New Zealand Government

Security Requirements for Offshore Hosted Office Productivity Services Explained

Version: v1.1

19th January 2017

New Zealand Government

Published by the Department of Internal Affairs

www.ict.govt.nz

Document Control

Project ID/Name	Accelerating Adoption of Cloud Programme
Author	Phil Cutforth MBE MSc
Title	Security Requirements for Offshore Hosted Office Productivity Services Explained
DMS/File Reference	SST-3201-16-4722134DA

Document Classification: UNCLASSIFIED

Revision history

Version	Date	Author	Description of changes
0.1	9/8/16	P Cutforth / C Roberts / J Collier / A Stapleton	Initial draft and development from early adopter agencies (NZQA, NZTE, DOC, NIWA) workshops and Cabinet Paper.
0.15	28/11/16	P Cutforth	External review and consultation. Amendments added.
1.0	23/12/16	P Cutforth / C Roberts	Finalised, for publishing approval and signing.
1.1	19/01/17	P Cutforth / C Roberts	Post-release edits and clarifications.

Document Approval

Department of Internal Affairs

Approved as providing guidance in-line with AoG policy.

Name / Role:	James Collier, Government Enterprise Architect, Department of Internal Affairs	
Signature:		Date: 19/1/2017

Government Communications Security Bureau

Approved as addressing the NZ Information Security Manual (NZISM) security requirements identified in Paragraph 43 of CAB-16-MIN-0316.

Name / Role:	Sam Sargeant, Assistant Director, Information Assurance Branch, Government Communications Security Bureau	
Signature:		Date: 19/1/2017

Contact us: Enquiries regarding this document are welcome to;

Government Enterprise Architect
Department of Internal Affairs
147 Lambton Quay
Wellington 6140
New Zealand
Email: gcio@dia.govt.nz

Table of Contents

References

See Appendix 1.

Definitions

Appendix 2 defines specific terms used in this document in order to ensure clarity of purpose, intent, or meaning for this guidance.

Executive Summary

In CAB Min (16) 03/16, '*Cabinet Minute of Decision – Accelerating the Adoption of Public Cloud Services*' [Reference A], Cabinet supported accelerating the adoption of cloud computing within the public sector. Perceptions of the level of difficulty and risk in implementing cloud vary considerably, in both public and private sectors. On the other hand, unsanctioned or non-mainstream uses of cloud are commonplace (often described as shadow IT).

This paper provides guidance on the management of risk and the provision of assurance in the use of cloud office productivity services by agencies (such as Microsoft Office 365 and Google G-Suite / Applications for Businesses). This guidance recognises the need for secure operations and the requirement to follow government strategic and security policies.

It explains the security requirements and appropriate controls for agencies adopting offshore hosted (cloud) office productivity services. The guidance is principally focussed on the security requirements called out in paragraph 43 of Reference A, in order to provide timely assistance to agencies in adopting public cloud office productivity services. These security requirements cover strategy (policies and processes), architecture, encryption, access control, backup, archiving, recovery, incident management, decommissioning, and third-party assurance.

The scope of this paper excludes other risk areas, such as commercial, jurisdiction, sovereignty, or Privacy Act related factors. More comprehensive guidance in respect of requirements for the adoption of public cloud services by agencies will be developed separately.

The intent here is not to replace or supersede existing policies and guidance, but rather to assist agencies in better understanding their obligations under the Cabinet Minute. It also assists agencies to better understand the risk, and the appropriate management and control mechanisms that can be used to derive adequate levels of assurance for risk owners and chief executives.

This discussion covers the Cabinet Minute policy on office productivity, a description of the security requirements themselves with applicable controls and advice on addressing the requirements, and statements on the applicability of the guidance, and how it integrates into an agency's risk management framework and the GCIO cloud assurance framework.

A detailed description of specific control mechanisms that address the security requirements is included in Appendix 4, to assist security, architecture, project delivery and assurance practitioners.

Security Requirements for Offshore Hosted Office Productivity Services Explained

Purpose

1. This guidance is provided by DIA (GCIO) and GCSB to address the security and assurance requirements from CAB Min (16) 03/16, '*Cabinet Minute of Decision – Accelerating the Adoption of Public Cloud Services*' [Reference A – hereinafter referred to as 'the Cabinet Minute']. It describes how the New Zealand Information Security Manual (NZISM) should be applied in the context of off-shore hosted[1] office productivity services when integrated into agency enterprise ICT environments.
2. This guidance focusses on reducing the perceived risk and uncertainty around the use of offshore hosted office productivity services, by providing the basic security requirements needed for agency enterprise environments that support safe use of public cloud services.
3. This guidance will assist agencies to meet their strategic outcomes in an assured manner. It will also assist in implementing effective measures to manage, protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

Applicability

4. This guidance applies to agencies and their commercial service providers that are subject to the NZISM. Other Public Sector agencies and entities are encouraged to consider this guidance as good practice. The NZISM remains the authoritative reference source for government ICT security controls[2].

5. This guidance applies to agency ICT systems and services protecting official information classified at RESTRICTED and below.

6. This guidance describes how the **security requirements** from the Cabinet Minute are to be addressed within the context of the **security controls framework** of the NZISM [Reference B] in support of the New Zealand Protective Security Requirements (PSR) policy [Reference C]. It does not provide an exhaustive taxonomy of requirements covering other risk areas, such as privacy, jurisdiction, sovereignty, legislative and regulatory, intellectual property, financial and commercial[3].

---

1 Includes public cloud delivery models.

2 Note that alignment between this guidance and the NZISM is taking place, though due to approvals and publishing cycles, there will be a lag between sources. In the interim, specific use cases or queries regarding this guidance should be addressed either to GCIO (gcio@dia.govt.nz) or your NCSC Outreach Manager (info@ncsc.govt.nz).

3 The GCIO 'Cloud Information Security and Privacy Considerations' document and associated 'Cloud Risk Assessment Tool' (105 Questions) covers many of these risk areas. Further documents will be developed providing generic guidance for agencies use of public cloud services.

7. The principal audience for this guidance is Public Sector CISOs, ITSMs, security architects and practitioners, as well as government service providers, security risk assessors, assurance practitioners and auditors. It will also be of reference for agency business managers, project and programme teams, other architects, information managers, and web and digital practitioners.

Background

8. In July 2016, Cabinet agreed a programme of work to 'accelerate the adoption of cloud services' within the Public Sector [Reference A] in support of the extant "Cloud First" principle. The Cabinet Minute specifically removed the restriction on the use of offshore hosted office productivity services for data and information systems classified at RESTRICTED and below, provided agencies conform with guidance to be issued from the Department of Internal Affairs (DIA) and the Government Communications Security Bureau (GCSB) prior to the use of such services.

9. This initial guidance refers specifically to the security requirements stated in the Cabinet Minute. This document describes the basic 'hygiene' measures required to ensure the protection of New Zealand Government official information classified up to RESTRICTED [Reference C], and threat and vulnerability profiles of agency enterprise networks are properly examined and adequately addressed.

10. This guidance has been developed by DIA (GCIO) and GCSB based on government, industry and international good practice, as well as experiences from early adopter agencies and suppliers of office productivity services[4].

11. This guidance is intended to provide agencies with an understanding of their obligations in regard to implementing secure offshore hosted office productivity services.

12. It also describes New Zealand Government's expectations of commercial service providers and their services. Service providers are invited to utilise this document to provide assurance statements of the 'control' mechanisms their services provide to meet stated control requirements. This information will support agencies in conducting risk assessments and product selection.

Office Productivity Policy

13. New Zealand government agencies may use offshore hosted office productivity services provided they conform to the security requirements from the Cabinet Minute, and other relevant NZISM controls[5], as detailed in this guidance.

---

[4] Includes National Institute of Water and Atmospheric Research (NIWA), New Zealand Qualifications Authority (NZQA), New Zealand Trade and Enterprise (NZTE), Department of Conservation (DOC), Microsoft New Zealand, and Google.

[5] Such as those identified by a separate agency risk assessment.

14. Office Productivity policy and this guidance supports the intent of the 'Government Use of Offshore Information and Communication Technologies (ICT) Service Providers – Advice on Risk Management' policy [Reference F].

15. Appendix 2 defines key terms used in the Cabinet Minute, as applied in this guidance.

Government Enterprise Architecture (GEA-NZ) Alignment

16. The 'Office Productivity' services stated in the Cabinet Minute[6] are considered consistent with the GEA-NZ Application Services taxonomy (A3.04 Productivity Suite) category [Reference D]:

    a. office applications (word processing, spreadsheets, presentations),
    b. email[7],
    c. collaboration (publishing, file/database storage, desktop instant messaging, desktop conferencing[8]), and
    d. web browser (A3.02.11).

17. Although useful as a guide for providing assurance over and auditing inter-system connectivity, this guidance does not cover:

    a. any collaboration functionality in other tools, such as development toolsets and social networking,
    b. data exchange across agency networks, line of business systems, or organisational boundaries (where data does not leave those agency's enterprise boundaries),
    c. agency staff or external agents accessing services/databases from another agency for collaboration purposes (where appropriate user access and data leakage/loss protection (DLP) controls are already implemented), and
    d. the AoG ICT Common Capability (ICT-CC) portfolio and shared agency services that are considered government private/community cloud services[9].

---

6 Reference A, Paragraph 48 states: "email, word processing, spreadsheets, presentations, and collaboration tools and services (such as shared workspaces and video conferencing)".

7 Separate guidance will be produced to address Email as its own subject, though the controls in this document still apply.

8 Refer also to NZISM Sect 19.5 covering VoIP and Unified Communications (UC), and NZISM Glossary of Terms.

9 These are separately certified for RESTRICTED use. Though AoG ICT-CC service providers should consider the controls in this guidance as good practice and be able to demonstrate compliance if requested.

Risk Management and Independent Assurance

18. Agency chief executives are the organisation's risk owner and are responsible for all ICT services their agency consumes, which includes adoption of offshore hosted (including public cloud) office productivity services.

19. The ICT security 'Certification and Accreditation' (C&A) process outlined at NZISM Chapter 4 is a PSR Requirement (INFOSEC-5) and provides the decision-making context for this guidance. The C&A process supports agency Chief Executives in approving agency ICT systems and services to operate, including formal granting of exemptions and acceptance of residual risks.

20. State Service agencies are required to follow the 'Cloud Computing Risk and Assurance Framework' [Reference E]. The AoG Cloud Computing: Information Security and Privacy Considerations document [Reference F] is a fundamental component of that framework and should be used to consider all aspects of risk identified with offshore hosted (cloud) service delivery. This guidance on security related requirements only partly addresses the scope of risk considerations at Reference F.

21. Risks associated with hosting government official information or data in foreign jurisdictions and the sovereignty of that information is explored at References F and G. Further clarification of the jurisdiction and sovereignty issues related to hosting offshore is expected in 2017, though in the interim the security requirements here offer effective mechanisms to address the extant risks.

22. This guidance recognises that agencies are required to adopt a risk management approach to cover all areas of protective security activity across their organisation (Reference C, Requirement GOV-3) and operate their own ICT risk assurance and assessment frameworks[10] in accordance with the NZISM[11]. For cloud services, inputs into this process include information gathered through:

    a. completion of the 'Cloud Information Security and Privacy Considerations' questionnaire [Reference F][12],
    b. risk assessments and Service Security Certificates (SSC) for public cloud services produced by DIA[13],

---

[10] For agencies without a risk framework, the Cabinet mandated cloud risk assessment process (Reference E) defined by GCIO can be found at: https://www.ict.govt.nz/assets/ICT-System-Assurance/Risk-Assessment-Process-Information-Security.pdf

[11] NZISM statements aligning with the government 'Risk Based Approach' can be found in NZISM Chapter 1, paragraphs 1.1.53 to 1.1.58 (risk management section); Chapter 4 – System Certification and Accreditation; and Chapter 5 – Information Security Documentation.

[12] https://www.ict.govt.nz/guidance-and-resources/information-management/requirements-for-cloud-computing/cloud-computing-mitigating-risk/.

[13] DIA (AoG) SSC and associated artefacts available through DIA CSD ITSM. Email gcio@dia.govt.nz with requests.

c. valid independent reporting, such as ISO/IEC-27001, CSA STAR and CCM, ISAE-3402, SSAE-16, or AICPA SOC audit reports, or certifications and other types of vendor or 3rd party assurance information,

d. other evidence available from suppliers and independent assessors, such as professional auditing or consulting firms.

23. This guidance includes a number of security requirements under the category of "Third Party (Independent) Assurance" (Requirements 12-15). These are designed to address risk areas where physical inspection and audit by agencies are not feasible or practical.

Security Requirements

24. Appendix 3 maps the Cabinet Minute security requirements to respective PSR Requirements and NZISM sections.

25. These security requirements are further expanded on in Appendix 4:

- **Ser**: The serial, or *unique identifier,* for the requirement.
- **Security Requirement**: a *short title* of the security requirement.
- **Requirement / Risk Description**: a *description* of the requirement and why it is needed, and the risk category it addresses,
- **Baseline Controls**: the *baseline security controls* and agency implementation responsibilities, and,
- **Additional Considerations**: possible *compensating controls* and other approaches agencies might consider and employ.

26. The description of each security requirement at Appendix 4 should be considered in context of the risks it is addressing. The principal risks are identified in the DIA Service Security Certificates and Risk Assessments for Office Productivity services at References H-L.

27. It should be noted that an extensive review of the NZISM has been undertaken to ensure consistency of this guidance to facilitate the use of public cloud services.

28. Where an agency use case[14] or the services being considered are unable to implement relevant baseline controls, the NZISM requires agencies to apply formal risk management practices and implement compensating controls.

29. This guidance provides examples and illustrations of compensating controls. Agencies should not apply these illustrative compensating controls verbatim. It is vital that agencies undertake a risk assessment and consider the most effective mix of baseline

[14] Such as agency publicly-accessible (UNCLASSIFIED) websites, though noting these are already subject to AoG web standards security guidelines.

and compensating controls in order to achieve the required levels of compliance, security and assurance.

30. Agencies should note that compensating controls and control sets may not necessarily be provided by the productivity service they are seeking to adopt. For example, there may be controls that the agency can provide itself, or may be provided through the service providers 'ancillary services', or may be provided by third-party vendors or other service providers.

Appendix 1: References

Ser	Reference Body and Title
A	CAB Min (16) 03/16, Cabinet Minute of Decision – Accelerating the Adoption of Public Cloud Services, 4th July 2016[15]. Note that this guidance document refers to the specific control statements at Paragraph 43.
B	New Zealand Government Information Security Manual (NZISM) v2.5, July 2016[16]
C	CAB Min (14) 39/38, Cabinet Minute of Decision – Protective Security Requirements[17]
D	GEA-NZ Reference Taxonomies and Models v3.1[18]
E	CAB Min (13) 37/6B – Cabinet Minute of Decision – Cloud Computing Risk and Assurance Framework[19]
F	GCIO AoG Cloud Computing: Information Security and Privacy Considerations, April 2014[20]
G	SSC Government Use of Offshore Information and Communication Technologies (ICT) Service Providers – Advice on Risk Management, April 2009[21]
H	DIA AoG IaaS Public Cloud Risk Assessment Report, 31 May 2016
I	DIA Microsoft Office 365 Risk Assessment Report, 7 Oct 2015
J	DIA Microsoft Office 365 AoG Audit Report, July 2016
K	DIA Microsoft Office 365 RESTRICTED Guidance and Recommendations Report, May 2016
L	DIA Azure Active Directory (AAD) Risk Assessment Report, June 2016
M	NIST SP-800-145, Definition of Cloud Computing, 2011[22]
N	Public Records Act, 2005[23]
O	NZ Government Information and Records Management Standard, July 2016[24]
P	Privacy Act, 1993[25]

[15] https://www.ict.govt.nz/assets/Cloud-computing/Accelerating-the-Adoption-of-Public-Cloud-Services-Redacted.pdf.

[16] http://www.gcsb.govt.nz/publications/the-nz-information-security-manual/

[17] https://www.protectivesecurity.govt.nz/home/mandatory-requirements/.

[18] https://www.ict.govt.nz/guidance-and-resources/architecture/government-enterprise-architecture-for-new-zealand-framework/.

[19] https://www.ict.govt.nz/assets/Cabinet-Papers/Cab-Minute-Cloud-Computing-Risk-and-Assurance-Framework-Oct-2013.pdf.

[20] https://www.ict.govt.nz/assets/ICT-System-Assurance/Cloud-Computing-Information-Security-and-Privacy-Considerations-FINAL2.pdf.

[21] https://www.ict.govt.nz/assets/ICT-System-Assurance/offshore-ICT-service-providers-april-2009.pdf

[22] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

[23] http://www.legislation.govt.nz/act/public/2005/0040/latest/whole.html.

[24] http://records.archives.govt.nz/assets/Guidance-new-standard/16-S1-Information-and-records-management-standard-Pdf.pdf.

[25] http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html.

Appendix 2: Definitions

Specific terms used in this document are defined in the table below, in order to ensure clarity of purpose, intent or meaning for this guidance. The reference sources are PSR and NZISM. Other sources used are stated in this table.

Term	Definition
Assurance	Assurance is a measure of confidence that the security features, practices, procedures, and architecture of an information system accurately interprets and implements security policy and prescribed controls.
Baseline Control	Information and controls that are used as a minimum implementation or starting point to provide a consistent minimum standard of systems security and information assurance. Baseline controls ('MUST' / 'MUST NOT' and 'SHOULD' / 'SHOULD NOT' controls – see below) are minimum acceptable levels of controls and sometimes referred to as "systems hygiene". Addressing baseline security controls is an obligatory requirement. Some controls cannot be individually risk managed by agencies without jeopardising multi-agency, All-of-Government or bi/multi-lateral international systems and related information.
Compensating Control	A compensating control (or alternative control) is employed where it is impractical or impossible to implement a baseline control. Compensating controls provide equivalent or comparable protection as the specified baseline control. Compensating controls usually encompass control sets, rather than an individual replacement control. Replacement controls alone are unlikely to be as effective as the specified baseline control. The key determinant on the extent of the compensating control set is the level of assurance required and mitigation of risk. For example, organizations with significant staff limitations may compensate for the separation of duty security control by strengthening the audit, accountability, and personnel security controls. [NIST SP 800-53]
Multifactor Authentication (MFA)	System user or administrator verification using two or more different factors to achieve authentication. Factors include [NIST SP 800-53]: • something you know (e.g. password/PIN); • something you have (e.g., cryptographic identification device, token); or • something you are (e.g., biometric, location, pay-rolled staff, etc.). In this context, a user is a real person. Machine or device-to-device communication and interaction may also require authentication, including mobile devices. Refer to the NZISM for guidance on machine-machine authentication.
MUST / MUST NOT	Requirements and controls with a "MUST" or "MUST NOT" compliance statement indicates that application of the control is essential, as it is mandatory to effectively manage the identified risk, unless the control is

	demonstrably not relevant to the respective system or service. A "MUST" or "MUST NOT" control is a baseline (or 'system hygiene') control and is deemed essential. Non-use is high risk. Where the controls as specified cannot be implemented because of technical or practical considerations, the rationale and justification for the non-use of controls and the selection of the compensating control set must be formally recorded. The residual risk from the replacement of the specified controls with a set of compensating controls must be formally acknowledged and agreed by the Accreditation Authority as part of the certification and accreditation process.
Public Cloud	A cloud deployment model where the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider. [NIST SP 800-145] A cloud deployment model where cloud services are potentially available to any cloud service customer and resources are controlled by the cloud service provider. [ISO/IEC 17788]
Risk Assessment	A systematic process of evaluating the potential risks related to a well-defined situation and a recognized threat or hazard that may be involved in a projected activity or undertaking. [ISO/IEC 31000] In the context of an information service/system, a risk assessment identifies, analyses and evaluates the risks related to the use of the information service/system, and measures them in context of likelihood/probability and impact. A risk assessment must precede, and is the basis of, the 'Certification and Accreditation' assurance process[26] government agencies are required to follow, to assure that information and its associated technology are well-managed. 'Security assessments' are a specific form of a risk assessment. These are third-party or internal audits (by an independent department of an organization) of on-premise or cloud-based systems. Traditional security assessments for infrastructure or applications and compliance audits are well defined and supported by multiple standards such as NIST, ISO, HIPAA, GLBA, PCI, CIS and CSA.
Security Control	A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements. [FIPS 199, NIST SP 800-53]. A statement as to 'how' a requirement or risk will be addressed or mitigated.

[26] Aligns more accurately to the risk treatment and risk acceptance steps of ISO 31000:2009, as part of an agencies Risk Management framework or strategy.

Security Requirement	Requirement on an information system or service that is derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted. [FIPS 200] A statement of 'what' is to be achieved in context of a threat or risk. A statement that identifies a necessary attribute, capability, characteristic, or quality of a system for it to have value and utility to an organization.
SHOULD / SHOULD NOT	Requirements and controls with a "SHOULD" / "SHOULD NOT" compliance statement denote good and recommended practice. Non-use of these controls is considered to represent medium or high risk to agency systems. As for "MUST" or "MUST NOT" controls, non-use is to be formally recorded, compensating controls selected as required, and residual risk acknowledged and agreed by agency Accreditation Authority.

Appendix 3: Mapping of Security Controls for Offshore Hosted Office Productivity Services to PSR and NZISM

Serial	Description	References (PSR Requirement / NZISM Chapter)
Strategy and Architecture		
1	Information, data or materials classified at CONFIDENTIAL and above MUST NOT be stored or processed in off-shore hosted office productivity services.	• Cabinet Minute CAB Min (13) 37/6B • INFOSEC-1,2,3, PHYSEC Protocol • CH22.1.8 – Enterprise Systems Security
2	Agencies MUST have process controls relating to intrusion detection, prevention, investigations and enterprise logging in operation.	• GOV-7, INFOSEC-2,3,4 • CH5 – Information Security Documentation • CH6 – Information Security Monitoring • CH7 – Information Security Incidents • CH16 – Access Control • CH18 – Network Security • CH19 – Gateway Security
3	Agencies MUST architect their ICT Networks to ensure that cloud services can be used safely and effectively.	• GOV-4, GOV-8, PERSEC-1, INFOSEC-1,2 INFOSEC-4[27], PHYSEC-6, INFOSEC Protocol • CH2 – Information Security Within Government • CH5 – Information Security Documentation
4	Agencies MUST have control over the interaction between public cloud services and end user devices.	• PERSEC-1, INFOSEC-2, INFOSEC-4, PHYSEC-6 • CH11 – Communications Systems and Devices • CH16 – Access controls • CH21 – Working Off-Site (21.4 BYOD) • CH22 – Enterprise Systems Security
5	Agencies MUST ensure compatibility with existing government security technology services in use, such as SEEMail and cyber defence capabilities.	• INFOSEC-3, INFOSEC-4 • CH16 – Access Control • CH18 – Network Security • CH19 – Gateway Security
Cryptography		
6	Agencies MUST ensure that data is encrypted in transit and at rest.	• GOV-9[28], INFOSEC-4, INFOSEC Protocol • CH17 – Cryptography • CH19 – Gateway Security

[27] It may be more appropriate for an agency to associate this requirement with INFOSEC-3.

[28] GOV-9 in context of referring to sovereignty concerns of NZ and partner nation agreements for shared information.

7	Agencies MUST have sole control over the associated cryptographic key.	• GOV-9, INFOSEC-4, INFOSEC Protocol • CH17 – Cryptography • CH22.1.22 – Enterprise Systems Security
Access Control		
8	Agencies MUST ensure that multi-factor authentication is used to control access to the service.	• GOV-4, GOV-8,9, PERSEC-1, INFOSEC-4 • CH12 – Product Selection • CH16 – Access Control (16.4) • CH19.1.18 – User Authentication
Backup and Recovery		
9	Agencies MUST identify where data stored by a service is replicated and/or backed-up.	• GOV-3, GOV-9, INFOSEC-2,3,4, PHYSEC-1,6,7 • CH16 – Access Control • CH20 – Data Management
10	Agency MUST revise their agency disaster-recovery plans to cater for cloud-based services.	• GOV-3,4,10, INFOSEC-2,3,4 • CH5 – Information Security Documentation • CH6 – Information Security Monitoring • CH7 – Information Security Incidents
System Decommissioning		
11	Agencies MUST have decommissioning processes as outlined in the NZISM.	• GOV-4, GOV-10, INFOSEC-4 • CH13 – Decommissioning & Disposal • CH22 – Enterprise Systems Security
Third Party (Independent) Assurance		
12	Agencies MUST have assurance checks on cloud service providers in accordance with the NZISM.	• GOV-5,6,8,9,10, PERSEC-1, INFOSEC-4,5, PHYSEC-6 • CH5 – Information Security Documentation • CH6.1 – Information Security Reviews • CH12.7 – Product Security, Supply Chain
13	Agencies MUST ensure that there are appropriate security controls over physical access to data centres.	• GOV-7,8, PERSEC-1, INFOSEC-4, PHYSEC-1,2,6 • CH8 – Physical Security • CH5 – Information Security Documentation • CH10 – Infrastructure
14	Agencies MUST have assurance that appropriate patching and maintenance of software is undertaken.	• GOV-8, INFOSEC-4 • CH10 – Infrastructure • CH12.4 – Product Security, Product Patching and Updating • CH14 – Software Security
15	Agencies MUST ensure there are technical protections to prevent data-mingling on shared storage platforms.	• GOV-8, INFOSEC-3,4 • CH5 – Information Security Documentation • CH16 – Access Control • CH18 – Network Security • CH19 – Gateway Security

Appendix 4: Controls and Considerations for Offshore Hosted Office Productivity Security Requirements

Ser	Security Requirement	Requirement / Risk Description	Baseline Controls	Additional Considerations
	Strategy and Architecture			
1	Information, data or materials classified at **CONFIDENTIAL and above** MUST NOT be stored or processed in off-shore hosted office productivity services.	**Information Classification**. Classifying information in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure. **Labelling of Information**. Establish information management procedures for information labelling (or tagging) to cover official information, and its related assets in physical and electronic formats.	Agencies are to ensure the target information set is classified and protected in accordance with the PSR[29].	The PSR provides clear instructions on how to classify official information, as well as how it should be subsequently handled.
2	Agencies MUST have process controls relating to **intrusion detection, prevention, investigations and enterprise logging**.	**Intrusion Detection and Prevention (IDP)**. Monitor network and/or system activities to identify malicious activity, record information about such activities, implement automated protection measures, and report incidents. Traditional network-based IDP measures are less effective where mobile devices (including BYOD) and remote access to cloud services is permitted, without traversing an agency's enterprise environment. **Event Logging, Alerting and Auditing**. Operate documented logging and reporting processes. Ensure that the service can provide an adequate level of logging and reporting that agencies are able to investigate and respond to security incidents in a timely manner. Auditing activities such as analysis of logs assists in identifying anomalies, vulnerabilities or incidents, which may then be proactively addressed. **Information Security Incident Management**. An incident management framework will allow agencies to respond to information security incidents. It enables a considered response, incident containment and impact minimisation. **Visibility or Transparency**. Visibility into user, application and data behaviour is essential for good cloud service management. Services should provide basic reporting mechanisms that cover metrics such as service usage, administrator activity, and user and application transactions.	Agencies are to have a governing policy on how intrusion detection, prevention and management will be managed with the cloud service provider. Specific considerations are to include: • Assurance that the service provider has effective intrusion detection capabilities. • Assurance that there are adequate procedures in place for the reporting and handling of breaches of privacy and security specific to the agency. • A named single point of contact for managing incidents with the service provider. • Service provider logs are made available to the agency (ie. commercially - through terms or conditions in agreements; and technically – through secured and resilient (out of band) channels), to ensure logs can be retained to meet an agencies internal policy requirements and records management obligations. • Service provider logs can be incorporated into internal logging and alerting systems and/or processes (in a timely manner). • Incident response plans are in place to address data leakages and breaches, and ensure appropriate timely reporting. • Where cyber threat intelligence (CTI) information exchange is available, then open standards are supported (eg. STIX, TAXII). Obtain and review a copy of any valid independent	See also Requirements #12 and #14. The adoption of cloud security services (whether through third-party providers or equivalent capabilities provided by the office productivity provider), can mitigate the gaps with traditional enterprise IDP and data loss prevention solutions: • Visibility — Dashboards that provide an aggregated view of employee usage behaviour for approved and unapproved cloud applications. • Compliance — Out-of-the-box compliance reporting modules and/or the ability to inform auditors about cloud security effectiveness. • Data Security — Encryption or tokenization of data in transit and at rest, while enabling organizations to retain control and preserve cloud application functionality. • Threat Prevention — Reduction of risk from both authorized (e.g., insider threats) and unauthorized (e.g., external malicious entities) sources, typically implemented as an access control function. NCSC recommend the following logs are retained for a minimum of 3 months for incident response purposes: • Workstation logs (eg. application whitelisting, events, anti-virus, and authentication). • Network device logs (eg. proxy, DHCP, DNS, VPN, firewall). • Server logs (eg. email, authentication, web access, remote access).

[29] https://www.protectivesecurity.govt.nz/home/information-security-management-protocol/new-zealand-government-security-classification-system/

Ser	Security Requirement	Requirement / Risk Description	Baseline Controls	Additional Considerations
			third-party audit reports (e.g. ISAE 3402, SSAE 16, ISO 27001, ISO 22301, ISO 27017, and ISO 27018) to provide assurance that appropriate controls are in place (NB. The full version of the audit report is preferred, rather than an executive summary. Audit reports are typically provided direct to an agency under a NDA).	
3	Agencies MUST **architect** ICT networks to ensure that cloud services can be used safely and effectively.	**Hardening of Systems, Devices and Applications**. Ensuring operating systems, applications, virtual hosts, networks, and end-user devices and services are designed and appropriately configured limits the opportunity for a vulnerability in the service to be exploited. **Architecture and Design review**. Reviewing the architecture and design of the service ensures that it meets the functional and non-functional business requirements including adequate controls to protect the confidentiality, integrity and availability of information stored, processed or transmitted by the service. An Architecture and Design review will also assess the organisation's adoption of, and integration with, the service to ensure that the organisation's own security controls will meet the businesses requirements.	Agencies must ensure that the architecture and operational assurance of their networks, client platforms and other supporting infrastructure (e.g. directories) are fit-for-purpose for cloud services that they intend to consume. Agencies are to consider all official and personal data and information held offshore, including: • development and production environments, • backup and archive services, and • disaster recovery services.	
4	Agencies MUST have control over the **interaction** between public cloud services and **end user devices**.	**End User Equipment.** GEA-NZ (I.4) identifies this category as including mobile and portable devices (ie. laptops, notebooks, netbooks, tablets, smartphones, and mobile phones) and desktop computers/terminals (thick, thin and zero clients). **Mobile Device and Application Management (MDM/MAM)**. Defining, documenting and managing secure mobile device configurations ensures that all devices used to access the service are hardened to a consistent baseline. MDM/MAM also provides the ability to remotely control devices and mobile applications (including remote device wiping) and apply agency's mobile device policies. **Mobile Device Encryption**. Ensuring all mobile devices used in the service are encrypted will reduce the likelihood of unauthorised access to the information they hold, should they be lost or stolen.	This control applies to agency supplied mobile devices and approved staff personal mobiles (BYOD). Implement a policy governing management and use of agency staff mobile devices, including encryption of information stored on the device, and control/approval for the use of specific mobile applications. Agencies should review their existing mobile device policies in context of use of public cloud services. Implement containers, sandboxes and other segregation techniques as appropriate for end user devices.	The use of a MDM/MAM application or third-party service provides a range of tools to meet the intent of this control. Consider the use of AoG TaaS services, which are designed to comply with the 'Government Network' (GNet) architecture approach (ie. the transport layer between devices and agency networks or cloud services is an untrusted zone).

Ser	Security Requirement	Requirement / Risk Description	Baseline Controls	Additional Considerations
5	Agencies MUST ensure **compatibility** with existing government security technology services such as SEEMail and, where appropriate, cyber defence capabilities.	Multi-agency and AoG services are subject to a higher risk threshold than an individual agency may consider appropriate for their own purposes (ie. the principle of aggregated assets and attack vector). This is particularly relevant in shared environments were boundary controls traditionally are not effected (eg. Email systems with SEEMail). The configuration of cloud office productivity services can compromise or bypass AoG services, impacting the benefits and regulatory requirements (eg. TICSA) of those services through poor design and implementation planning. See also Requirement #3.	Agencies must consider how to securely integrate cloud office productivity services with required AoG security services and are implemented in a way that does not compromise their own systems, data or those of other agencies.	The cloud service should support open standards and API's, where interaction with other agency systems is required; such as the OASIS CTI Standards (STIX, TAXII) for threat intelligence information exchange, and S/MIME for email. Separate guidance on Email controls will be developed. Though, for Exchange Online and email management, agencies should use sender policy framework (SPF); Domain Keys identified mail (DKIM); and domain-based message authentication, reporting, and conformance (DMARC) to reduce the amount of spoofed inbound email. If not already in use, the migration to offshore hosted services is a good time to enable them.
	Cryptography			
6	Agencies MUST ensure that information and data is **encrypted in transit and at rest**.	**Encryption of Data in Transit**. Ensuring official and National Security information that flows over public or untrusted networks, such as the Internet, is protected using NZISM approved cryptographic protocols and encryption algorithms. Transport Layer Security (TLS) protects connections to all services when using native clients and browsers, ensuring that data in transit is protected from eavesdropping. Alternatively, IPSec may be considered more appropriate, particularly where machine-to-machine communications occurs. **Encryption of Data at Rest**. Ensuring official and National Security information stored on media in offshore data centres is encrypted using NZISM approved cryptographic protocols and encryption algorithms. This requirement covers user authentication data (see also Requirement #8), as well as all forms of structured and unstructured official data and information. **Encryption of data in Processing**. Whilst this is not explicitly covered by this requirement, this aspect of data/information lifecycle should be considered in context of adhering to the intent of this requirement and efforts made to minimise the risk of exposure of unencrypted data/information in a service provider's environment. (eg. data should not be transported unencrypted from its storage location (in data centre 'A') to a processing application in a different location (data centre 'B'); or saved on hardware during processing).	Agencies must enforce the use of NZISM approved protocol and algorithm standards for encrypting data in transit and at rest. Note: TLS v1.2 and IPsec, using AES-256, are both NZISM approved cryptographic protocols and encryption algorithm combination for data in transit uses. The layering of encryption within a service providers environment (eg. at the hardware and application layers separately) may be considered to enhance the overall mitigation, though all layers of encryption should meet NZISM requirements.	Current market and technology maturity should allow for adequate levels of encryption to be applied to official information, both in transit and at rest. Some functionality of office productivity cloud service may be compromised by enforcement of encryption of data (files) in storage, and typically files need to be decrypted prior to processing in a cloud server environment. This issue is especially difficult where the Private Keys for the encryption algorithm are not shared (trusted) with the service provider (see following control section). In these circumstances, either the office productivity service provider or an independent third-party vendor can provide alternative mechanisms (options) within their services to minimise the residual risk and information exposure. Enforcing the use of secure web browser sessions (HTTPS) is industry accepted standard practice. TLS v1.2 should be the default mechanism allowed for such sessions. It is also recommended to use HTTP Strict Transport Security (HSTS) with HTTPS to protect users from man-in-the-middle attacks.

Ser	Security Requirement	Requirement / Risk Description	Baseline Controls	Additional Considerations
7	Agencies MUST have sole **control** over the associated **cryptographic keys**.	**Cryptographic Key Management**. Develop, document and implement key management processes to ensure that cryptographic keys are solely controlled by agencies throughout their algorithm and supply chain lifecycle are fit for purpose. Cryptography-based controls (Requirement #6) can help mitigate a range of information security risks. That mitigation can be negated by inappropriate key management. Cryptographic key management needs to be considered in context of data in transit and at rest, and also data *in processing* within the service providers infrastructure. Robust key management addresses the confidentiality, integrity, availability, authentication and non-repudiation aspects of protecting official information, as well as avoiding potential data loss, or loss of access to data. Rigorous key management practices and encryption of data throughout its lifecycle offshore mitigates the risk of unauthorised foreign state or criminal group acquisition of agency data/information. It will also mitigate against such scenarios as foreign judiciaries petitioning agency data from service providers for local court cases. To assure the effectiveness of approved encryption techniques in protecting official information and data, the (private) keys used for that encryption must be properly managed and controlled. This requires comprehensive management oversight and control over private keys throughout the entire supply chain and key lifecycle (including revocation). This requirement does not preclude the use of trusted third-party key management service providers, whose purpose is to provide assistance to agencies in the generation, storage, operation, management and retirement (disposal) of keys associated with their environments. The TaaS PKI managed services would be considered a trusted third party in this context. Office productivity services in particular may not yet	Agencies must ensure they have complete visibility over all uses and access of their private keys when operating with cloud service providers (ie. assured key management practices). Agencies must be able to demonstrate that any third party holding, using or managing agencies private keys in order to ensure functionality of a service is not compromised, or to provide a greater level of assurance over the management and security of keys than an agency itself may be able to provide, demonstrate (evidence-based) equitable credentials to that required of agency staff or other government outsourced service providers. Agencies must ensure that their cloud key management decisions do not compromise the security of other tenants, agencies or external parties. In all cases, agencies should ensure the use of a hardware security module (HSM) or equivalent to generate, manage, and store cryptographic keys. In cases where sole control of private keys (such as Hold Your Own Key [HYOK] approach) is impractical, agencies must consider carefully the nature of information that they are entrusting to a cloud service provider, and the different threats, adversary motivations and mitigations that are applicable, in order to reduce the risk and information exposure.	TaaS provides key management services through accredited (trusted) NZ-based PKI service providers, as well as ability for agencies to apply unique agency-specific encryption key to their cloud-based information sources. Note that TaaS PKI services provide options for high-level of information assurance and protection. The TaaS PKI managed services address the risk where an agency may have inadequate internal key management processes and skillsets to implement this control. Use of government approved HSM's allows private keys to be managed and/or hosted by third-party providers whilst maintaining full access control to those keys, providing access control to the HSM device is managed by the agency. Compensating control groups that should be considered where full and sole control of private keys is not achievable include: **Audit and Assurance**. Agency accreditation authorities must certify that service provider key management processes are robust, independently audited and fit for purpose, that any changes or incidents are notified and that any risks that cannot be mitigated by provider-held keys are noted in certification reports. Note 1: Commercial independent assurance audits would not be expected to consider the specific requirements of a government customer over any other customer group tenanted in a service provider's environment. Note 2: Audits of PKI key management environments have unique aspects not typically considered when following a traditional security risk assessment process (such as NZISM, ISO 27001, or CSA CCM). WebTrust[30] and ETSI[31] based audits cover the supplementary characteristics for PKI key management. **Contractual and legislative provisions**. Service providers should have clear policies (and track record) regarding their resistance to orders for disclosure of keys and data, and of operating only in countries with appropriate regulatory and legislative controls. Note that "Safe Harbour" type agreements are generally bi-lateral agreements that do not provide any safeguards for those countries not party to the specific agreement. Examples are the EU General Data Protection Regulation (GDPR 2016/679), US Cyber Security Act 2015, and EU-US Privacy Shield framework.

[30] Canada Institute of Chartered Accountant's (ICA) WebTrust Program for Certification Authorities: http://www.webtrust.org/homepage-documents/item54279.pdf.

[31] European Telecommunications Standards Institute (ETSI) Electronic Signature and Infrastructure Policy requirements for Certification Authorities issuing public key certificates: http://www.etsi.org/deliver/etsi_ts/102000_102099/102042/02.04.01_60/ts_102042v020401p.pdf.

Ser	Security Requirement	Requirement / Risk Description	Baseline Controls	Additional Considerations
		fully support this requirement in terms of 'sole control' of keys (ie. customer generated, owned and managed keys) in that functionality of the associated office applications will likely be degraded or even non-functional. In these circumstances, consideration of 'compensating controls' to address the risks in different ways is a valid action.		Note: Service providers may additionally commit to extend any contractual commitments it makes in regard to meeting the requirements of such mechanisms to customers that are domiciled outside of the territories in question. **Data segregation**. Using content filtering, robust information management policies and practices, or other data segregation techniques to restrict some information classifications from being transmitted to and stored in the service. **Procedural controls for Administrative access**. Service providers should have high quality, robust and audited processes in place to ensure their administrators' access to customer data is rigorously secured and controlled, and all such access is monitored, logged and open to customer inspection. This applies to any third-party staff that the service provider employees and grants access to customer environments. **Bring Your Own Key (BYOK)**. Using the office productivity service provider's infrastructure to manage and store cryptographic keys generated by an agency; and used by them to encrypt and decrypt agency information. Some services may not support HYOK, third-party HYOK or BYOK, hence care should be taken to understand capabilities at a service level rather than a provider level.
	Access Control			
8	Agencies MUST ensure that **multi-factor authentication** is used to control access to the service.	For a user (a real person) authenticating to an external service that handles official and/or personal information, multi-factor authentication provides the strongest level of authentication. Multi-factor authentication (MFA) requires a combination of at least two authentication factors (2FA). The intent of this requirement is to ensure Internet-based office productivity services are protected from unauthorised access via the Internet. This would not normally apply to users operating from within an agency's enterprise network boundary and having authenticated to the agency network, either from within an access-controlled physical agency building or using two-factor authentication (2FA). Remote users need a different combination of factors because they are not located within agency premises. Direct or remote user access to offshore office productivity services requires at least the same level of user access control and protections as agency staff accessing agency enterprise systems today.	Agencies must ensure the use of multi-factor authentication for all users (including privileged users and service provider staff) when using offshore hosted office productivity services. Agencies must ensure the office productivity service is capable of implementing a multi-factor authentication mechanism for direct remote connections to the Service. Agencies should ensure the office productivity service access control technologies and processes are compatible and integrated with the agency's enterprise systems. Note: It is not the intent that cloud access requires a second round of user MFA (2FA) authentication, either for each cloud or for cloud access collectively. The exception would be where the protection of compartmented or other special types of information may dictate further authentication mechanisms. This additional requirement is unlikely to affect many agencies.	Where a user has authenticated to an agency network using MFA (typically two authentication factors) then: • Step-up (re-authentication or additional) authentication is not automatically required. • Agency gateway authentication may compensate for a user-held second factor. • Remote users securely accessing cloud office productivity services via an agencies enterprise network (eg. using RAS token over VPN connection) may be considered as contributing to this control requirement. Conditional access controls and contextual authentication may also be used (e.g. restrict user access based on IP address, geo-location, agency office buildings and agency network log-in access controls). Where a user is operating from within an agency's enterprise boundary (including approved remote access mechanisms), they should already have met the MFA requirements. In these scenarios agency user access policies, such as Single/Same Sign-On (SSO), should be applied. It is important to note that device/machine authentication will

Ser	Security Requirement	Requirement / Risk Description	Baseline Controls	Additional Considerations
		The NZISM requires agency users to authenticate to all classified (agency) systems/services (19.1.18.C01). This control requires that multi-factor authentication is implemented as part of an agencies user access security control plan (including privileged users and service provider staff), which includes accessing offshore hosted services. Machine or device-to-device communication and interaction may also require authentication, including mobile devices. It is important to note, however, that the usual mechanisms applied to real persons cannot always be used in device-to-device authentication (e.g. biometrics).		also be required, and consider the differences between user and device authentication.
	Backup and Recovery			
9	Agencies MUST identify where data stored by a service is **replicated or backed-up**.	Agencies have an obligation to retain various types of content (records), and ensure its authenticity and integrity for many years. Defining and implementing a back-up process will ensure that all business-critical information, configurations, logs, etc. are recoverable to assist in meeting the business owner's Recovery Point Objective. The process may include appropriate controls required to protect the highest classification of information included in the back-up as well as regular back-up restoration tests to confirm its effectiveness. An offline encrypted copy of all back-ups may be required and maintained in a location that meets the physical and environmental security requirements for back-up media. Consideration should be given to ensuring a local copy of backup data is held to support business continuity in case of failure of the service or related communications. It is unusual for SaaS providers, or cloud providers generally, to provide backup or archive functionality of customer data, without specific provisions in the service contract, terms of use, or service agreements. Typically, they rely on SLA uptime availability of high tier data centres, and with some services having contingency of replicating data to secondary data centre for real-time	Agencies need to be aware at all times of the geographical location of all states of their data and information (development, operational, backup, archive) stored within offshore office productivity services. Agencies must consider privacy, legal and regulatory conditions within the jurisdictions where agency data may reside, as well as the registered jurisdiction of the service provider / vendor themselves. Agencies must ensure appropriate retention policies are set for information held within offshore office productivity services. This should include a process for backing up the data within the services and ensure any critical data that may be backed-up outside of the service is encrypted where it is held/stored by service providers. Agencies should ensure their data and information is suitably protected throughout the whole information/data lifecycle. Agencies should consider whether the office productivity service provides for point-in-time record recovery, as well as routine backup and Records Act compliant archive requirements. Agencies should safeguard against sharing Primary mailboxes with the email archive content.	Agencies must apply baseline controls #6 and #7 to backups and archived official information/data held offshore, in addition to the real-time information in service providers operational data centres. The enforcement of baseline controls #6 and #7 will largely reduce the risk of information loss to other actors or national governments, as sufficiently encrypted information[32] using agency-controlled private keys held in NZ will negate the ability of third-parties to decrypt official information within an anticipated useful timeline. Though the exact useful life-cycle of any official information stored in offshore hosted data centres is for the agency in question to determine. Email journaling/archive should maintain integrity of messages, in that users should not be able to delete from the formal archive / journal storage, and must not be able to do so without a record being retained of that event. Agencies should consider any potential need to retain original messages including full meta-data for evidential purposes. Some Data Centres backup whole data centre server storage to geographically isolated data centres, though these DC backups do not differentiate between multi-tenanted customer data, making it difficult to reconstitute individual customer information without significant resources. DC-DC (SAN) replication and backup traffic links may not be encrypted at all, or may not meet New Zealand Government

[32] In accordance with NZISM cryptographic protocols and encryption algorithms.

Ser	Security Requirement	Requirement / Risk Description	Baseline Controls	Additional Considerations
		fail-over and business continuity incidents.		standards.
10	Agency MUST revise their agency **disaster-recovery and incident management plans** to cater for offshore hosted office productivity services.	**Disaster Recovery Plan**. Defining, implementing and testing a Disaster Recovery plan supports the Recovery Point Objective and Recovery Time Objective requirements defined in the agency's Business Continuity Plan. If a separate data centre is used as secondary site, the same security requirements as the primary site is used and would ideally not be affected by the same environmental effects as the primary site (ie. geographical isolation against natural and localised events). **Incident Response Plan**. The purpose of developing an Incident Response Plan is to ensure that information security incidents are appropriately managed. In most situations, the aim of the response will be to contain the incident and prevent the information security incident from escalating. The preservation of any evidence relating to the information security incident for criminal, forensic and process improvement purposes is also an important consideration.	Agencies must review their availability and disaster recovery requirements when substituting cloud services for on-premise solutions. While cloud architectures can offer simpler and cheaper mechanisms for disaster recovery, agencies must ensure that services offer suitable geographic dispersal and data replication capabilities to meet Business Continuity objectives, whilst observing jurisdictional and sovereignty requirements. Agencies must consider network availability and integrity risks and may wish to consider on-shore/off-shore or local hybrid solutions to cater for communications restrictions or failures. Agencies must follow procedures specified in the NZISM and PSR in the event of suspected data leakage/loss that may constitute a breach. Agencies should ensure that their Security Risk Management Plan, Security Plan, procedures (SOPs) and Incident Response Plan are revised appropriately to include contingencies for use of offshore hosted (cloud) services, and remain logically connected and consistent for agency enterprise environments and with the agency's Security Policy, and other agency systems were appropriate.	Agencies could consider usage of a secondary cloud service provider for recovery in case of outages or disasters. Where CONFIDENTIAL or above classified information (Control #1) could be, or is, inadvertently handled; in/by offshore hosted office productivity services, agencies must have processes in place to work with the service provider to sanitise and/or purge hardware.
	System Decommissioning			
11	Agencies MUST have **decommissioning** processes as outlined in the NZISM.	**Media Sanitisation and Disposal Process/Plan**. A defined and implemented media sanitisation and disposal process and plan will assure that all media and devices are correctly sanitised prior to disposal or reuse. It will also outline the procedures to be followed if media cannot be adequately sanitised, for example when using cloud services such as offshore hosted office productivity services. In terms of cloud services, this will be considered in terms of the service providers 'decommissioning' or exit process. An audit trail of data sanitisation and decommissioning will provide the required assurance.	Agencies should ensure secure decommissioning processes are included in respective contracts, terms of use, or agreements. Agencies should ensure they have an appropriate exit strategy and decommissioning process, including the removal of all agency data. Agencies should obtain and review supporting audit artefacts to assure appropriate sanitisation and decommissioning processes are defined and used in line with the NZISM when exiting a cloud service. Agencies should ensure that supporting services, such as system logs and encryption key storage are also adequately sanitised.	Data disposal and service decommissioning processes are included in several industry assurance standards requirements (eg. ISO 27001, CSA CCM, FedRAMP). Agencies should check cloud service providers assurance and audit reports that this component meets agency requirements. Decommissioning of an office productivity services storage environment for both structured and unstructured information could be achieved through the revocation of the encryption keys implemented for data at rest, especially where these keys are 'owned' by the agency. Alternatively, the application of a unique 'disposal' encryption key to the storage environment may achieve the same outcome.

Ser	Security Requirement	Requirement / Risk Description	Baseline Controls	Additional Considerations
	Third Party (Independent) Assurance			
12	Agencies MUST require **assurance checks** on cloud service providers in accordance with the NZISM.	A 'controls audit' assesses the effectiveness of the processes and controls in place for the associated service. This could be done through internal or external audit. For cloud services, audits are usually performed annually to assure customers that the security of the environment holding information is managed and maintained as agreed and documented. Multiple international and industry bodies sponsor approved cloud assessment schemes and assurance frameworks, which are available as independently conducted reports and audits of a cloud service provider's environment. These standardised schemes include ISO-27001, ISAE-3402, SAE-16, CSA CCM & STARWatch, PCI-DSS, HIPAA, as well as others. Each assessment scheme or assurance standard covers a unique set of control areas, with no single scheme covering all risk areas affecting NZ Government interests. Where the assessment frameworks do not cover specific risk areas or this documents control groups, agencies will need to identify and address the gaps. Respected cloud service providers conduct independent audits against these schemes as part of their due diligence and to provide customers with evidence of quality service provision and compliance.	Agencies must obtain a full copy[33] of any valid independent third-party audit reports (e.g. ISAE-3402, SSAE-16 ISO-22301, ISO-27001) and review as part of their certification and accreditation process, and specifically to inform a risk assessment. Agencies must address findings (discrepancies, issues, risks) identified in independent audit reports in their own assessment. Agencies must monitor for incidents and changes in the cloud service provider operations, and incidents with other tenants, to continuously manage their risk profile. (NB. DIA AoG Team will monitor and advise agencies on common-use office productivity service providers). Agencies must ensure that provisions are included in contracts, terms of use or agreements for the agency to request future independent audit reports (usually on an annual basis).	Note that third party reports are valid for a fixed period of time, which normally does not exceed 12 months. It is important to check validity and expiry dates on any third party reports. Agencies should expect service providers to renew audit reports on an annual basis, or when major infrastructure changes occur (eg. change of data centre, etc.). Agencies may wish to request provision of additional or supporting assurance evidence is included in the service terms of use, or other contractual documentation. In some instances, agencies may wish the ability to request their own independent audit is conducted. In such cases, agencies should consider using internationally recognised auditors. Note: DIA (GCIO) and the Cloud Security Alliance (CSA) will publish informative mapping guidance of the principal assurance schemes against NZISM Controls in the CSA Cloud Controls Matrix (CCM), for agencies risk assessment use. A glossary of relevant cloud standards that include approved cloud assurance frameworks will also be published.
13	Agencies MUST ensure that there are appropriate security controls over **physical access** to data centres.	**Physical Security Perimeter**. The use of physical security perimeters defines the boundary of controlled areas that contain sensitive information and/or information processing facilities. Physical protection can be achieved by creating one or more robust physical barriers. The use of multiple barriers gives additional protection and appropriate entry controls ensure that only authorised personnel are allowed access. **Supporting Utilities and Environmental Security**. Ensuring environmental factors and supporting facilities are factored into equipment security considerations will	Agencies must obtain and review a full copy of any independent third-party physical security audit reports (e.g. ISO 27001), and ensure that appropriate security controls comply with the PSR and NZISM.	See also Requirement #12. Agencies should monitor for changes in regulations applicable to cloud service provider operations.

[33] Obtaining a full copy of an audit report is required for the agency's records and government requirements in the event of a serious incident.

Ser	Security Requirement	Requirement / Risk Description	Baseline Controls	Additional Considerations
		provide a holistic approach to security. Offshore data centres cannot be subjected to NZ Government physical audits as readily (if at all) as domestic facilities. Hence, a significant reliance on the service providers' evidenced assurances in this respect is to be expected.		
14	Agencies MUST have assurance that appropriate **patching and software maintenance** is undertaken.	A comprehensive Patch and Vulnerability Management strategy defines the implementation of software patching for the service that includes all system components (e.g. operating systems, databases, applications and network device firmware).	Agencies must obtain and review a full copy of any valid independent third-party audit reports (e.g. ISO-27001, CSA CCM / STARWatch, ISAE 3402, SSAE 16) to ensure timely software patch management practices are documented and operated by service providers.	See also Requirement #12.
15	Agencies MUST ensure there are technical protections to prevent **data-mingling on shared storage platforms**.	The implementation of logical segregation and isolation of all tenants on an IaaS platform (e.g. virtual networks with restrictions placed on communications and connectivity between them) will ensure that security incidents that affect a co-tenant are contained within that tenant's security domain and do not impact other tenants' services. The use of customer-unique encryption keys for file and data encryption will reduce the risks around cross-platform ingress.	Agencies must define clear business requirements for cloud services, including their intended boundaries for information sharing and segregation. Agencies' risk assessments must consider both the impact that agency services may have on other tenants, and potential threats from compromised or malicious co-tenants.	See also Requirement #12.