2.3. Using Cloud Services

Objective

2.3.1. Agencies understand and manage their cloud services to ensure they are secure, effective and efficient.

Context

Scope

2.3.2. This section provides guidance on agency responsibilities when using cloud services.

2.3.3. It is important that agencies understand their responsibilities with respect to the use of cloud services. Agency official and classified information, regardless of the system that it is held in (including cloud services), is still required to be protected in accordance with Cabinet directives, the Protective Security Requirements (PSR), the NZISM, the New Zealand Government Security Classification System and with other government security requirements and guidance

2.3.4. Reference should also be made to the following sections in the NZISM:

- Chapter 4 – System Certification and Accreditation
- Chapter 5 – Information Security Documentation
- Chapter 13 – Decommissioning and Disposal
- Chapter 16 – Access Control
- Chapter 17 – Cryptography
- Chapter 19 – Gateway Security
- Chapter 20 – Data Management
- Chapter 22 – Enterprise Systems Security

2.3.5. Detailed controls for Cloud Computing are provided in Section 22.1 – Cloud Computing. Detailed controls for Public Cloud services are provided in Chapter 23 - Public Cloud Security.

Mandates, Directives and Requirements

2.3.6. In 2012, Cabinet directed government agencies to adopt public cloud services in preference to traditional IT systems. Offshore-hosted office productivity services were excluded **[CAB Min (12) 29/8A]**

2.3.7. 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]**. Under the 'cloud first' policy state service agencies are expected to adopt approved cloud services either when faced with new procurements, or a contract extension decision.

2.3.8. Cabinet also incorporated the cloud risk assessment process into the system-wide ICT assurance framework **[CAB Min (13) 20/13]**.

2.3.9. The New Zealand Government ICT Strategy released in October 2015 requires agencies to outsource their IT functions using common capabilities and public cloud services where this was feasible and practical.

2.3.10. In 2014 The Government Chief Information Officer published Cloud Computing Information Security and Privacy Considerations. This guidance is designed to assist agencies systematically identify, analyse, and evaluate information security and privacy risks related to individual public cloud services.

2.3.11. In July 2016, new measures were confirmed to accelerate the adoption of public cloud services by New Zealand's government agencies. The new measures complement existing policies and risk assessment processes and provide appropriate checks and balances.

Background

2.3.12. 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, assurance, technical and security risks.

2.3.13. Security requirements and drivers in the cloud differ significantly from traditional data centre environments requiring new security models and architectures. Key factors include:

- The dynamic nature of the cloud and its related infrastructure;
- No customer ownership or control of infrastructure;
- Limited visibility of architectures and transparency of operations;
- Shared (multi-tenanted) physical and virtual environments; and
- May require re-architecting of agency system to optimise use of cloud services.

2.3.14. While there is potential for significant benefit, flexibility and cost saving, any use of cloud services carries risk. All cloud computing decisions should be made on a case-by-case basis after a proper risk assessment, the agency technology architecture is developed and security is properly considered and incorporated.

2.3.15. There is also likely to be a significant mismatch in service-level agreements (SLAs) between existing systems and outsourcing arrangements and those of cloud-based services.

2.3.16. It is important to note that although agencies can outsource operational **responsibilities** to a service provider for implementing, managing and maintaining security controls, they cannot outsource their **accountability** for ensuring their data is appropriately protected, including any system or service decommissioning or termination.

2.3.17. The Government Chief Digital Officer (GCDO) has developed a risk and assurance framework for cloud computing, which agencies are required to follow when they are considering using cloud services.

Information Security and Zero Trust

2.3.18. Information security relates to the protection of information regardless of its form (electronic or physical). Within government, information security has traditionally been construed using the concepts of confidentiality, availability and integrity of information.

2.3.19. Relating these concepts to people who access, manage and use that information requires the use of methods to provide:

- Authentication;
- Authorisation; and
- Non-repudiation.

2.3.20. With the growth of the internet and cloud services, the proliferation of data and the growth in malicious and cyber-criminal activities, older methods of enabling information security are “fragile”, can be fragmented, and are in some cases, ineffective.

2.3.21. Zero Trust is a security concept based around the idea that systems and users should not be given access to any information without verification, even when they are connected to internal networks. Zero Trust looks to acknowledge that the previous concept and approach of using perimeter defences and providing free access within the secure perimeter is no longer practical or appropriate for securing information assets. As such, it should be replaced with robust authentication and verification steps being continuously performed.

2.3.22. The concept of Zero Trust provides a more complete means of providing information security in an internet and cloud environment. Understanding, planning for and preparing to adopt cloud services is an ideal time to incorporate Zero Trust concepts and principles into an agency’s information security policies, operations and information handling, processing storage and disposal.

References

2.3.23. Additional guidance on cloud services can be found at:

Reference	Title	Publisher	Source
CAB Min (12) 29/8A	**Managing The Government's Adoption of Cloud Computing**	Cabinet Office	Managing the Government's adoption of cloud computing | NZ Digital government
CAB Min (13) 20/13	**Improving Government Information and Communications Technology Assurance**	Cabinet Office	Cabinet Minute: Improving Government Information and Communications Technology (digital.govt.nz)
	Zero Trust Maturity Model	CISA (Cybersecurity and Infrastructure Security Agency) Cybersecurity Division	Zero Trust Maturity Model | CISA
	Cloud Computing – Information Security and Privacy Considerations April 2014	DIA	https://digital.govt.nz/assets/Documents/1Cloud-Computing-Information-Security-and-Privacy-Considerations-FINAL2.pdf [PDF, 185 KB]
	Strategy for a Digital Public Service	DIA	https://digital.govt.nz/digital-government/strategy/strategy-summary/
	Accelerating the Adoption of Public Cloud Services	DIA	https://digital.govt.nz/dmsdocument/15-accelerating-the-adoption-of-public-cloud-services/html
	Cloud Risk Assessment Tool [Excel Spreadsheet]	DIA	Risk assessment tool for public cloud services | NZ Digital government
	Risk Assessment Process	DIA	Assess the risks of using a public cloud service | NZ Digital government
	Build Security Into Your Network's DNA: The Zero Trust Network Architecture by John Kindervag	Forrester	https://virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf [PDF 1.06 MB]
	Zero Trust Architectures and Solutions	Gartner	https://gartner.com/teamsiteanalytics/servePDF?g=/imagesrv/media-products/pdf/Qi-An-Xin/Qi-An-Xin-1-1OKONUN2.pdf
NIST SP800-207	**Zero Trust Architecture**	NIST	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf [PDF, 944 KB]
	Developing a Framework to improve Critical Infrastructure Cybersecurity	NIST	https://nist.gov/system/files/documents/2017/06/05/040813_forrester_research.pdf [PDF, 430 KB]
	Implementing a Zero Trust Architecture	NIST/NCCoE	https://nccoe.nist.gov/projects/implementing-zero-trust-architecture

	Embracing a Zero Trust Security Model	NSA	https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF [PDF, 643 KB]
	Evolving Zero Trust – Microsoft Position Paper	Microsoft	https://microsoft.com/en-nz/security/business/zero-trust

PSR References

2.3.24. Additional information on third party providers is provided in the PSR.

Reference	Title	Source
PSR Mandatory Requirements	GOV4, GOV5, INFOSEC1, INFOSEC2, PERSEC1, PERSEC2, PERSEC3 and PERSEC4	Home | Protective Security Requirements Security governance (GOV) | Protective Security Requirements Information security (INFOSEC) | Protective Security Requirements Personnel security (PERSEC) | Protective Security Requirements

Rationale & Controls

Cloud Adoption Strategy

2.3.25.R.01. **Rationale**

Cloud technologies require a different mindset for the delivery of ICT services, as compared to traditional agency-owned IT servers. Increasingly, ICT will be available only in 'as-a-service' delivery models, which may lead to agencies adopting cloud services in an ad-hoc manner unless an overarching strategy is developed and put in place.

2.3.25.R.02. **Rationale**

This will introduce new and different risks, including:

- where information is located;
- where it is able to be accessed from;
- who is able to access information; and
- how ICT services are funded and sustained.

2.3.25.R.03. **Rationale**

Cloud providers are more likely to adopt modern security and development approaches, including agile development techniques (e.g. DevOps), Zero Trust Networking, serverless computing and continuous integration / continuous deployment (CI/CD) pipelines for automation. These approaches are likely to be incompatible with existing ICT processes that focus on legacy delivery models and may present significant challenges to agencies that are not adequately prepared.

2.3.25.R.04. **Rationale**

Developing a strategy that outlines how an agency will look to exploit the opportunities presented by cloud while managing the risks and change required in ICT governance and management processes is essential to the successful adoption of cloud services for agencies.

2.3.25.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7045]

Agencies intending to adopt public cloud technologies or services MUST develop a plan for how they intend to use these services. This plan can be standalone or part of an overarching ICT strategy.

2.3.25.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7046]

An agency's cloud adoption plan SHOULD cover:

- Outcomes and benefits that the adoption of cloud technologies will bring;
- Risks introduced or mitigated through the use of cloud, and the agency's risk tolerance;
- Financial and cost accounting models;
- Shared responsibility models;
- Cloud deployment models;
- Cloud security strategy;
- Resilience and recovery approaches;
- Data recovery on contract termination;

- Cloud exit strategy and other contractual arrangements; and
- A high level description of the foundation services that enable cloud adoption, including:
    - User, device and system identity;
    - Encryption and key management;
    - Information management;
    - Logging and alerting;
    - Incident management;
    - Managing privileged activities; and
    - Cost management.

Zero Trust

2.3.26.R.01. **Rationale**

Zero Trust is becoming the de-facto approach to ICT system security and is recommended by GCSB as the approach agencies should take, particularly as part of the adoption of cloud services.

Zero Trust is a set of principles and outcomes, not an architecture or a solution. You cannot 'buy' Zero Trust.

Zero Trust is compatible with other ICT outcomes, such as improved access to information, increased agility and better security.

Key aspects of Zero Trust focus on:

- Visibility (through telemetry) and analytics of how services are functioning – this comes through as focus on monitoring, event gathering and machine learning based analysis; and
- Automation of service delivery and security actions.

2.3.26.R.02. **Rationale**

Public cloud services are often built following Zero Trust principles, and agencies will find adoption of this approach will lead to more successful security outcomes than trying to recreate legacy perimeter security controls in the cloud.

2.3.26.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7049]

Agencies intending to adopt public cloud technologies or services SHOULD incorporate Zero Trust philosophies and concepts.

2.3.26.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7050]

Agencies SHOULD leverage public cloud environment native security services as part of legacy system migrations, in preference to recreating application architectures that rely on legacy perimeter controls for security.

Risk Assessment

2.3.27.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. The geographic location of agency data should be identified as this may include offshore data centres.

2.3.27.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:255]

Agencies intending to adopt cloud technologies or services MUST conduct a comprehensive risk assessment, in accordance with the guidance provided by the Government Chief Digital Officer (GCDO) before implementation or adoption.

2.3.27.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:256]

Agencies MUST ensure cloud risks for any cloud service adopted are identified, understood and formally accepted by the Agency Head or Chief Executive and the agency's Accreditation Authority.

Security Architecture

2.3.28.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.

2.3.28.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:259]

Agencies intending to adopt cloud services SHOULD review and enhance existing security architectures and systems design to prudently manage the changed risk, technology and security environment in adopting cloud services.

Selection of Services

2.3.29.R.01. **Rationale**

A number of cloud related service, contracts and other arrangements have been negotiated on behalf of the New Zealand Government with a number of cloud service providers. Agencies must consider these services before negotiating individual contracts or supply contract with cloud service providers.

2.3.29.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4935]

Agencies MUST consider the use of any All of Government contracts with cloud service providers before negotiating individual contracts.

System Decommissioning and Contract Termination

2.3.30.R.01. **Rationale**

It is important that agencies understand how and where their data is processed, managed, stored, backed up and archived within the cloud service provider's environment (systems architecture). This may result in multiple copies of agency data in several data centres, possibly also in several countries.

2.3.30.R.02. **Rationale**

When an agency system or service is decommissioned or a service provider's contract terminated, it is important that agencies ensure data is returned to the agency and no copies are retained by the service provider.

2.3.30.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:263]

Agency system architectures and supply arrangements and contracts SHOULD include provision for the safe return of agency data in the event of system or service termination or contract termination.