necessarily undertake their own comprehensive risk assessment and select controls to manage those risks.

References - Guidance

20.1.17. While NOT an exhaustive list, further information on Cloud can be found at:

Reference	Title	Publisher	Source
CAB Min (12) 29/8A	**Cabinet Minute of Decision – CAB Min (12) 29/8A – 'Cloud First' Policy**	Cabinet Office	
CAB Min (13) 37/6B	**Cabinet Minute of Decision – CAB Min (13) 37/6B – Cloud Computing Risk and Assurance Framework**	Cabinet Office	Cabinet minutes for public cloud services | NZ Digital government
	All-of-Government Cloud Services	Government Chief Information Officer	https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/cloud-services/
	Risk Assessment Process: Information Security	Government Chief Information Officer	https://www.digital.govt.nz/dmsdocument/3~Risk-Assessment-Process-Information-Security.pdf [PDF, 282 KB]
	Government Use of Offshore Information and Communication Technologies (ICT) Service Providers – Advice on Risk Management April 2009	State Services Commission	http://ict.govt.nz/assets/ICT-System-Assurance/offshore-ICT-service-providers-april-2009.pdf
	Cloud Computing a Guide to Making the Right Choices – February 2013	Office of the Privacy Commissioner (OPC)	Office of the Privacy Commissioner | Making the right choices in cloud computing - new Privacy Commissioner guidance
	Cloud Computing Security Considerations	ASD	https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-computing-security-considerations
	Cloud Computing Policy and Guidance 2014	Australian Government Information Management Office (AGIMO)	http://www.finance.gov.au/agict//policy-guides-procurement/cloud
	Cloud Control Matrix	CSA	https://cloudsecurityalliance.org/research/cloud-controls-matrix/
	Security Guidance for Critical Areas of Focus in Cloud Computing	CSA	https://cloudsecurityalliance.org/research/guidance/
	Top Threats to Cloud Computing	CSA	https://cloudsecurityalliance.org/research/working-groups/top-threats/
	Governance, Risk Management and Compliance Stack	CSA	http://www.cloudsecurityalliance.org/grcstack.html
	Security & Resilience in Governmental Clouds - Making an informed decision	ENISA	https://www.enisa.europa.eu/publications/security-and-resilience-in-governmental-clouds
	Cloud Computing Information Assurance Framework	ENISA	https://www.enisa.europa.eu/publications/cloud-computing-information-assurance-framework
	Cloud Computing Security Risk Assessment	ENISA	https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment
	Critical Cloud Computing – A CIIP perspective on cloud computing services	ENISA	Critical Cloud Computing-A CIIP perspective on cloud computing services — ENISA (europa.eu)
NIST Special Publication 800-144, December 2011	**Guidelines on Security and Privacy in Public Cloud Computing**	NIST	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf [PDF, 1.08 MB]

	Enterprise Risk Management for Cloud Computing	COSO	Cloud-Computing-Thought-Paper.pdf (coso.org)
	Cloud Security	Cloud Industry Forum	Knowledge Hub - Cloud Industry Forum
	OASIS – various reference and guidance documents	OASIS	https://www.oasis-open.org/committees/tc_cat.php?cat=cloud

References - Standards

20.1.18. Further standards can be found at:

Reference	Title	Publisher	Source
NIST Special Publication 800-145, September 2011	**The NIST Definition of Cloud Computing**	NIST	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf [PDF, 84 KB]
NIST Special Publication 800-146, May 2012	**Cloud Computing Synopsis and Recommendations**	NIST	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf [PDF, 1.44 MB]
NIST Special Publication 500-291, version 2, July 2013	**Cloud Computing Standards Roadmap**	NIST	http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf [PDF, 2.19 MB]
NIST Special Publication 500-292, September 2011	**Cloud Computing Reference Architecture**	NIST	http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505 [PDF, 1.42 MB]
ISO/IEC 17788:2014	**Information technology -- Cloud computing -- Overview and vocabulary**	ISO	https://www.iso.org/standard/60544.html
ISO/IEC 17789:2014	**Information technology -- Cloud computing -- Reference architecture**	ISO	https://www.iso.org/standard/60545.html
ISO/IEC 17826:2012	**Information technology -- Cloud Data Management Interface (CDMI)**	ISO	https://www.iso.org/standard/60617.html
ISO/IEC CD 19086-1:2016	**Information technology -- Cloud computing -- Service level agreement (SLA) framework and Technology -- Part 1: Overview and concepts**	ISO	https://www.iso.org/standard/67545.html
ISO/IEC NP 19086-2:2018	**Information technology -- Cloud computing -- Service level agreement (SLA) framework and Technology -- Part 2: Metrics**	ISO	https://www.iso.org/standard/67546.html
ISO/IEC NP 19086-3:2017	**Information technology -- Cloud computing -- Service level agreement (SLA) framework and Technology -- Part 3: Core requirements**	ISO	https://www.iso.org/standard/67547.html
ISO/IEC AWI 19941:2017	**Information Technology -- Cloud Computing -- Interoperability and Portability**	ISO	https://www.iso.org/standard/66639.html
ISO/IEC AWI 19944-1:2020	**Information Technology - Cloud Computing - Data and their Flow across Devices and Cloud Services**	ISO	https://www.iso.org/standard/79573.html

ISO/IEC DIS 27017:2015	**(In Draft) Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services**	ISO	https://www.iso.org/standard/43757.html
ISO/IEC 27018:2019	**Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors**	ISO	https://www.iso.org/standard/76559.html

PSR references

20.1.19. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV2, GOV5, GOV6, INFOSEC1, INFOSEC2, INFOSEC3 and INFOSEC4	Home | Protective Security Requirements Security governance (GOV) | Protective Security Requirements Information security (INFOSEC) | Protective Security Requirements

Rationale & Controls

Applicability

20.1.20.R.01. **Rationale**

Security controls may not be available, cost effective or appropriate for all information classification levels. Much will depend on the cloud computing deployment model adopted. It is important that agencies understand when it is appropriate to use cloud services and how to select appropriate cloud services and service models, based on the classification of the information, any special handling endorsements and associated confidentiality, availability and integrity risks.

20.1.20.R.02. **Rationale**

Systems and information classified CONFIDENTIAL and above require higher levels of protection. This applies in all types of cloud models including private, community, hybrid, and public cloud models and deployments.

20.1.20.C.01. **Control System Classifications(s): Top Secret, Secret, Confidential; Compliance: Must** [CID:4800]

The use of cloud services and infrastructures for systems and data classified CONFIDENTIAL, SECRET or TOP SECRET MUST be approved by the GCSB.

20.1.20.C.02. **Control System Classifications(s): Top Secret, Confidential, Secret; Compliance: Must** [CID:4801]

Agencies intending to adopt cloud technologies or services MUST ensure cloud service providers apply the controls specified in this manual to any systems hosting, processing or storing agency data and systems.

20.1.20.C.03. **Control System Classifications(s): Confidential, Secret, Top Secret; Compliance: Must Not** [CID:4802]

Agencies MUST NOT use public, hybrid (incorporating a public element), or other external cloud services for systems and data classified CONFIDENTIAL, SECRET or TOP SECRET.

20.1.20.C.04. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:4803]

Agencies MUST NOT use public or hybrid (incorporating a public element) cloud services to host, process, store or transmit NZEO endorsed information.

20.1.20.C.05. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4804]

Agencies intending to adopt cloud technologies or services SHOULD obtain formal assurance cloud service providers will apply the controls specified in this manual to any cloud service hosting, processing or storing agency data and systems.

Risk Assessment

20.1.21.R.01. **Rationale**

The adoption of cloud technologies will introduce a wide range of technology and information system risks *in addition* to the risks that already exist for agency systems. It is vital that these additional risks are identified and assessed in order to select appropriate controls and countermeasures. Trust boundaries must be defined to assist in determining effective controls and where these controls can best be applied.

20.1.21.R.02. **Rationale**

The **responsibility** for the implementation, management and maintenance of controls will depend on the service model and deployment model (refer to NIST SP800-145) used in the delivery of cloud services.

20.1.21.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4808]

Agencies intending to adopt cloud technologies or services MUST conduct a risk assessment *before* implementation or adoption.

20.1.21.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4809]

Agencies intending to adopt cloud technologies or services MUST determine trust boundaries *before* implementation.

20.1.21.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4810]

Agencies intending to adopt cloud technologies or services MUST determine where the responsibility (agency or cloud service provider) for implementing, managing and maintaining controls lies in accordance with agreed trust boundaries.

20.1.21.C.04. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4811]

Agencies MUST ensure cloud risks for any cloud service adopted are understood and formally accepted by the Agency Head or Chief Executive (or their formal delegate) and the agency's Accreditation Authority.

20.1.21.C.05. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4812]

Agencies MUST consult with the GCDO to ensure the strategic and other cloud risks are comprehensively assessed.

20.1.21.C.06. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4813]

Agencies procuring or using cloud services to be used by multiple agencies MUST ensure all interested parties formally agree the risks, controls and any residual risks of such cloud services.

20.1.21.C.07. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4814]

Agencies using cloud services MUST ensure they have conducted a documented risk assessment, accepted any residual risks, and followed the endorsement procedure required by the GCDO.

Offshore Services

20.1.22.R.01. **Rationale**

Cloud services hosted offshore introduce several additional risks, in particular, jurisdictional, sovereignty and privacy risks. Foreign owned cloud service providers operating in New Zealand, are subject to New Zealand legislation and regulation. They may, however, also be subject to a foreign government's privacy, lawful access and data intercept legislation.

20.1.22.R.02. **Rationale**

The majority of these jurisdictional, sovereignty and privacy risks cannot be adequately managed with controls available today. They must therefore be carefully considered and accepted by the Agency Head or Chief Executive before the adoption of such cloud services.

20.1.22.R.03. **Rationale**

Some cloud services hosted within New Zealand may be supported by foreign based technical staff. This characteristic introduces a further risk element to the use of foreign-owned cloud service providers.

20.1.22.R.04. **Rationale**

Further complexity can be introduced when All-of-Government or multi-agency systems are deployed or integrated with cloud services. Any security breach can affect several agencies and compromise large or aggregated data sets.

20.1.22.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4820]

Agencies using cloud services hosted offshore MUST ensure jurisdictional, sovereignty and privacy risks are fully considered and formally accepted

by the Agency Head or Chief Executive and the agency's Accreditation Authority.

20.1.22.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4821]

Agencies using cloud services hosted offshore MUST ensure that the agency retains ownership of its information in any contract with the cloud service provider.

20.1.22.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4822]

Agencies using cloud services hosted offshore and connected to All-of-Government systems MUST ensure they have conducted a risk assessment, accepted any residual risks, and followed the endorsement procedure required by the GCDO.

20.1.22.C.04. **Control System Classifications(s): Confidential, Top Secret, Secret; Compliance: Must Not** [CID:4823]

Agencies MUST NOT use cloud services hosted offshore for information or systems classified CONFIDENTIAL, SECRET or TOP SECRET.

20.1.22.C.05. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:4824]

Agencies MUST NOT use cloud services hosted offshore for information with an NZEO endorsement.

20.1.22.C.06. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:4825]

Agencies SHOULD NOT use cloud services hosted offshore *unless*:

- privacy, information sensitivity and information value has been fully assessed by the agency;
- a comprehensive risk assessment is undertaken by the agency;
- controls to manage identified risks have been specified by the agency; and
- the cloud service provider is able to provide adequate assurance that these controls have been properly implemented *before* the agency uses the cloud service.

System Availability

20.1.23.R.01. **Rationale**

The availability of agency systems, business functionality and any customer or client online services, is subject to additional risks in an outsourced cloud environment. A risk assessment will include consideration of business requirements on availability in a cloud environment.

20.1.23.R.02. **Rationale**

Risks to business functionality may include service outages, such as communications, data centre power, backup and other failures or interruptions. Entity failures such the merger, acquisition or liquidation of the cloud service provider may also present a significant business risk to availability.

20.1.23.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4829]

Agencies intending to adopt cloud technologies or services MUST consider the risks to the availability of systems and information in their design of cloud systems architectures and supporting controls and governance processes.

20.1.23.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4830]

Any contracts for the provision of cloud services MUST include service level, availability, recoverability and restoration provisions.

20.1.23.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4831]

Agencies MUST ensure contracts with cloud service providers include provisions to manage risks associated with the merger, acquisition, liquidation or bankruptcy of the service provider and any subsequent termination of cloud services.

Unauthorised Access

20.1.24.R.01. **Rationale**

Cloud service providers may not provide adequate physical security and physical and logical access controls to meet agencies requirements. An assessment of cloud service risks will include physical and systems security. Refer also to Chapter 19 – Gateway Security, Section 22.2 – Virtualisation and Section 22.3 – Virtual Local Area Networks.

20.1.24.R.02. **Rationale**

Some cloud services hosted within New Zealand may be supported by technical staff, presenting additional risk. In some cases the technical staff are based offshore. The use of encryption can provide additional assurance against unauthorised access – refer to Chapter 17 – Cryptography.

20.1.24.R.03.

Rationale

Data Loss Prevention (DLP) technologies and techniques are implemented to safeguard sensitive or critical information from leaving the organisation. They operate by identifying unauthorised access and data exfiltration and take remedial action by monitoring, detecting and blocking unauthorised attempts to exfiltrate data. For DLP to be effective, all data states (processing, transmission and storage) are monitored.

20.1.24.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4836]

Agencies intending to adopt cloud technologies or services SHOULD ensure cloud service providers apply the physical, virtual and access controls specified in this manual for agency systems and data protection.

20.1.24.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4837]

Agencies intending to adopt cloud technologies or services SHOULD apply separation and access controls to protect data and systems where support is provided by offshore technical staff.

20.1.24.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4838]

Agencies intending to adopt cloud technologies or services SHOULD apply controls to detect and prevent unauthorised data transfers and multiple or large scale data transfers to offshore locations and entities.

20.1.24.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4839]

Agencies intending to adopt cloud technologies or services SHOULD consider the use of encryption for data in transit and at rest.

Incident Handling and Management

20.1.25.R.01. **Rationale**

Cloud service providers may not provide the same level of incident identification and management as provided by agencies. In some cases, these services will attract additional costs. Careful management of contracts is required to ensure agency requirements for incident detection and management are fully met when adopting cloud services.

20.1.25.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4842]

Agencies MUST include incident handling and management services in contracts with cloud service providers.

20.1.25.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4843]

Agencies MUST develop and implement incident identification and management processes in accordance with this manual (See Chapter 6 – Information Security Monitoring, Chapter 7 – Information Security Incidents, Chapter 9 – Personnel Security and Chapter 16 – Access Control).

Backup, Recovery Archiving and Data Remanence

20.1.26.R.01. **Rationale**

Cloud service providers will invariably provide some business continuity and disaster recovery plans, including system and data backup, for their own operational purposes. These plans may not include customer data or systems. Where cloud service providers do not adequately meet agency business requirements, an agency defined backup and recovery plan may be necessary.

20.1.26.R.02. **Rationale**

Residual information remaining on a device or storage media after clearing or sanitising the device or media is described as data remanence. This characteristic is sometimes also described as data persistence, although this description may include the wider implication of multiple copies.

20.1.26.R.03. **Rationale**

Full consideration of risks associated with data remanence and data persistence is required to ensure agency requirements for backup, recovery, archiving and data management is included in any cloud service contract.

20.1.26.R.04. **Rationale**

In addition to backups, cloud service providers may also archive data. Multi-national or foreign based cloud service providers may have established data centres in several countries. Backup and archiving is invariably automated and there may be no feasible method of determining where and in what jurisdiction the data have been archived. This can create an issue of data remanence and persistence where cloud service contracts are terminated but not all agency data can be effectively purged or deleted from the provider's systems.

20.1.26.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4849]

Agencies MUST develop and implement a backup, recovery and archiving plan and supporting procedures (See Section 6.4 – Business Continuity and

Disaster Recovery).

20.1.26.C.02. **Control System Classifications(s): All Classifications; Compliance: Must [CID:4850]**

Agencies MUST include a data purge or secure delete process in any cloud service contracts.

20.1.26.C.03. **Control System Classifications(s): All Classifications; Compliance: Must [CID:4851]**

Any data purge or secure delete process in any cloud service contracts MUST be independently verifiable.

User Awareness and Training

20.1.27.R.01. **Rationale**

The introduction of cloud services will introduce change to the appearance and functionality of systems, how users access agency systems and types of user support. It is essential that users are aware of information security and privacy concepts and risks associated with the services they use.

Support provided by the cloud service provider may attract additional charges.

20.1.27.C.01. **Control System Classifications(s): All Classifications; Compliance: Must [CID:4854]**

Agencies MUST develop and implement user awareness and training programmes to support and enable safe use of cloud services (See Section 9.1 – Information Security Awareness and Training).