23.2. Governance, Risk Assessment & Assurance

Objective

23.2.1. Agency cloud initiatives follow the risk management, assurance, governance, and control requirements in this manual.

Context

Scope

23.2.2. Good governance is required to ensure appropriate mechanisms and lines of accountability are in place to understand, assess, document, and manage cloud risks. This section describes the requirements for agencies to identify, respond to, and manage risks relevant to public cloud services.

23.2.3. Reference to other chapters and sections in this document is essential. In particular:

- Section 2.3 – Using cloud services
- Chapter 3 – Information security governance – roles and responsibilities
- Chapter 4 – System certification and accreditation
- Chapter 5 – Information security documentation
- Section 5.8 – Independent assurance reports
- Chapter 6 – Information security monitoring
- Chapter 7 – Information security incidents
- Chapter 9 – Personnel security
- Chapter 16 – Access control and passwords
- Chapter 17 – Cryptography

Public cloud services

23.2.4. Cloud computing affects governance, since it either:

- introduces a third party into the process (as in the case of public cloud or hosted private cloud); or
- potentially alters internal governance structures (as in the case of self-hosted private cloud).

23.2.5. The primary issue to remember when governing cloud computing is that an organisation can never outsource responsibility for governance, even when using external providers. This is always true, cloud or not, but is useful to keep in mind when navigating cloud computing's concept of shared responsibility.

23.2.6. As with any outsourcing arrangement, agencies bear ultimate responsibility for identifying and managing these risks even if they rely on their cloud service provider to implement mitigating controls.

23.2.7. Cloud services that are hosted or managed from outside New Zealand pose jurisdictional, data sovereignty, and privacy risks. Even when the service is hosted in New Zealand and subject to New Zealand law, an overseas provider may also be subject to its home country's privacy, data access, and lawful intercept legislation, which may conflict with New Zealand law.

23.2.8. Cloud services that support multiple agencies or All-of-Government capabilities also pose governance and risk management challenges that must be addressed by establishing privacy, security, and compliance policies in order to protect the corporate assets and intellectual property of participating organisations' data.

Obligations and responsibilities

23.2.9. Agencies must be aware of their statutory and regulatory obligations to protect Official, Classified and personal information and data. Any move to using cloud services cannot allow compromise of these statutory obligations.

Cloud contracts

23.2.10. Cloud contracts should consider data stewardship, data sovereignty, jurisdiction, storage and access, including any backups. It remains, however,

the responsibility of individual agencies to ensure their legislative and regulatory responsibilities for data stewardship are met.

23.2.11. As with any outsourcing arrangement, use of cloud services carries the risk of the provider going out of business or otherwise being unable to provide contracted services to the consuming agency. This is a commercial risk that technical security controls cannot address, but one agencies need to consider as part of their due diligence.

23.2.12. It is essential that appropriate legal advice is taken before any cloud contracts are finalised.

Regular assurance checks

23.2.13. Changes made to a cloud tenancy may have an adverse impact on the security posture of an agency's cloud service configuration. Usually, in such circumstances (e.g., if the change was initiated by the agency on-site) this may trigger the commencement of the certification and accreditation process. In addition, changes would usually be subject to approval, review, and testing, as part of an agency's IT change control process. However, this may not be the case in a cloud environment, as platform changes are made by the cloud service provider and may occur with minimal or no notice (see section 5.8 – Independent assurance reports).

References

23.2.14. Further references can be found at:

Reference	Title	Publisher	Source
	Cloud computing security for tenants	Australian Cyber Security Centre (ACSC)	Cloud Computing Security for Tenants | Cyber.gov.au
	CCMv4.0 auditing guidelines	CSA	CCMv4.0 Auditing Guidelines | CSA (cloudsecurityalliance.org)
	CSA Security Guidance for Critical Areas of Focus in Cloud Computing	CSA	CSA Security Guidance for Cloud Computing | CSA (cloudsecurityalliance.org)
	Cloud computing — information security and privacy considerations	Digital.govt.nz	Cloud computing information security and privacy considerations | NZ Digital government
	About public cloud services	Digital.govt.nz	About public cloud services | NZ Digital government
	Secure cloud strategy	Australian Government	Secure Cloud Strategy | Digital Transformation Agency (dta.gov.au)
NIST SP 500-291 (2011)	NIST cloud computing standards roadmap	NIST	NIST-SP 500-291, NIST Cloud Computing Standards Roadmap | NIST

PSR References

23.2.15. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR mandatory requirements	GOV2 - Take a risk-based approach GOV5 - Manage risks when working with others GOV6 - Manage security incidents INFOSEC1 - Understand what you need to protect INFOSEC2 - Design your information security INFOSEC3 - Validate your security measures INFOSEC4 - Keep your security up to date	Mandatory requirements | Protective Security Requirements
PSR protocol for information security	Management protocol for information security	Management protocol for information security | Protective Security Requirements

Rationale & Controls

Understanding levels of assurance for public cloud

23.2.16.R.01.

Rationale

Although roles and responsibilities for public cloud services may be shared between an agency and the cloud service provider, ultimately an agency owns security risks and is responsible for all ICT services their agency consumes, including public cloud services.

23.2.16.R.02. **Rationale**

It is an agency's responsibility to ensure that cloud service providers have adequate safeguards in place to address security risks specific to their public cloud instance.

23.2.16.R.03. **Rationale**

Adoption of public cloud services introduce risks to agency systems that need to be identified, assessed, and formally accepted in order to understand the appropriate use of public cloud services and select effective controls and countermeasures.

23.2.16.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7386]

Agencies MUST update their risk assessment process to account for public cloud specific risks, prior to implementation or adoption of public cloud services.

23.2.16.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7387]

Agencies MUST undertake a cloud specific risk assessment in line with the process outlined by the GCDO for each public cloud service, prior to implementation or adoption of public cloud services.

23.2.16.C.03. **Control System Classifications(s): Secret, Top Secret, Confidential; Compliance: Must Not** [CID:7388]

Agencies MUST NOT accredit public cloud services for use with data classified CONFIDENTIAL, SECRET, or TOP SECRET.

23.2.16.C.04. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:7389]

Agencies MUST NOT accredit public cloud services to host, process, store, or transmit NZEO endorsed information.

System availability

23.2.17.R.01. **Rationale**

It is important that connectivity between an organisation and their cloud service providers meets requirements for latency and reliability. In support of this, an organisation and their cloud service providers should discuss any specific network requirements, performance characteristics, or planned responses to availability failures, especially when high-availability requirements exist.

23.2.17.R.02. **Rationale**

An organisation and their cloud service providers should discuss whether dedicated communication links or connections over the internet will be used and whether any secondary communications links will provide sufficient capacity to meet operational requirements should the primary communication link become unavailable.

23.2.17.R.03. **Rationale**

Feedback should be provided to cloud service providers when performance does not meet service level agreement targets. To assist with this, anomaly detection can be performed through network telemetry that is integrated into security monitoring tools.

23.2.17.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7394]

Agencies MUST consider risks to the availability of systems and information in their design of cloud systems architectures, supporting controls, and governance processes prior to implementation or adoption of public cloud services.

Regular assurance checks

23.2.18.R.01. **Rationale**

Cloud service providers should conduct independent assurance activities as part of their due diligence and to provide customers with evidence of quality service provision and compliance. It is important that such assurance activities are undertaken by an assessor with the appropriate expertise to validate the existence and performance of security controls.

23.2.18.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7397]

Agencies SHOULD obtain regular assurance checks on cloud service providers, ensuring they have been undertaken by a suitably qualified assessor.

Cloud service providers – patching and software maintenance

23.2.19.R.01. **Rationale**

Data transmitted, stored, and processed off site presents a risk to an organisation. This includes reliance on a cloud service provider to not only identify software vulnerabilities, but to apply these in a timely manner, as well providing evidence to an agency of this.

23.2.19.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7400]

Agencies MUST obtain assurance that cloud service providers undertake appropriate software and operating system patching and maintenance.

Assurance around workload isolation on shared infrastructure

23.2.20.R.01. **Rationale**

Responsibilities for workload isolation in public cloud are shared between the cloud provider and consumer. Workload isolation in a public cloud security context ensures compute processes or memory in one virtual machine/container are not visible to another tenant, even when they are running processes on the same physical hardware.

23.2.20.R.02. **Rationale**

To mitigate the risk of unauthorised access between resources in separate tenancies, it is important that adequately architected security controls are built into the design. Examples of adequate security controls include zero touch configuration and separation of administrative control interfaces.

23.2.20.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7404]

Agencies MUST obtain assurance that technical protections exist to adequately isolate tenants.

Use of baseline security templates

23.2.21.R.01. **Rationale**

GCSB endorsed NZISM baseline security templates are intended to assist agencies in understanding the security posture of their cloud environments. They provide a baseline level of security within a cloud environment to significantly reduce agency's assurance activities and focus then on moving towards continuous security posture assessments.

23.2.21.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7407]

Agencies SHOULD make use of the GCSB endorsed baseline security templates where applicable.