23.4. Data Protection in Public Cloud

Objective

23.4.1. Data is protected throughout its lifecycle on public cloud platforms.

Context

Scope

23.4.2. This section provides information on keeping data in a public cloud environment secure from creation to destruction, whether at rest, in-transit, during processing, or when it is no longer required.

23.4.3. Key considerations for keeping agency data secure in public cloud are that data is stored and processed on systems that:

- Are not under direct agency control.
- Are designed to be potentially accessible from anywhere.
- Can be accessed by multiple end-point devices.
- May replicate the data to multiple locations.

23.4.4. Where these systems are located outside New Zealand, or a New Zealand-based service is provided by an entity subject to another country's laws, there may be additional jurisdictional risks to privacy and sovereignty to consider.

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

- Section 6.4 – Business continuity and disaster recovery
- Section 13.1– System decommissioning
- Chapter 17 – Cryptography
- Chapter 18 – Network security
- Chapter 20 – Data management
- Chapter 21 – Distributed working
- Chapter 23.2 - Public cloud services - Governance, risk assessment and assurance

Data accessibility

23.4.6. Public cloud services are often promoted for their ability to make organisations' data assets more accessible, both within the organisation and to partners or customers. This benefit also brings risks such as default accessibility from the internet and requires agencies to carefully manage access to data.

References

23.4.7. Further references can be found at:

Reference	Title	Publisher	Source
	Cloud security technical reference architecture	CISA	Cloud Security Technical Reference Architecture | CISA
ISO 27001:2013	Information technology — Security techniques — Information security management systems — Requirements	ISO	ISO - ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements
NIST SP 800-144 (2011)	Guidelines on security and privacy in public cloud computing	NIST	Guidelines on Security and Privacy in Public Cloud Computing | NIST

PSR References

23.4.8. 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

Data protection mechanisms

23.4.9.R.01. **Rationale**

Agencies remain accountable for the confidentiality, integrity, and availability of their data, even though cloud service providers may define and implement the mechanisms used to protect their data in the cloud environment.

23.4.9.R.02. **Rationale**

The mechanisms available for agency control and management of keys in a public cloud environment are often tied to a specific cloud environment and migrating data to a new environment may require decryption and re-encryption.

23.4.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7461]

For each cloud service, agencies MUST ensure that the mechanisms used to protect data meet agency requirements.

23.4.9.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7462]

Agencies MUST update key management plans to account for differences in public cloud before storing organisational data in a public cloud environment.

23.4.9.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7463]

Agencies MUST ensure their key management plan includes provision for migrating data from the cloud environment where it was created.

Data accessibility

23.4.10.R.01. **Rationale**

Many public cloud services are designed to make customer data directly accessible through multiple interfaces. These service endpoints may be internet-accessible by default, and will have specific mechanisms that restrict access to authorised parties. Failure to consider these endpoints or to control their default accessibility risks exposure of agency information to unauthorised parties.

23.4.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7466]

Agencies MUST apply the principle of least privilege and configure service endpoints to restrict access to authorised parties.

Data location

23.4.11.R.01. **Rationale**

The geographic locations where public cloud data is stored may have security or privacy implications for agencies. These locations may be in jurisdictions with differing laws from New Zealand or be subject to particular environmental risks that agencies have not previously had to consider. While these factors do not of themselves prevent placing agency data in such locations, agencies have a responsibility to fully understand where their data is stored or processed and to manage any resulting risks appropriately.

23.4.11.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7469]

Agencies MUST identify where data used in conjunction with a public cloud service is stored or processed, including any replicas or backups that may be created.

23.4.11.C.02.

Control System Classifications(s): All Classifications; Compliance: Must [CID:7470]

Agency risk assessments of public cloud services MUST include any risks arising from data location. Any actions required to mitigate these risks must be identified and documented prior to implementation or adoption of public cloud services.

Revise disaster recovery plans to include data in public cloud

23.4.12.R.01. **Rationale**

As specified in Section 6.4, Business continuity and disaster recovery, agencies must plan for recovery from loss of data to ensure they can continue to operate. Public cloud services can provide alternative mechanisms to back up and restore data from those used on premises. Recovery processes and plans may need to be updated to account for these differences to avoid agencies finding their ability to recover from data loss is compromised.

23.4.12.R.02. **Rationale**

As well as protecting data stored natively in public cloud services, agencies may choose to back up on-premises data to the cloud or vice versa. The same considerations and opportunities for new approaches apply in all these cases.

23.4.12.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7474]

Agencies MUST update their disaster recovery plans prior to storing or replicating data in public cloud services, to ensure these plans address any cloud-specific aspects of backup and recovery.

23.4.12.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7475]

When planning tests of disaster recovery processes in accordance with 6.4.6 Backup strategy, agencies MUST include tests of any cloud-specific data recovery processes.

Data retrieval and removal

23.4.13.R.01. **Rationale**

It is important to consider what would be involved in leaving or changing the provider of a public cloud service. Planning for ending the use of a cloud service should be done before commissioning and deployment of data into the cloud.

23.4.13.R.02. **Rationale**

Terminating cloud service contracts can have undesired consequences and risks for an agency if a managed process is not followed, for example:

- All or some agency data being retained on the cloud platform by the provider.
- Agency data being removed prior to being retrieved by the agency.
- Agency data being replicated to other jurisdictions before or after decommissioning.

23.4.13.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7511]

Agencies MUST have a defined exit strategy for each public cloud service they consume, including a process by which their data can be retrieved and erased from the cloud service as part of contract termination.

23.4.13.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7512]

Agencies MUST ensure all data they need to retain is retrieved from the cloud service provider prior to decommissioning.

23.4.13.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7513]

Agencies MUST have assurance that no agency-owned data is retained on the cloud service being decommissioned.