axenic
Information Management
Security and Privacy

Internal Audit Review of Certification and Accreditation of Cloud Based IT Systems

Report

Document Information

Statement of Work	STATS2016001
Client	Statistics New Zealand
Author	[redacted]

Document History

Version	Date	Author	Description of changes
1.0	24 June 2016	[redacted]	Final Audit Report.

Document Reviewers

Name	Role	Organisation	Version
[redacted]	Internal Auditor	Statistics New Zealand	1.0
[redacted]	IT Solutions Group Chief Technology Officer (Security Manager)	Statistics New Zealand	1.0

Document Approval

The following persons have endorsed this report.

Approved by	Signature	Date
[Name] [Position]		
[Name] [Position]		

Table of Contents

Contents

Tables

1 Executive summary

Background

This audit has been undertaken by Axenic Limited to support Statistics New Zealand's Internal Audit function review of the cloud adoption policies, processes and practices in place at Statistics New Zealand (SNZ), and to ascertain the appropriateness and effectiveness of the implementation of these practices. The audit involved the review of documentation, interviews with SNZ staff and observations based on site visits.

The audit was guided by the principles of ISO/IEC 27001:2013 Information Security Management Systems and the findings are presented with reference to the New Zealand Protective Security Requirements (PSR)[1] and New Zealand Information Security Manual (NZISM) [2].

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

2 Review of Certification and Accreditation of Cloud Based IT Systems

2.1 Background

The Statistics New Zealand (SNZ) Chief Technology Officer has become aware of issues with the certification and accreditation (C&A) of cloud based IT systems being used for SNZ business activities. These issues revolve around projects not being aware that certification and accreditation is required, knowing that there are specific requirements but not meeting them, or not obtaining appropriate sign off on the necessary project documentation that was produced.

If the controls over certification and accreditation of cloud based IT systems are inadequate, then SNZ may be vulnerable to increased risk exposure stemming from:

- breaches of security, privacy and/or confidentiality.
- a failure to integrate with existing systems (e.g. not being able to use single sign on).
- a lack of availability of cloud based systems to meet business requirements.
- not aligning with the strategic direction of SNZ or its enterprise architecture.
- a growth of “shadow services” (use of uncertified cloud services).
- potential non-compliance with GCIO, PSR, NZISM and Cabinet directives.
- having official information and data held in unauthorised repositories.

2.2 Purpose of engagement

Statistics New Zealand (SNZ) engaged Axenic Limited to perform a review of its cloud adoption policies, processes and practices, in order to provide the Chief Technology Officer and Internal Audit with understanding of any potential gaps in the current processes, as well as provide recommendations to improve alignment with agency requirements.

2.3 Audit objectives

The objectives of this audit were to review SNZ’s cloud adoption policies, processes and practices, in order to:

- Confirm whether appropriate frameworks are in place.
- Consider whether decision and implementation processes for cloud based IT systems are in place, operating and being complied with.
- Determine whether information risk assessments are being adequately completed, approved, and the risks addressed across cloud based services and systems.
- Review whether SNZ is complying with GCIO, PSR and NZISM requirements.

2.4 Audit scope

The scope of this audit plan was to examine and evaluate the following:

- The application and effectiveness of SNZ practices for adoption of cloud services including risk assessment, risk management, certification and accreditation.
- The responsibilities for sign off and approvals.

- Staff awareness of policies and procedures for adoption of cloud services.
- Auditor selected sampling of up to four representative initiatives, of either completed and/or in-flight cloud based projects, to determine whether all the required processes have been followed and are effective.

2.5 Audit criteria

This audit has referenced the following standards, frameworks or requirements:

- SNZ's own relevant policies, standards, guidelines, processes and procedures; including the risk management framework, risk assessment processes, certification and accreditation processes, security practices and project execution, staff awareness and training plans.
- ISO/IEC 27001:2013;
- Requirements from the Government Chief Information Officer (GCIO)[3]
- Protective Security Requirements; and
- NZISM November 2015, Version 2.4.

2.6 Audit processes and methods

Documentation reviews

This was conducted off site at the Axenic Limited office, and comprised the review of various SNZ documents, including but not limited to: policy documentation, internal audit reports, risk management framework and process, certification and accreditation process documentation, project lifecycle processes, sample projects for review, staff awareness and training plans and organisational charts.

Interviews

These were conducted on site at SNZ premises in Wellington, or via video conference link to other SNZ locations, and included; random sampling, role/responsibility specific interview questionnaires and discussions.

Observations

These were performed on site at SNZ premises in Wellington, including but not limited to: record observations, viewing of sensitive documentation which was not electronically shared and any differences between observed and documented policy and processes.

2.7 SNZ Project Manager

- [redacted]

2.8 Auditors

Axenic Quality Assurance and Oversight

- [redacted]

[3] GCIO and Cabinet requirements for Agencies using cloud computing https://www.ict.govt.nz/guidance-and-resources/information-management/requirements-for-cloud-computing/

Auditor(s)

- [redacted]
- [redacted]

2.9 Auditees

The following table lists the identified roles or functions that were interviewed for this audit. Please note that some role titles do not exactly match the actual role at SNZ, although the staff member holding the equivalent role and/or responsibility was selected to be interviewed as part of this audit.

Table 1 SNZ Auditees

Function/Responsibility	Name (Initial Identifier) and SNZ Role
Chief Technology Officer (CTO/CISO)	[redacted] – IT Solutions Group Chief Technology Officer
Chief Security Officer / Chief Privacy Officer (CSO/Chief Privacy Officer)	[redacted] – DCE Organisational Capability & Services
Manager Information Management (MIM)	[redacted] - Manager – Information Management reporting to [redacted] - Senior Manager – Standards & Design
Manager Security Office / Information Technology Security Manager (ITSM)	[redacted] – Security Manager
Enterprise Project Management (EPO)	[redacted] - Director – Enterprise Programme Office
HR Manager (HR)	[redacted] – Chief People Officer
Risk Manager (RM)	[redacted] – Senior Advisor – Strategy, Performance & Risk
Manager IT Operations and Services (IT Ops & Svcs)	[redacted] – Senior Manager IT Operations
Asset Manager – IT / Supplier Relationships IT (IT AM/SR)	[redacted] - Manager IT Sourcing and Supply
User Access Manager (UAM)	[redacted] – Manager Service Delivery
Legal Counsel (LC)	[redacted] – Legal Counsel
Privacy Officer (PO)	[redacted] – Senior Advisor – Strategy, Performance & Privacy

Function/Responsibility	Name (Initial Identifier) and SNZ Role
Business Owner – ECP (aka Salesforce) (ECP – Salesforce)	[redacted] [redacted] – Senior Manager – Operations Strategy & Development [redacted] [redacted] *(Solutions Architect) and Ashika Hogbin (IT Project Manager) were interviewed as* [redacted] [redacted] *was unavailable.*
Project Manager – ECP (ECP - PM)	[redacted] [redacted] – Programme Manager – Data Processes & Infrastructure

3 Audit process and findings

This audit process is based on the guidelines for auditing management systems ISO/IEC 19011:2011 and ISO/IEC 27007.

3.1 Audit findings ratings

The findings of this audit were categorised by the intent, implementation and effectiveness ratings identified in Tables 2 and 3 below.

Table 2 Intent and implementation ratings

4	Green - This indicates that there is **clear intent** to meet the expectations and the means to support the control objectives **have been implemented**.
3	Yellow – This indicates that there is **some intent** to meet the expectations and the means to support the control objectives are **frequently implemented.**
2	Amber – This indicates that there is **little or no intent** to meet the expectations and the means to support the control objectives are **partially implemented**.
1	Red - This indicates that there is **no clear intent** to meet the expectations, or **no implementation** to support the control objectives.

Table 3 Effectiveness ratings

4	Green - This indicates that the means to support the control objectives appear to be **consistently effective**.
3	Yellow – This indicates that the means to support the control objectives are **frequently effective**.
2	Amber – This indicates that the means to support the control objectives are **partially effective**.
1	Red - This indicates that the means to support the control objectives are **not effective**.

3.2 Detailed audit findings

A detailed summary of audit activities, findings, rationale and ratings are provided here in Table 4, with all supporting documentation which was provided listed in Table 6.

Table 4 Detailed audit findings

ID	Title	Activity	High Level Findings	Rating Rationale	Intent and implementation	Effectiveness of the control	ISO/IEC 27001: 2013 Annex A Controls Reference	PSR	NZISM 2015 V2.4
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	🟨	🟧	[redacted]	[redacted]	[redacted]

ID	Title	Activity	High Level Findings	Rating Rationale	Intent and implementation	Effectiveness of the control	ISO/IEC 27001: 2013 Annex A Controls Reference	PSR	NZISM 2015 V2.4
			• [redacted]		🟨	🟧			
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	🟩	🟨	[redacted]	[redacted]	[redacted]

ID	Title	Activity	High Level Findings	Rating Rationale	Intent and implementation	Effectiveness of the control	ISO/IEC 27001: 2013 Annex A Controls Reference	PSR	NZISM 2015 V2.4
			- [redacted]		🟩	🟨			
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	🟩	🟨	[redacted]	[redacted]	[redacted]

ID	Title	Activity	High Level Findings	Rating Rationale	Intent and implementation	Effectiveness of the control	ISO/IEC 27001: 2013 Annex A Controls Reference	PSR	NZISM 2015 V2.4
			[redacted]		🟩	🟨			
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	🟧	🟧	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	🟧	🟧	[redacted]	[redacted]	[redacted]

ID	Title	Activity	High Level Findings	Rating Rationale	Intent and implementation	Effectiveness of the control	ISO/IEC 27001: 2013 Annex A Controls Reference	PSR	NZISM 2015 V2.4
		[redacted]			🟧	🟧			
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	🟨	🟧	[redacted]	[redacted]	[redacted]4 16.5

ID	Title	Activity	High Level Findings	Rating Rationale	Intent and implementation	Effectiveness of the control	ISO/IEC 27001: 2013 Annex A Controls Reference	PSR	NZISM 2015 V2.4
			[redacted]		🟨	🟧			
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	🟧	🟥	[redacted]	[redacted]	[redacted]

ID	Title	Activity	High Level Findings	Rating Rationale	Intent and implementation	Effectiveness of the control	ISO/IEC 27001: 2013 Annex A Controls Reference	PSR	NZISM 2015 V2.4
			[redacted]		🟧	🟥			
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	🟨	🟨	[redacted]	[redacted]	[redacted]

ID	Title	Activity	High Level Findings	Rating Rationale	Intent and implementation	Effectiveness of the control	ISO/IEC 27001: 2013 Annex A Controls Reference	PSR	NZISM 2015 V2.4
			[redacted]		🟨	🟨			
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	🟨	🟨	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	🟨	🟧	[redacted]	[redacted]	[redacted]

ID	Title	Activity	High Level Findings	Rating Rationale	Intent and implementation	Effectiveness of the control	ISO/IEC 27001: 2013 Annex A Controls Reference	PSR	NZISM 2015 V2.4
		[redacted]	[redacted]		🟨	🟧			
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	🟧	🟧	[redacted]	[redacted]	[redacted]

ID	Title	Activity	High Level Findings	Rating Rationale	Intent and implementation	Effectiveness of the control	ISO/IEC 27001: 2013 Annex A Controls Reference	PSR	NZISM 2015 V2.4
			[redacted]		🟧	🟧			
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	🟨	🟧	[redacted]	[redacted]	[redacted]

ID	Title	Activity	High Level Findings	Rating Rationale	Intent and implementation	Effectiveness of the control	ISO/IEC 27001: 2013 Annex A Controls Reference	PSR	NZISM 2015 V2.4
		[redacted]	[redacted]		🟨	🟧			
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	🟥	🟥	[redacted]	[redacted]	[redacted]

ID	Title	Activity	High Level Findings	Rating Rationale	Intent and implementation	Effectiveness of the control	ISO/IEC 27001: 2013 Annex A Controls Reference	PSR	NZISM 2015 V2.4
		[redacted]	[redacted]	[redacted]	🟥	🟥			[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	🟩	🟨	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	🟨	🟧	[redacted]	[redacted]	[redacted]

ID	Title	Activity	High Level Findings	Rating Rationale	Intent and implementation	Effectiveness of the control	ISO/IEC 27001: 2013 Annex A Controls Reference	PSR	NZISM 2015 V2.4
		[redacted]	[redacted]	[redacted]	🟨	🟧			
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	🟨	🟧	[redacted]	[redacted]	[redacted]

ID	Title	Activity	High Level Findings	Rating Rationale	Intent and implementation	Effectiveness of the control	ISO/IEC 27001: 2013 Annex A Controls Reference	PSR	NZISM 2015 V2.4
		[redacted]	[redacted]	[redacted]	🟨	🟧			
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	🟨	🟧	[redacted]	[redacted]	[redacted]

ID	Title	Activity	High Level Findings	Rating Rationale	Intent and implementation	Effectiveness of the control	ISO/IEC 27001: 2013 Annex A Controls Reference	PSR	NZISM 2015 V2.4
			• [redacted]		🟨	🟧			
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	🟨	🟧	[redacted]	[redacted]	[redacted]

ID	Title	Activity	High Level Findings	Rating Rationale	Intent and implementation	Effectiveness of the control	ISO/IEC 27001: 2013 Annex A Controls Reference	PSR	NZISM 2015 V2.4
			• [redacted]		🟨	🟧			
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	🟨	🟧	[redacted]	[redacted]	[redacted]

ID	Title	Activity	High Level Findings	Rating Rationale	Intent and implementation	Effectiveness of the control	ISO/IEC 27001: 2013 Annex A Controls Reference	PSR	NZISM 2015 V2.4
			• [redacted]		🟨	🟧			
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	🟨	🟧	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	🟩	🟧	[redacted]	[redacted]	

ID	Title	Activity	High Level Findings	Rating Rationale	Intent and implementation	Effectiveness of the control	ISO/IEC 27001: 2013 Annex A Controls Reference	PSR	NZISM 2015 V2.4
		[redacted]	[redacted]	[redacted]	🟩	🟧	[redacted]	[redacted]	

ID	Title	Activity	High Level Findings	Rating Rationale	Intent and implementation	Effectiveness of the control	ISO/IEC 27001: 2013 Annex A Controls Reference	PSR	NZISM 2015 V2.4
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	🟩	🟨	[redacted]	[redacted]	[redacted]

3.3 Out of scope controls

The following management system controls were considered out of scope for this audit review.

Table 5 Out of scope controls

ID	Title	Justification	ISO/IEC 27001: 2013 Annex A Controls Reference	Relevant SNZ ID reference
XSNZ01	Organisation of information security	Mobile devices and teleworking are unlikely to have a bearing on cloud based services and system adherence to SNZ's certification and accreditation process.	6.2 Mobile devices and teleworking	SNZ15
XSNZ02	Asset Management	Cloud based services and systems are not SNZ's responsibility to manage, these requirements are contracted to the service/system provider, and reviewed using SNZ's certification and accreditation process.	8.1 Responsibility for assets	SNZ15
XSNZ03	Physical and environmental security	The physical and environmental security of cloud based services and systems are not SNZ's responsibility to manage, these requirements are contracted to the service/system provider and reviewed using SNZ's certification and accreditation process.	11.1 Secure areas	SNZ15
XSNZ04	Physical and environmental security	The physical and environmental security of cloud based services and systems are not SNZ's responsibility to manage, these requirements are contracted to the service/system provider and reviewed using SNZ's certification and accreditation process.	11.2 Equipment	SNZ15
XSNZ05	Operations security	Malware protection mechanisms of cloud based services and systems are not SNZ's responsibility to manage, these requirements are contracted to the service/system provider and reviewed using SNZ's certification and accreditation process.	12.2 Protection from malware	SNZ15
XSNZ06	Operations security	The controlled installation of operational software on cloud based systems are not SNZ's responsibility to manage, these requirements are contracted to the service/system provider and reviewed using SNZ's certification and accreditation process.	12.5 Control of operational software	SNZ15
XSNZ07	Communications security	SNZ network security, which is under SNZ control, is not likely to have a bearing on cloud based services and system adherence to SNZ's certification and accreditation process.	13.1 Network security management	-

4 Appendix

4.1 Documented evidence summary

The following pieces of evidence were provided by SNZ in support of the controls evaluated in this audit review. The Evidence Number and Evidence Required columns refer to the number of the piece of evidence requested by Axenic, which were subsequently mapped to the appropriate SNZ ID it was deemed to be applicable to.

Table 6 Documented evidence summary

ID	Title	Evidence Number	Evidence required	Title of document provided as supporting evidence	Key points and comments	Date of last document review	Date of next review	Provided to Axenic (DD/MMM/YYYY)
SNZ01	Security policies	1	Information Security Governance Framework	ID Ref 01 IPSaC Governance Group Terms of Reference.doc	• The IPSaC group is responsible for overseeing the management of organisation's risk, adherence to legislation, AOG direction and guidance with regards to privacy, security and confidentiality. • Terms of Reference sections: o Background o Scope o Purpose o Roles and Responsibilities o Meetings • Roles and responsibilities of the Information Privacy Security and Confidentiality Governance Group are documented. • The IPSaC Governance group consists of various business units and exec chair is DCE Organisation Capability & Services ([redacted] [redacted] • Meetings are held every 2 months.	-	-	24/05/2016
SNZ01	Security policies	1	Information Security Governance Framework	ID Ref 01 IPSaC working group Terms of Reference.docx	• The IPSac Working Group has been established at the recommendation of the IPSaC Governance Group. They are responsible for execution and monitoring the improvement plan (roadmap) that meets the goals of the IPSaC Governance Group. • The IPSaC Working group consists of senior manager and chair is Manager – Information Management ([redacted] [redacted] • Terms of Reference sections: o Background o Scope o Purpose o Roles and Responsibilities o Meetings • Appear to have the same sections from the Governance group, however the 'Focus Area' column has not been completed. • Roles and responsibilities of the Information Privacy Security and Confidentiality Working Group are documented. • Meetings are held every month or more frequently when the need arises.	-	-	24/05/2016
SNZ01	Security policies	1	Information Security Governance Framework	ID Ref 1 2016-06-14 Aligning ITS to the 4YP Decision Document audit copy	• Aligning ITS to the 4YP Decision Document – excerpt provided for auditing requirements. • CTO will change to Chief Digital Officer. • CTO will oversee five service lines are proposed, four of which will have a dedicated Service Assurance Consultant. • Security team will be separate from these service lines, and report to the Chief Digital Office, and will have two Security Advisors and a Security Manager.	06/2016	-	14/06/2016

ID	Title	Evidence Number	Evidence required	Title of document provided as supporting evidence	Key points and comments	Date of last document review	Date of next review	Provided to Axenic (DD/MMM/YYYY)
SNZ01	Security policies	2.1	Information Security Policy / Policies	ID Ref 02.1 Security Policies Framework.pdf	• SNZ takes into account several legislation and government-directed security framework in creating their policies. (Statistics Act 1975, PSR, NZISM, and AS/NZS ISO/IEC 27001 and 27002). • There are two ICT Assurance Frameworks in place at SNZ: ICT Operations and ICT Projects and Programmes. • Several policies are referred in the framework, these policies are under one of the four sections: Data Security, IT Security, Physical Security and Procedural & Administrator Security. • Consequence for breach of the policies is stated. • Security incidents are reported to the Security Office in the Security event database, guidance on reporting is provided. • Changes to policies, guidelines and procedures are communicated through Bulletin Board, Corporate Notices and email. • Framework review cycle is done every two years. • Approved by management.	07/07/2015	07/07/2016	24/05/2016
SNZ01	Security policies	2.2	Information Security Policy / Policies	ID Ref 02.2 Access to statistical and corporate data is provided on a need to do the job basis policy.pdf	• Guidelines on how to protect SNZ information and data from unauthorised access is stated. • SNZ staff and data custodian(s) responsibilities are stated. • Controls are in place to ensure the confidentiality of SNZ information and data remains protected. (e.g. Locking computer screen when left unattended, database restrictions, and etc.). • There are 7 Security Classifications at SNZ: Commercial In Confidence, Embargoed until, In Confidence, Policy in Confidence, Respondent in Confidence, Staff in Confidence, Unrestricted. • Best practice requirements are followed for secure storage and transfer of data (physically and electronically). • Changes to policies, guidelines and procedures are communicated through Bulletin Board, Corporate Notices and email. • Consequence for breach of the policy is stated. • Policy review cycle is done annually. • Approved by management.	13/07/2015	13/07/2016	24/05/2016
SNZ01	Security policies	2.3	Information Security Policy / Policies	ID Ref 2.3 Scope responsibility and secure use of our IT environment policy.pdf	• Cloud based and third party hosted software and services are part of the scope (IT environment) and covered in this policy. • Roles and unacceptable behaviour of the users of any IT environment within SNZ are clearly stated. • Managers are responsible for ensuring trainings are completed, staff are kept up to date with policies, and protecting the security and integrity of data, hardware, and software under their control. • Sections include: USB key and mobile device security, Virus protection, Use of non-standard hardware, software and data. • Changes to policies, guidelines and procedures are communicated through Bulletin Board, Corporate Notices and email. • Consequence for breach of the policy is stated. • Policy review cycle is done annually. • Approved by management.	13/05/2014	13/05/2015	24/05/2016
SNZ01 SNZ08	Security policies Access control	2.4	Information Security Policy / Policies	ID Ref 2.4 Access to and use of our IT environment is provided on a need to do the job basis Policy.pdf	• Sections include: Guidelines, Access rights and the use of strong passwords on SAS, Windows, and Lotus Notes. • There is a section about Passwords, which includes guidelines on Password Management. Passwords within Windows and Lotus Notes are changed every 90 days with a 14-day prompt. • Changes to policies, guidelines and procedures are communicated through Bulletin Board, Corporate Notices and email. • Consequence for breach of the policy is stated.	13/05/2014	13/05/2015	24/05/2016

ID	Title	Evidence Number	Evidence required	Title of document provided as supporting evidence	Key points and comments	Date of last document review	Date of next review	Provided to Axenic (DD/MMM/YYYY)
					• Policy review cycle is done annually. • Approved by management.			
SNZ01	Security policies	2.5	Information Security Policy / Policies	ID Ref 2.5 You have reasonable and appropriate personal use of the IT environment Policy.pdf	Sections include guidelines on reasonable and appropriate personal use for: ○ Usage of personal data ○ use of resources for personal use ○ use of non-standard hardware, software or data, ○ personal use of SNZ notes email ○ unacceptable use. ○ Copyright material ○ Use of PC or laptop for personal educational purposes ○ Electronic introduction or distribution • Changes to policies, guidelines and procedures are communicated through Bulletin Board, Corporate Notices and email. • Consequence for breach of the policy is stated. • Policy review cycle is done annually. • Approved by management.	13/05/2014	13/05/2015	24/05/2016
SNZ01 SNZ08	Security policies Access control	2.6	Information Security Policy / Policies	ID Ref 2.6 Our workplace security practices safeguard our work environment Policy.pdf	• Sections: ○ Manager's responsibilities ○ Clear Desk practices ○ Printing confidential data ○ Discussing confidential conversation ○ Waste Disposal ○ Password protected screensaver ○ Taking Photographs ○ Working away from the office ○ Logging off workstation ○ Protecting embargoed data and work areas ○ Responsibilities • Changes to policies, guidelines and procedures are communicated through Bulletin Board, Corporate Notices and email. • Consequence for breach of the policy is stated. • Policy review cycle is done annually. • Approved by management.	17/09/2015	17/09/2016	24/05/2016
SNZ01	Security policies	2.7	Information Security Policy / Policies	ID Ref 2.7 Security Incidents are reported to the Security Office for investigation Policy.pdf	• Security incidents are reported to managers and logged in the Security Events database, whether it is an actual or potential security incident or risk. • Security office will be responsible for investigating, mitigating or preventing the incident or risk. • Anyone can record and incident on the database but only the Security Office and other staff on a "need to know" basis has access to other recorded incidents. • There is a definition of what constitutes a security incident. (Category, Examples) • Guidance on how to report a security incident is included. • Changes to policies, guidelines and procedures are communicated through Bulletin Board, Corporate Notices and email. • Consequence for breach of the policy is stated.	13/05/2014	13/05/2015	24/05/2016

ID	Title	Evidence Number	Evidence required	Title of document provided as supporting evidence	Key points and comments	Date of last document review	Date of next review	Provided to Axenic (DD/MMM/YYYY)
					• Policy review cycle is done annually. • Approved by management.			
SNZ01	Security policies	2.8	Information Security Policy / Policies	ID Ref 2.8 Secure Information and Data Transfer ID Ref 2.8 Secure Information and Data Transfer Guidelines Part 2.pdf	• SNZ uses SEEMail, WinZip and MS Office Encryption are used to securely transfer data across the Internet. • Step-by-step instructions on how to use SEEMail, WinZip and MS Office Encryption are documented. • Consequence for breach of the policy is stated. • Policy review cycle is done annually. • Approved by management.	24/04/2014	24/04/2015	24/05/2016
SNZ01	Security policies	2.8	Information Security Policy / Policies	ID Ref 2.9 The role of the Security Office.pdf	• The Security Office regularly monitor access, attempted access, access to inappropriate access and unauthorised cloud based services. • SNZ aims to have a lean, modular and cloud based for its Technology Capability in the Target Operating Model Summary.	13/05/2014	13/05/2015	24/05/2016
SNZ01	Security policies	3	Cloud adoption specific or relevant documentation: e.g. policies, standards, guidelines, processes and procedures.	ID Ref 3 - 2016-04-15 Statistics NZ 2016 ISSP - Edition 1.pdf	• ISSP focus areas: o Delivering IT as a Service (ITaaS) o Modularised enterprise o Future operating model o Enhancing enterprise collaboration o Data access and integrated analytics • Focus Area 1: Delivering IT as a Service covers the End State Vision, Activities and Challenges. • The aim is to migrate to IAAS, TAAS, and DAAS to support its IT as a Service (ITaas) technology capability. • Focus Area 3: Future Operating Model. In the activities section, there is an intent to establish a Cloud Centre of Excellence to provide best practices, standards and technical oversight for all cloud services.	14 April 2016	N/A	24/05/2016
SNZ01	Security policies	4	Risk Management framework	ID Ref 4 - Risk Management Framework Design approved by ELT 17 August 2015	One-page visual representation of the SNZ Risk Management Framework. Includes an area called "Mandate and Commitment from the Executive Leadership Team", which includes expectations and accountabilities, risk management principles, risk appetite, strategic and enterprise risks. Also has an area called " Risk Management Framework Design", which includes reference to SNZ Context, a Risk Management policy, risk reporting schedule, resources and communication.	17/08/2015	-	25/05/2016
SNZ01 SNZ17	Security policies System acquisition, development and maintenance	4	Risk Management framework	ID Ref 4 A127155_Risk Appetite Statements A4 - Version 1 - 6 October 2014	Risk Appetite Statements from SNZ Gives guidance on the types and level of risk SNZ are willing to consider. Eight sections, and cloud adoption appetite may fall within more than one section, though most relevant areas would be: • Technology and information management – Open and Cautious • Core responsibilities – Cautious.	6/10/2014	-	13/06/2016
SNZ01	Security policies	5.1	Risk Management Process and Template	ID Ref 5.1 One page risk rating tool 5 November 2014	One-page Risk Rating Tool. Includes a consequences table, likelihood table and risk rating matrix (5x5, Very Low, Low, Medium, High, Very High).	5/11/2014	-	25/05/2016
SNZ01	Security policies	5.2	Risk Management Process and Template	ID Ref 5.2 Risk Register template	Excel spreadsheet example of a Risk Register for a Group/Project. Contains risk statement, inherent and residual risk assessment, risk owner, recommended controls and treatment activity, and a control/mitigation owner.	23/08/2013	-	25/05/2016

ID	Title	Evidence Number	Evidence required	Title of document provided as supporting evidence	Key points and comments	Date of last document review	Date of next review	Provided to Axenic (DD/MMM/YYYY)
SNZ01	Security policies	5.3	Risk Management Process and Template	ID Ref 5.3 Security Risk Assessment Template	Example template Risk Assessment Process document. Note that the risk matrix differs from the matrix in 5.1, and in the risk matrix section of the same document.	22/04/2013	-	25/05/2016
SNZ01	Security policies	15	Acceptable Use Policy	ID Ref 15 - Acceptable Use Policy	See evidence provided for: • ID Ref 2.2 Access to statistical and corporate data is provided on a "need to do the job" basis Policy • ID Ref 2.4 Access to and use of our IT Environment is provided on a 'need to do the job' basis Policy • ID Ref 2.5 You have reasonable and acceptable use of the IT environment Policy	-	-	26/05/2016
SNZ01	Security policies	29 31	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	26/05/2016
SNZ02	Organisation of information security	6	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
SNZ02	Organisation of information security	9.1	Project lifecycle process and management	ID Ref 9.1 EPO Project and Programme Home Page.pdf	• Screenshot of the Project and Programme Home page. Sections: ○ Management About us	-	-	24/05/2016

ID	Title	Evidence Number	Evidence required	Title of document provided as supporting evidence	Key points and comments	Date of last document review	Date of next review	Provided to Axenic (DD/MMM/YYYY)
					o Frameworks and Governance o Resources and Tools			
SNZ02	Organisation of information security	9 .2	Project lifecycle process and management	ID Ref 9.2 EPO Project and Programme Home Page.pdf	- SNZ's project lifecycle is aligned with PRINCE2. o Start-up o Initiation, Planning & Design o Delivery o Closure	-	-	24/05/2016
SNZ02	Organisation of information security	9.3	Project lifecycle process and management	ID Ref 9.3 Project Management Framework.pdf	Sections: o Project Management (definition) o Why use a project management method? o Methodology used at Statistics NZ o PRINCE2 Principles o Tailoring and scaling projects o Programmes vs projects o Project organisation o Project Lifecycle - No mention of security practices and processes in the project framework.	-	-	24/05/2016
SNZ02	Organisation of information security	9.4 9.5	Project lifecycle process and management	- ID Ref 9.4 Gating approval process diagram_Visio_0.2.vsd - ID Ref 9.5 Gating approval process_v1.0.pptx	- The CTO and other roles from the SLT are involved in providing a feedback during the Portfolio review.	-	-	24/05/2016
SNZ02	Organisation of information security	12	Chief Information Security Officer and IT Security Manager responsibilities (e.g. role description).	- ID Ref 12 FINAL_CTO_PD.pdf - ID Ref 12 FINAL_DCE - Organisation Capability and Services PD.pdf - ID Ref 12 Security Manager - PD.pdf	- CTO, DCE, and the SM responsibilities are clearly stated. (What is expected, how to achieve expectations, and benefits) - The CTO is also the CISO. - The Security Manager reports to the CTO. Manages and maintain the Cyber Security Strategy and oversee the Information Security Management Framework as well as the budget planning for security initiatives.	Dec 13	-	24/05/2016
SNZ02	Organisation of information security	13	Organisation Structure showing CSO role and roles of all IPSAG members and Investment Board members (*please list membership of each group)*.	ID Ref 13.3 FINAL Investment Board Terms of reference with list of members in section 8.docx	- CSO role is not identified in the ORG structure. - The CISO role is not identified in the ORG structure. - Investment board description and structure, Purpose, Responsibilities, Expectations from members, decision making, membership are covered in the Terms of Reference. - Roles and responsibilities are clearly stated. - Privacy Officer is a member of the Investment Board and CTO was invited to attend to provide expert input. - The meetings are held every 2 months. - The TOR has not been formally signed off by the Acting Government Statistician and Chief Executive.	-	-	24/05/2016
SNZ02	Organisation of information security	9 10	Project lifecycle process and management	ID Ref 9 and 10 FW Customer Focus	Copy of an internal SNZ heads up email from the Customer Focus Programme Manager to a group of internal stakeholders, including the Security Manager ([redacted] [redacted] and the CTO/CISO ([redacted]	28/10/2015	6/11/2015	25/05/2016

ID	Title	Evidence Number	Evidence required	Title of document provided as supporting evidence	Key points and comments	Date of last document review	Date of next review	Provided to Axenic (DD/MMM/YYYY)
			Security practices and processes executed during a project's lifecycle.	Programme Plan - A heads up for Review	[redacted] to book in time to review the Customer Focus Programme Plan, due the following week on Friday. The feedback would go to the portfolio board for their review and approval process.			
SNZ02	Organisation of information security	10	Security practices and processes executed during a project's lifecycle.	ID Ref 10 FW Project Plan - Transfer of Meshblock Custodianship from LINZ	Copy of an internal SNZ from the Enterprise Programme Office Programme Manager to a group of internal stakeholders, including the Security Manager [redacted] to review a Project Plan: Transfer of Meshblock Custodianship to LINZ.	10/12/2016	18/12/2016	25/05/2016
SNZ02	Organisation of information security	10.1	Security practices and processes executed during a project's lifecycle.	ID Ref 10.1 Project Plan Standard Template	Project plan template document. Approvers document signoff does not include Security Manager or CTO/CISO by default. CTO is included in the Portfolio Gating Endorsement section, which is a removed section if the Programme Gating approval section applies instead. The risk management section of this document advises risks will be managed in accordance to the <Programme's> Risk Management Strategy and the EPO Risk Management guidelines. Only Project risks are identified in this document, not a full risk assessment. Also has an Issue Management section, however actual issues are not recorded here.	16/07/2014	-	25/05/2016
SNZ02	Organisation of information security	10.2	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	25/05/2016
SNZ02	Organisation of information security	10.3	Security practices and processes executed during a project's lifecycle.	ID Ref 10.3 Quality and Assurance Monitoring and Control Template	Quality and Assurance Management Strategy and Plan, Monitoring and Control Strategy template document. In the "What will be reviewed and controlled" section, Risks and issues management is included. Security is mentioned in the "Project Quality Processes" section under the step name Security Review.	26/03/2013	-	25/05/2016
SNZ02	Organisation of information security	10.7	Security practices and processes executed during a project's lifecycle.	ID Ref 10.7 EDA Decision Making Guidance Template	Design and Standards Review PowerPoint template. Business Owner/Project Executive must be present for presentation. Includes: • Information Management Standards slide: *Demonstrate adherence to the Data and Information Management policy, specifically the four policy statements and three principles.* • Design Considerations – Government slide: Security section describing security features to be enabled. • Design Considerations – Information Privacy Security and Confidentiality (IPSaC): ○ Data ownership and classification ○ Security and privacy risk assessment ○ Privacy and Security by design ○ Cloud based solutions - GCIO cloud computing questionnaire responses.	-	-	26/05/2016
SNZ03	Human resource security	14.1	Staff information security responsibility acknowledgement	ID Ref 14.1 Security and IT Policies Declaration Form.docx	• One page document for SNZ employees and contractors to sign after reading the provided SNZ Security and IT Policies.	N/A	N/A	24/05/2016
SNZ03	Human resource security	14.2	Staff information security responsibility acknowledgement	ID Ref 14.2 Security and IT Policies for Induction.pdf	• The document consists of high level summary of the security policies in place at SNZ. • All SNZ employees and contractors are required to read and understand the policies. • Consequence for breach of the policy is stated. (Disciplinary action, up to and including dismissal)	N/A	N/A	24/05/2016

ID	Title	Evidence Number	Evidence required	Title of document provided as supporting evidence	Key points and comments	Date of last document review	Date of next review	Provided to Axenic (DD/MMM/YYYY)
SNZ03	Human resource security	14	Staff information security responsibility acknowledgement	ID Ref 14 Statistics New Zealand forms - email	Email from [redacted] [redacted] (HR Administrator) containing: • Full staff induction pack – Including code of conduct, MoJ check form (1/2/2016) • Declaration of secrecy form to sign • IRD Certificate of secrecy (IR820).	-	-	9/6/2016
SNZ03	Human resource security	14	Staff information security responsibility acknowledgement	ID Ref 14 Request for evidence on Orientation Journey for Internal Audit Review of Certification and Accreditation of Cloud Based IT Systems – email and attachments	Email from [redacted] [redacted] forwarded from [redacted] [redacted] of SNZ Learning and Development team. Confirms that all staff must complete Orientation Journey online CBT, and that the content of this course includes mentioning of The Security Framework, and various other information security related policies and practices. Attachments showed the current online training slides, and the updated copy of the course as it is in the process of being refreshed. Also contained a copy of the automated email for new users once they have been registered into HR systems.			22/06/2016
SNZ03 SNZ08	Human resource security Access Control	11.1	SNZ staff/project manager awareness and training activities and plans (relevant to cloud service/system adoption).	ID Ref 11.1 PMCoP Project Management Community of Practice Home Page showing meeting dates and topics	Project Management Community of Practice (PMCoP) Seemingly relevant topics from the list on the intranet: • 16 March 2015 Gating approval process. • 27 Jul 2015 System security certification and accreditation process. • 7 December 2015 Lord of the Rings and Stakeholder Engagement. • 7 March 2016 Procurement questions – What have you learnt today. • 28 Apr 2016 Procurement at Stats NZ	-	-	25/05/2016
SNZ03 SNZ08 SNZ15	Human resource security Access Control Operations Security	11.2	SNZ staff/project manager awareness and training activities and plans (relevant to cloud service/system adoption).	ID Ref 11.2 PMCoP presentation 27.07.15 on Certification and Accreditation	Copy of the presentation dated 27 Jul 2015: Security Certification and Accreditation (C&A), (identified in 11.1). • *SNZs Information Privacy, Security and Confidentiality Governance Group (a subcommittee of ELT) made **C&A compulsory** for all new systems from 1 July 2015.* • Your responsibilities slide, includes: *Identify and **manage** information **security** and **privacy risks** at the project level* • Supporting documentation slide, includes mapping of C&A requirements to the project lifecycle stage and prime party responsible: ○ Concept stage = Security and privacy risk scope assessment. Business Owner or Project Team. ○ Requirements and design stages = Security and privacy risk assessment. Project Team. ○ Requirements and design stages = Third party due diligence. Project Team. ○ Design stage = Relevant security standards. Sec Team. ○ Design stage = System Security Plan & Standard Operating Procedures. Project Team. ○ Design stage = Review solution design. Sec Architect. ○ Test stage = Security testing. Project Team. ○ Deploy stage = Certification review. Sec Team. ○ Deploy stage = Accreditation. CTO.	27/07/2015	-	25/05/2016
SNZ15	Operations security	11.2	SNZ staff/project manager awareness and training activities and plans (relevant to cloud service/system adoption).	ID Ref 11.2 W1316551_Security - Process Diagram - System Certification and Accreditation, V4.1	Copies of the System Certification and Accreditation process in two flow diagrams. Covers pre-certification requirements, CA review and Certification artefacts. CA is the SNZ Security Manager and the AA is the CTO/CISO. [redacted] advised via feedback email on 22/06/2016: SGC oversees this process, however this team no longer exists (last meeting 8/5/2014). Advised that this committee has been replaced by IPSaC governance group, first meeting 30/07/2014.	21/11/2014	-	8/6/2016

ID	Title	Evidence Number	Evidence required	Title of document provided as supporting evidence	Key points and comments	Date of last document review	Date of next review	Provided to Axenic (DD/MMM/YYYY)
					Minutes to the first IPSaC meeting state that Kelvin (Watson) provided background relating to the merger of the previous Privacy Advisory and Security Governance Groups following the restructure into the new entity.			
SNZ15	Operations security	7	Certification and Accreditation process	ID Ref 7 W1316551_Security - Process Detail - System certification and accreditation.docx	Draft V0.1 of the *Security Process Document System Certification and Accreditation* document, written by [redacted] [redacted] Security Manager, approved by the CTO (though unsigned). Based on MBIE C&A process document. Contains a significant number of C&A artefact documents which are required, including Security Risk Management Plan, System Security Plan, Standard Operating Procedures, Statement of Applicability, Security Risk Register completion, Risk Acceptance Memo etc. which do not appear to have been completed for the sample projects provided as a part of the Phase 3 review.	05/2015	-	22/06/2016
SNZ03 SNZ08	Human resource security Access Control	11.3	SNZ staff/project manager awareness and training activities and plans (relevant to cloud service/system adoption).	ID Ref 11.3 Security Newsletter May 2015 front page	May 2015 Security Newsletter front page, on intranet. Includes: • Privacy Week recap: Thanks for those who attended refresher training. • What is encryption? • Connectsmart • System Certification and Accreditation • In the News: How secure are kiwis online? ***Values and cornerstone principles:*** ***Leading, Connecting, Communicating, Statistical Excellence.*** *Integrity – Our reputation is one of our most valuable assets. It strengthens public trust and cooperation, and we work hard to maintain it.* *Confidentiality and data security – We set the highest standards for protecting the confidentiality and security of data.*	05/2015	-	25/05/2016
SNZ03 SNZ08	Human resource security Access Control	11.4	SNZ staff/project manager awareness and training activities and plans (relevant to cloud service/system adoption).	ID Ref 11.4 Security Newsletter - System Certification and Accreditation article May 2015	May 2015 Intranet news article: System Certification and Accreditation (identified in 11.3). Reminder that IPSaC made C&A mandatory from 1 July 2015 for all new systems or major upgrades to existing systems.	25/05/2016	-	25/05/2016
SNZ04	Asset management	17	Information Classification Policy	ID Ref 17 Stats NZ - Guidelines for Classifying Official Information.pdf	• Guidelines exists and were in line with the SIGS requirements for classifying information, which has been superseded by the PSR (NZISM). • There are 6 categories, however SNZ are most likely not to handle any information above RESTRICTED. • Guides for classifying In-Confidence and Sensitive information in SNZ's context are stated in the document. • Any information that doesn't fall under an In-Confidence or Sensitive classifies is categorised as unclassified. • There are three endorsements that are used at SNZ: Budget, Commercial and Staff. • If SNZ receives information of a higher classification, it will adhere to all agreements regarding the handling of that documentation. • Referred to several documents for additional guidelines: o Internal confidentiality rules o Guidelines for Protection of Official Information o Guide to Cabinet Committee Process	08/05/2014	08/05/2015	24/05/2016

ID	Title	Evidence Number	Evidence required	Title of document provided as supporting evidence	Key points and comments	Date of last document review	Date of next review	Provided to Axenic (DD/MMM/YYYY)
SNZ04 SNZ16	Asset management Communications security	17	Information Classification Policy	ID Ref 17 Information Classification Matrix from Tui Tuia 080616	Intranet published Information Classification Matrix, provided by MIM during interview on 8 June 2016. Matrix has information classifications which are not consistent with the Guidelines for Classifying Official information, although these guidelines are under review.	-	-	08/06/2016
SNZ01 SNZ04	Asset management	18	Information Handling Policy	18.1 Information and Data Management Policy.pdf	• SNZ has to comply with several legislative requirements and these are listed in the document. • Roles and responsibilities of Staff, Data Custodians, Tier 3 Managers and Manager of Information Management are stated. • The Government Statistician is responsible for ensuring the compliance of SNZ with legislative requirements for information and data management. • There is a Monitoring Framework that consists of the high level requirements for information handling. • Policy is reviewed every three years. • There is no guidance around handling of information of different classifications. However, under the Additional Resources section, several links are referred to that has specific instructions but these were not reviewed.	07/03/2013	12/02/2016	24/05/2016
SNZ05	Asset management	16	Storage Media Handling policy	ID ref 16 Media Handling Policy	See evidence provided for: • ID Ref 2.2 Access to statistical and corporate data is provided on a "need to do the job" basis Policy • ID Ref 2.3 Scope, responsibility and secure use of our IT environment Policy	-	-	26/06/2016
SNZ05 SNZ06	Asset management	28	Information asset allocation of ownership and responsibilities (information custodianship)	ID Ref 28	Security Manager [redacted] [redacted] advised to [redacted] [redacted] *“System certificates identify the system owners for cloud services that have been certified. The IT application portfolio / configuration management database / definitive software library are outdated and / or incomplete, this is a piece of work David Dingle’s team are working on to update.”* [redacted] [redacted] is Senior Manager, Enterprise Solutions.	-	-	26/05/2016
SNZ06	[redacted]	30	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	26/05/2016
SNZ06	[redacted]	30.2	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	27/05/2016
SNZ06	[redacted]	30.2	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	27/05/2016
SNZ10	[redacted]	35 36	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	26/05/2016

ID	Title	Evidence Number	Evidence required	Title of document provided as supporting evidence	Key points and comments	Date of last document review	Date of next review	Provided to Axenic (DD/MMM/YYYY)
SNZ11	Operations security	32	Change Management Process	ID Ref 32 - IT Change Management Policy incl guidelines	IT Change Management Policy (part of IT Service Management) *"There will be only one Change Management policy and process, as defined and maintained by the Change Manager."* Configuration items under change control: • All IT Environments: Development, Test, UAT, Production….. • Physical assets such as servers or network devices. • Virtual assets, such as virtual assets or virtual storage. • Software and applications, including third party software such as …..and externally hosted applications • Third party infrastructure and systems, including those managed by vendors…. Configuration items excluded from change control: • Documentation…..is not controlled…. • Metrics and SLAs…. • The below do not require changes/releases: o ….Copying data from one location/environment to another as requested by the business information custodian. Types of changes: Standard, Minor, Significant, Major, Emergency. Significant and Major changes approved by CAB, Emergency changes need to be approved by the business Owner and one of Change Manager/IT Ops and Services Manager/Emergency CAB. CAB, meets fortnightly, membership includes: Security and Information Management (as required), and must have unanimous approval to allow a Significant or Major change to progress. Review cycle: To be reviewed every two years, however approval table has a list of approvers with no dates next to approval being given. Consultation process completed 15/11/2013 for 13 SNZ Teams.	8/8/2014	8/08/2015	26/05/2016
SNZ15	Operations security	7.3	Certification and Accreditation process (including sign off responsibilities).	ID Ref 7.3 System Security Certificate - Template	System Security Certificate (template) document for the Enterprise Collection Platform – *not completely cleansed of information.* Included: • List of artefacts reviewed and their acceptability, including a Security and Privacy risk assessment (PIA threshold analysis). • Summary of risks and recommended actions. • Signoff: CA is Security Manager, Business Owner, Accreditation signoff CTO/CISO. PIA was deemed not required, although information was classified as RESTRICTED or SENSITIVE.	18/11/2014	01/03/2016	25/05/2016
SNZ15	Operations security	8.1	Recent Certification and Accreditation which has been performed on a cloud based IT system.	ID Ref 8.1 System Security Certificate - Loomio	System Security Certificate document for Loomio (SaaS). Unsigned document, references NZISM V2.3 2015 so not most recent considering date of the document is April 2016. Included: • List of artefacts reviewed and their acceptability, including a Security and Privacy risk assessment (PIA threshold analysis, PIA not required), GCIO cloud security requirements questionnaire, procurement involvement to ensure appropriate contractual agreements are in place, due diligence of Loomio and its third parties, security standard accreditation provided for	13/04/2016	15/04/2018	25/05/2016

ID	Title	Evidence Number	Evidence required	Title of document provided as supporting evidence	Key points and comments	Date of last document review	Date of next review	Provided to Axenic (DD/MMM/YYYY)
					AWS and Heroku application (available through Salesforce), SOPs, solution design (online available information only), security testing not reqd for UNCLASSIFIED information, Service Mgmt, DR plan. • Summary of risks and recommended actions. • Signoff: CA is Security Manager, Business Owner, Accreditation signoff CTO/CISO.			
SNZ15 SNZ10	[redacted]	8.2	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	25/05/2016
SNZ15	Operations security	27	Evidence of security reviews on each of the cloud based IT service/system providers (identified in evidence number 26)	ID Ref 27 Apprvd Cloud Endorsement SNZ - AzureAD	Cloud Endorsement by Agency for Azure AD / Single Sign On. Describes some of the steps taken by SNZ in assessing the cloud service, including: Stats review of GCIO Cloud Considerations questionnaire responses –Microsoft Azure, and various other security activities as part of the formal assessment and assurance of service utilisation. Endorsement is sent to GCIO at DIA via the ICTAssurance@dia.govt.nz mailbox.	26/04/2016	-	26/05/2016

ID	Title	Evidence Number	Evidence required	Title of document provided as supporting evidence	Key points and comments	Date of last document review	Date of next review	Provided to Axenic (DD/MMM/YYYY)
SNZ15	Operations security	27	Evidence of security reviews on each of the cloud based IT service/system providers (identified in evidence number 26)	ID Ref 27 Apprvd Cloud Endorsement SNZ - Livechat	Cloud Endorsement by Agency for Livechat. Describes some of the steps taken by SNZ in assessing the cloud service, including: GCIO Cloud Computing User Assessment tool, and various other security activities as part of the formal assessment and assurance of service utilisation. Endorsement is sent to GCIO at DIA via the ICTAssurance@dia.govt.nz mailbox.	26/04/2016	-	26/05/2016
SNZ15	Operations security	27	Evidence of security reviews on each of the cloud based IT service/system providers (identified in evidence number 26)	ID Ref 27 Apprvd Cloud Endorsement SNZ - Loomio	Cloud Endorsement by Agency for Loomio. Describes some of the steps taken by SNZ in assessing the cloud service, including: GCIO Cloud Computing User Assessment tool, and various other security activities as part of the formal assessment and assurance of service utilisation. Endorsement is sent to GCIO at DIA via the ICTAssurance@dia.govt.nz mailbox.	26/04/2016	-	26/05/2016
SNZ15	Operations security	27	Evidence of security reviews on each of the cloud based IT service/system providers (identified in evidence number 26)	ID Ref 27 Cloud Endorsement SNZ Salesforce	Cloud Endorsement by Agency for Salesforce, Unsigned WIP. Describes some of the steps taken by SNZ in assessing the cloud service, including: GCIO Cloud Considerations questionnaire responses from Salesforce, and various other security activities as part of the formal assessment and assurance of service utilisation. Endorsement is sent to GCIO at DIA via the ICTAssurance@dia.govt.nz mailbox.	None	-	26/05/2016
SNZ15	Operations security	27	Evidence of security reviews on each of the cloud based IT service/system providers (identified in evidence number 26)	ID Ref 27 Cloud Endorsement SNZ SurveyGizmo	Cloud Endorsement by Agency for Survey Gizmo, Unsigned WIP. Describes some of the steps taken by SNZ in assessing the cloud service, including: GCIO Cloud Computing User Assessment tool, and various other security activities as part of the formal assessment and assurance of service utilisation. Endorsement is sent to GCIO at DIA via the ICTAssurance@dia.govt.nz mailbox.	None	-	26/05/2016
SNZ15	Operations security	27	Evidence of security reviews on each of the cloud based IT service/system providers (identified in evidence number 26)	ID Ref 27 Cloud Endorsement SNZ Template	Cloud Endorsement SNZ Template document. *"This endorsement does not constitute system accreditation or certification as described in Chapter 4 of the New Zealand Information Security Manual."*	15/10/2014	-	26/05/2016
SNZ15 SNZ19 SNZ21 SNZ22	Operations security Information Security Incident Management Compliance Compliance	20	Reporting evidence of a recent internal or external audit on the information management systems, policies and processes.	ID ref 20 EY report RE Follow up on ID Ref 20 EY Report - email	Statistics New Zealand Security Assessment DRAFT Report – Phase 1 – V2.0 18 February 2014 EY Audit of SNZ Includes: • Recommendation to improve the security, privacy and confidentiality incident response process, ensuring it covers logging, reporting, oversight and governance. • Recommendation to improve accountability managing incident investigation, including a RACI model as part of the end to end Security Incident Management Process. • Recommendations on information handling. • Recommendations on people and culture – Awareness. Note that phase 2 was not commissioned, EY proposal never went ahead. Follow up email dated 30/05/2016 from [redacted] via consultation with [redacted] Relevant information for cloud adoption summarised here: • Security incident management processes: Implementation complete. • Accountability: Implementation complete, though RACI not used. • Commercial information: all information is treated the same way under the implemented Incident Management Process.	18/02/2014	-	25/05/2016 30/05/2016

ID	Title	Evidence Number	Evidence required	Title of document provided as supporting evidence	Key points and comments	Date of last document review	Date of next review	Provided to Axenic (DD/MMM/YYYY)
					• Access to information: Data custodians have been assigned and identified in Colectica for almost all current statistical outputs – this work is on track to be completed by 30.6.16. Splunk (SIEM tool) – proof of concept completed for it to be used for the IDI and it is about to go into active use. Otherwise, how to address this recommendation is still being considered. • Information dissemination: Email attachment self-release, spot checks done by Security team. • Encryption: Encryption of information on external devices is still not enforced, policy recommends encryption, our key control is from limiting which staff user profiles include a live USB/DVD port. • Organisational culture: This recommendation is addressed by the Internal Audit Review of Confidentiality of Business Respondent Information (review currently in draft). The Security Team do root cause analysis of privacy, security and confidentiality incidents – to date there has been no evidence of issues with organisational culture. • External contractors – Contracts and training: Key control is for researchers and contractors to sign declarations of secrecy under the Statistics Act, and (if relevant) Inland Revenue certificates of secrecy, and the associated explanation that precedes the signing of these documents. Researchers are required to complete specific researcher confidentiality training. Contractors are required to complete the Statistics NZ induction process, including security briefing and signing of declarations. Contractors (those filling staff vacancies) are required to complete the express version of the Orientation Journey. • Induction: Induction process covers confidentiality; business units do their own training on types of statistical information for new staff. The Orientation Journey is completed by staff and contractors filling staff vacancies. Researchers are required to complete the specific researcher confidentiality training. The Security Team and Privacy Officer are engaged in ongoing promotion of the Incident Management Process. Coffee clubs are no longer run, replaced by induction Day.			
SNZ15 SNZ17 SNZ18 SNZ21 SNZ22	Operations security System acquisition, development and maintenance Supplier relationships Compliance	26 (part 2) 37	List of all known cloud based IT service/systems in use by SNZ.	ID Ref 26 (part 2) - see body of email ID Ref 37 – See ID 26 - email	*The following is a summary of applications we [SNZ] need GCIO cloud endorsement signoffs for.* • Certified applications: ○ Loomio ○ Salesforce (WIP) ○ Azure ○ Live chat ○ Survey Gizmo (WIP) • Common capabilities or other agency services we consume and have/will place reliance upon the lead agency's assessment: ○ CabNet ○ Common Web Platform (SilverStripe) ○ Cohesion (Tui Tuia) ○ Shiny (interim solution - IDI use Treasury's implementation via Catalyst) ○ LINZ Data Service (environmental reporting) ○ TMIS (HR talent management info system) in the pipeline ○ 8Wire (Social Investment Unit file transfer system) in the pipeline • Certifications in progress: ○ Mulesoft (Cloudhub platform, in progress as part of the full certification of ECP)	-	-	26/05/2016

ID	Title	Evidence Number	Evidence required	Title of document provided as supporting evidence	Key points and comments	Date of last document review	Date of next review	Provided to Axenic (DD/MMM/YYYY)
					o WhosOnLocation (new visitor registration system) o Online Collection System (OCS – built on common web platform) • Known legacy applications not certified (will be certified at next major system upgrade): o Wingspan o Ako o RemAlly o StaffCV o IBM Kinetix (staff engagement survey) • Known unsanctioned 'shadow cloud' applications: o Trello o HootSuite o SurveyMonkey o Jira o Axonify • Unknown 'shadow cloud' applications: o 'Skyhigh' assessment identified 790 cloud services being accessed by SNZ staff. Still to determine if they are for personal / business use. Proof of concept for Skyhigh to prove there is an issue and so proposal to pursue solutions in the pipeline. Contracts reviewed by Sourcing and Legal, Security and Privacy only engaged ad hoc for inclusion prior to signing contracts.			
SNZ17 SNZ11	System acquisition, development and maintenance Operations security - Operational procedures and responsibilities	21	Architecture and/or design documentation and reviews for SNZ utilised information in cloud based systems.	ID Ref 21 - Architecture and or design documentation for SNZ utilised information in cloud based systems	[redacted] advised: [redacted] [redacted] *(Security Manager) has said he will show you on site as both the architecture/design documentation and reviews contain in-confidence information.* Appointment booked in for Thursday 2 June 9-10.30am. Lateral Security SSO V1.0 Draft report Released 10 Aug 2015 (Final) External penetration test and design review. 1xhigh 1x medium was resolved, 1xhigh remains unresolved around documentation. Accepted by C&A process approval. Note CB is business owner is also Certification Authority, so could be COI. 1xlow and 1x informational also in the pipeline for resolution. SurveyGizmo C&A Reviewed by SNZ Security Dept. 27/11/2015 Qualified System Security Certificate written by Security team to CB, to be reviewed 31/3/2016. Recertification currently WIP. Validation of controls effectiveness is carried out. Risks rated medium or below are within appetite. Risks above this need to be recorded in Operational Risk Registers however not all teams have an Operational Risk Register.	-	-	26/06/2016

ID	Title	Evidence Number	Evidence required	Title of document provided as supporting evidence	Key points and comments	Date of last document review	Date of next review	Provided to Axenic (DD/MMM/YYYY)
					CWP Architecture Document – Silverstripe document, not SNZ standardised documentation. Validation of design and implementation via Security Architect and independent security testing. Processes are not part of this review.			
SNZ19	Information security incident management	22	Information Security Incident Response and Management processes	ID Ref 22 Information Security Incident Response and Management Process	Reporting a Security, Privacy or Confidentiality Incident, process on intranet. Steps: • Attempt recovery • Report – Call to Security and/or Privacy directly. Notify your Manager or failing that their Manager ASAP. • Managers Review – review containment or recovery. See communication principles. Ensure incident has been logged in the Security & Privacy Incident Database. Ensure Security / Privacy teams have been alerted of the incident. • Notify your manager. • Follow up – identify action and prevent re-occurrence. • Security and Privacy Teams: ○ Advise and Act – they engage the Triage Team. Evaluate level of risk involved. ○ Prevention. • Triage Team, Chief Security / Privacy Officer: ○ Triage. Incident response is one of the GCIO questions, so SNZ is advised if the supplier has a process, and point of contact to SNZ (usually an individual).	-	-	26/06/2016
SNZ19	Information security incident management	23	Evidence of a post information security incident review (of a cloud based IT service/system incident)	ID Ref 23 – Security Incident Report	Copy of a Security Incident Report, rated as In Confidence, dated as 16/12/2015, for incident occurring 11/12/2015. Example of non-sanctioned cloud service Worditout.com Word Cloud used by SNZ staff member to create a word cloud for a serious injury data set. Note: the incident deals with a potential abrogation of the security of the parsed lists of descriptor variable observations from the fatal and serious non-fatal work-related serious injury data sets, that the word clouds were based on.	11/12/2015	-	26/06/2016
SNZ20	Information security aspects of business continuity	24	Recent Business Continuity test reports (showing RPO and RTO being met) of all cloud based IT services/systems	ID ref 24-26 – Cloud based IT services/systems BC test reports - email	Current situation with Business Continuity, as advised by [redacted] [redacted] Manager – Service Planning & Performance in Enterprise Solutions to [redacted]: *"These questions are a little premature for our level of organisational maturity, we have not previously had an organisational Business Continuity Programme. We have now established this programme and are in the process of completing the Business Impact Analysis (establishing our continuity requirements). One of the outputs of this process will allow us to articulate the RTO/RPO's for our systems prior to developing and implementing the appropriate Business Continuity Solutions. Once implemented they will part of an ongoing test (exercise) programme.* *Currently we have limited BC solutions of ITS systems involving our Email and Document Storage Systems (A Mixture of Active- Active (not requiring testing) and Active Passive), along with a comprehensive electronic offsite backup regime. These are designed to support basic Crisis management capability only at this time."* BCP Test Reports for cloud based IT services/systems: None at this time.	-	-	25/05/2016

ID	Title	Evidence Number	Evidence required	Title of document provided as supporting evidence	Key points and comments	Date of last document review	Date of next review	Provided to Axenic (DD/MMM/YYYY)
					BCP and/or DR remedial activities as a result of this testing: None at this time.			
SNZ21	Compliance	19	Reporting to show internal compliance with security policy (e.g. from managers to senior managers).	ID Ref 19 - Reporting to show internal compliance with security policy	None. *We do not do reporting to show internal compliance with security policy along the lines of your example of from managers to senior managers – Advised by Lance Edwards and Victoria Craig.*	-	-	26/06/2016
SNZ21 SNZ15	Compliance Operations security	33	Due diligence performed on cloud based IT services/systems	ID Ref 33 - Due diligence performed on cloud based IT services/systems - email	[redacted] advises: *No documents for this one.* [redacted] [redacted] *Security Manager, told me that "due diligence performed on cloud based IT services/systems" is part of the Certification and Accreditation process.* *It is done via the GCIO cloud questionnaire. Please refer to the ID Ref 7 documents.* See evidence provided for: • ID Ref 7 (SNZ17).	-	-	26/05/2016
SNZ21	Compliance	34	Service Level Agreements in place with cloud based IT services/systems (including how they will meet RPO and RTO)	ID Ref 34 - Cloud based SLAs - email	No documentation provided to support that SLA's were in place with cloud based providers, however the assertion from [redacted] [redacted] of SNZ after discussion with colleagues is as follows: • our cloud applications do have SLAs • in almost every case the SLA will be the provider's standard SLA • we do not usually have the "clout" to renegotiate an SLA away from the provider's standard SLA for the cloud applications that we currently use • where there are SLAs these are not kept in a central place, but are most likely with the business unit that uses the application • in the future we are likely to move to Desktop-as-a-service and other AoG mandated cloud services, in which case we may have negotiated SLAs • in other AoG mandated cloud services, we may be under DIA negotiated SLAs i.e. we won't have our own ones.	-	-	27/05/2016
SNZ21	Compliance	34	Service Level Agreements in place with cloud based IT services/systems (including how they will meet RPO and RTO)	ID Ref 34 – email from [redacted] [redacted]	Email from [redacted] regarding background information on contractual compliance. [redacted] has no visibility over cloud suppliers meeting SLAs, and also does not re-review T&Cs pre-negotiated with MBIE or DIA for all of government offerings (e.g. Intergen contract re ECMS, Silverstripe re Common Web Platform). He does help with the tailoring of SOWs etc. under these contracts (not that security or confidentiality are usually covered in SOWs). He has reviewed and provided advice and feedback re varying cloud based service agreements (e.g. re amazon web services, survey gizmo). The call as to whether these T&Cs tick the boxes re security standards, at least from a legal understanding, sits with the security team. [redacted] has also looked specifically at the characteristics of legal regimes (e.g. EU v Virginia in the US) to help inform the security assessment process.	-	-	7/06/2016
SNZ21 SNZ18	Compliance Supplier relationships	33	Due diligence performed on cloud based IT services/systems	ID Ref 33 Email re supplier contracts - example as discussed	Email from [redacted] in follow up to interview, containing evidence to support there are SNZ specific contract clauses pertaining to security and privacy.	-	-	10/06/2016

4.2 Phase 3 documented evidence summary

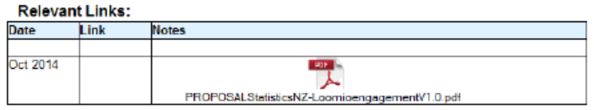
The following pieces of evidence were provided by SNZ as part of the evaluation of the effectiveness of SNZ's cloud service implementation practices, and to help identify any gaps/weaknesses. The Evidence Number and Evidence Requested columns refer to the number and piece of evidence requested by Axenic.

Table 7 Phase 3 documented evidence summary – 2018 Census Online Engagement Tool: Loomio, provided 17/06/2016

Evidence number	Evidence requested	Title of document(s) provided as supporting evidence	SNZ response in "email" document	Axenic comments (Italics quoted from evidence)	Acceptability and gaps	Recommendations
1.	System Security Certification and Accreditation document (approved/signed copy)	System Security Certificate – Loomio.docx	Attached	SSC dated 13/04/2016 Prepared by Security Manager (Certification Authority) for Business Owner and CTO (Accreditation Authority). Unsigned. Valid for 2 years. Evaluated to NZISM V2.3 2015 when documented C&A process is to Nov 2014 V2.1. All required artefacts were deemed acceptable by the SM. A detailed "System Security Certification and Accreditation" document was not provided (such as that for Microsoft Azure AD and SSO document).	No. Approval not verified by authorised signoff of SSC. A detailed SSC&A document was not provided.	• Complete consistent documentation, such as an SSC&A document, for all Certification and Accreditation activities. • Ensure that this formal document is appropriately completed, signed off and stored.
2.	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
3.	Security architecture review document	System Security Certificate – Loomio.docx	Does not exist – The Security Advisor researched available solution design online. As this is a cloud hosted solution no SNZ specific design documentation was required. https://www.heroku.com/policy/security https://devcenter.heroku.com/articles/dyno-isolation etc. https://aws.amazon.com/security https://www.loomio.org/privacy	*As this is a cloud hosted solution no SNZ specific design documentation was required*. This was deemed acceptable by the SM in the SSC.	No. Approval not verified by authorised signoff of SSC.	• Ensure a System (Security) Architecture review exists for all Certification and Accreditation activities (as it is assessed as part of the Certification process). • Ensure that this review is appropriately documented if required and also stored.
4.	Privacy impact assessment (if the system contains private data)	Stats Leg Review - Brief Privacy Analysis v0 1.docx	Combined with security risk assessment as system / data unclassified – Privacy Officer attended risk workshops. Have also attached the brief privacy impact analysis for a new Loomio use case (Stats leg review) which is in-flight.	PIA was determined to not be required, documented in the System Security Certificate. However, there is a privacy risk (R01) in the risk assessment, which confirms that a privacy risk is a valid risk, and that a privacy specific control was to be applied to mitigate this (Policies and rules of participation). Information classification is UNCLASSIFIED. Statistics Legislation Review document is currently a WIP, and the responses are inconsistent with information provided in the	No.	• Ensure the decision whether or not to conduct a PIA is made by a Privacy professional, and is formally agreed and recorded/stored. • Ensure that a PIA is conducted whenever a system contains private data. This is required by the Certification process.

Evidence number	Evidence requested	Title of document(s) provided as supporting evidence	SNZ response in "email" document	Axenic comments (Italics quoted from evidence)	Acceptability and gaps	Recommendations
				SSC (e.g. Loomio is hosted by Heroku with cloud services provided by AWS/EC2).		
5.	Security risk assessment and remediation plan (approved/signed copies)	Loomio Risk Assessment Template.docx	Attached	This risk assessment is undated and unsigned, and would appear to be a draft version (0.1), which still has Template in the title. The risk rating matrix in the risk assessment differs from the SSC as well as the current SNZ Risk rating tool and Risk Assessment process documentation. This is due to the risk assessment having been performed under older risk matrix criteria, and the SSC having been completed recently in April 2016 using a new risk matrix. This could lead to legacy risk assessments being rated at levels inconsistent with the current organisation risk rating scale. The Business Owner is identified in the SSC as being responsible for ensuring all identified controls are managed and remain in place during the life of the system, however the risks do not appear to have been entered into a risk register for the project/system or ICT operations risk register.	No. Approval not verified by authorised signoff of RA.	• Ensure that a consistent risk rating matrix is used in all risk assessments and that legacy risk assessment ratings are reassessed to align with the current risk rating scale for certification and/or recertification purposes. • Ensure that risk assessments are appropriately signed off and recorded/stored. • Ensure all identified residual risks which are outside SNZ appetite, after control effectiveness has been verified, are centrally recorded/stored to enable appropriate management. This is required by the Certification process.
6.	System classification (including information classification)	Cloud Computing Information Security and Privacy Considerations-Loomio.docx	Unclassified - refer system security certificate, risk assessment, and GCIO cloud considerations.	Information classification is UNCLASSIFIED. SSC also stated that entering names, email addresses and phone numbers were optional when registering, if a respondent chose to not be anonymous. It does not state how respondents register if they do wish to remain anonymous. GCIO Response 23 regarding privacy: *Yes – names and contact details captured during the registration process.* This is inconsistent with the Statistics Legislation Review document and the classification which was determined as UNCLASSIFIED.	No. Information classification is likely to be IN CONFIDENCE according to SNZ and PSR criteria. Only scenario where the rating would be UNCLASSIFIED is if registration of persons wanting to remain anonymous does not include personally identifiable information.	• Ensure that information classifications are consistently applied for all SNZ data. • Ensure that all project documentation has a consistent description and classification of the data involved. This is required by the Certification process. • Ensure that a consistent data classification policy is in use at SNZ.
7.	Risk acceptance and any exemptions required	System Security Certificate – Loomio.docx	Business owner sign-off of system security certificate.	Business owner is [redacted] [redacted] would need to sign off as accepting risk. Document provided was unsigned and not dated.	No. Approval not verified by authorised signoff of SSC.	• Ensure there is appropriate Business Owner risk ownership. This can be done by ensuring the Business Owner has signed off the RA, SSC&A and SSC. • Ensure the appropriate Business Owner is identified in the centrally managed risk register. • Ensure any exemptions to SNZ policy are appropriately signed off, recorded, and managed. This is required by the Certification process.
8.	Excerpt of risks entered in to the ICT operations risk register for the project/system	"Email" .doc – summarises SNZ responses to evidence request	Does not exist.	Although 6 risks were identified in the Security and Privacy Risk assessment in April 2016, it appears that as the residual ratings were not entered into the ICT operations risk register for the project/system. This was supposed to have been completed by the end of April 2016 according to the Endorsement form. This means that the risks identified are not able to be easily reassessed if the environment changes, or should current controls become less effective.	No. Was supposed to have been done by April 2016.	• Ensure all identified residual risks which are outside SNZ appetite, after control effectiveness has been verified, are centrally recorded/stored to enable appropriate management. • Ensure the appropriate business owner is identified in the centrally managed risk register. • Ensure that the residual risks have appropriate security controls (with

Evidence number	Evidence requested	Title of document(s) provided as supporting evidence	SNZ response in “email” document	Axenic comments (Italics quoted from evidence)	Acceptability and gaps	Recommendations
				The result is that the SSC could be misleading as the effectiveness of the current controls has not been validated and so the risk ratings may be more or less than assessed. This could also negatively impact recertification activities if the control effectiveness is not based on the inherent risk rating.		owners identified), to ensure ratings are accurate over time.
9.	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
10.	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
11.	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Evidence number	Evidence requested	Title of document(s) provided as supporting evidence	SNZ response in "email" document	Axenic comments (Italics quoted from evidence)	Acceptability and gaps	Recommendations
12.	GCIO cloud considerations – Completed responses and evaluation from SNZ on these responses	Cloud Computing Information Security and Privacy Considerations-Loomio.docx	Attached	Author is SNZ Security Manager – [redacted] (Certification Authority). Unsigned by [redacted] (Business Owner). Workshop participants are all SNZ staff: Privacy Officer, Security Manager, Statistical Analyst and Subject Matter Project Manager. All 105 responses are based on information provided/published on vendor websites and not directly from the vendor.	No. Approval not verified by authorised signoff of GCIO responses.	• Complete consistent documentation, such as the GCIO Cloud Computing Information Security and Privacy Considerations document, for all cloud related activities/projects. This includes AoG common capabilities. • Ensure that the responses are evaluated as to suitability to SNZ. • Ensure that this formal document is appropriately signed off and stored.
13.	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
14.	Endorsement form sent to ICTAssurance (approved/signed copy)	W1439109_Cloud Endorsement SNZ – Loomio.pdf	Attached	Endorsement form for Loomio has been completed, and signed off by the SM, CTO and CSO. Sending of this form to the GCIO would follow this process, though this is unconfirmed.	Yes. However, confirmation of sent message to GCIO is unconfirmed.	• Ensure that there is a process for completing and sending Endorsement forms to ICTAssurance. This would follow on from the Accreditation process. • Ensure that this formal document is appropriately signed off and stored.
15.	Business case – (approved/signed copy)	"Email" .docx – summarises SNZ responses to evidence request	 Relevant Links: Date | Link | Notes Oct 2014 | | PROPOSALStatisticsNZ-LoomioengagementV1.0.pdf Found in same DocOne doc as per item 9.	Business case document appears to exist in the DocOne system at SNZ. Content of this document is unknown. Approval is assumed due to project going ahead with due diligence and contracts.	Yes.	• Ensure that a formal business case document is appropriately signed off and stored (as it is a required artefact of the SSC).
16.	Design and configuration documentation – (approved/signed copy)	"Email" .doc – summarises SNZ responses to evidence request	Does not exist – refer item 3.	*As this is a cloud hosted solution no SNZ specific design documentation was required.* This was deemed acceptable by the SM in the SSC.	No. Approval not verified by authorised signoff of SSC.	• Ensure that a formal design and configuration document is appropriately signed off and stored (as it is a required artefact of the SSC). Exception is when there are no SNZ specific design components required or not deemed as required by the Security team.
17.	NZISM controls compliance - (all applicable controls and how compliance rating was determined)	"Email" .doc – summarises SNZ responses to evidence request	Does not exist – was not performed for the Loomio cloud based service (UNCLASSIFIED).	NZISM controls comparison not completed due to the information being classified as UNCLASSIFIED. However, as the system does contain private data (names, email, phone numbers) this rating may be incorrect, and a review of NZISM controls may/would have been required.	No. Approval not verified by authorised signoff of the RA. Information classification is likely to be IN CONFIDENCE according to SNZ and PSR criteria.	• Ensure all applicable security controls from the SNZ RA are mapped to NZISM security controls to measure NZISM compliance. • Ensure the document which maps security controls to NZISM compliance is appropriately signed off and stored (e.g. in a RA, Controls catalogue).

Evidence number	Evidence requested	Title of document(s) provided as supporting evidence	SNZ response in “email” document	Axenic comments (Italics quoted from evidence)	Acceptability and gaps	Recommendations
					Only scenario where the rating would be UNCLASSIFIED is if registration of persons wanting to remain anonymous does not include personally identifiable information.	
18.	Standard Operating Procedures	“Email” .docx – summarises SNZ responses to evidence request	Third Party SOPs have not been sighted - reliance was placed on independent certifications that these are in place. The Security Advisor reviewed SNZ SOPs for administering and operating the Census engagement instance of Loomio in 2014 – I do not have a copy of these.	SSC states: *The Security Advisor reviewed SNZ SOPs for administering and operating the Census engagement instance of Loomio which were of an acceptable standard.* As these were not provided upon request, it would appear that if these documents do exist they may not have been filed in a retrievable location.	No.	• Ensure that standard operating procedures are documented, appropriately signed off and stored (as it is a required artefact of the SSC and Certification process).
19.	Incident response plan (including service management relationship information)	“Email” .doc – summarises SNZ responses to evidence request Cloud Computing Information Security and Privacy Considerations-Loomio.doc	SNZ standard incident management process - http://tematapihi.stats.govt.nz/articles_landing_pages/Security/Reporting%20a%20Security%20Incident.aspx contact@loomio.org GCIO Q12 Response*: Loomio will promptly notify SNZ in the event of any security breach of the Service resulting in an actual or reasonably suspected unauthorised disclosure of Customer Data.*	Service Management section of SSC states: *The relationship with Loomio was managed directly by Census (*[redacted] [redacted] This was deemed acceptable by the SM in the SSC. GCIO Q12 Response: *Loomio will promptly notify SNZ in the event of any security breach of the Service resulting in an actual or reasonably suspected unauthorised disclosure of Customer Data.* However it is unclear how this will align with the SNZ incident management process in practice.	No. Approval not verified by authorised signoff of SSC or GCIO responses.	• Ensure that an incident response plan is documented, appropriately signed off and stored (as it is included within the SSC&A).
20.	Disaster recovery plan	“Email” .doc – summarises SNZ responses to evidence request	Loomio are subscribed to Heroku’s ‘Continuous Protection’ service (live replication). With ‘Continuous Protection’ every change to data is written to write-ahead logs, which are shipped to multi-datacenter, high-durability storage. In the unlikely event of unrecoverable hardware failure, these logs can be automatically 'replayed' to recover the data to within seconds of its last known state. https://devcenter.heroku.com/articles/pgbackups	GCIO Q80: The Agency will need to implement a data backup strategy to ensure they can recover from an incident that leads to data loss or corruption. These have been included in the controls identified within the Risk Assessment (C12 Backups, C13 Disaster Recovery), as being effective. This was deemed acceptable by the SM in the SSC.	No. Approval not verified by authorised signoff of RA, GCIO responses or SSC.	• Ensure that a disaster recovery plan is documented, appropriately signed off and stored (as it is included within the SSC&A).
21.	System security plan	“Email” .doc – summarises SNZ responses to evidence request	Does not exist	Not evidenced. This is a NZISM requirement for all systems to be covered, either separately or within a higher level SecPlan (5.1.8.C.01).	No.	• Ensure the system / service is covered in a System Security Plan, either separately or at a higher level (as it is a required artefact of the SSC).

Table 8 Phase 3 documented evidence summary – Agriculture Online, OCS Online Collection System, provided 19/06/2016

Evidence number	Evidence requested	Title of document(s) provided as supporting evidence	SNZ response email	Axenic comments (Italics quoted from evidence)	Acceptability	Recommendations
1.	System Security Certification and Accreditation document (approved/signed copy)	Certification and Accreditation - Agriculture Survey Online.docx	Attached	SSC&A is dated 16/07/2015 Prepared by Security Manager (Certification Authority) for Business Owner and CTO (Accreditation Authority). Unsigned. Valid for 2 years. Evaluated to NZISM V2.3 2015 when documented C&A process is to Nov 2014 V2.1.	No. Approval not verified by authorised signoff if the SSC&A.	• Complete consistent documentation, such as an SSC&A document, for all Certification and Accreditation activities. • Ensure that this formal document is appropriately completed, signed off and stored.

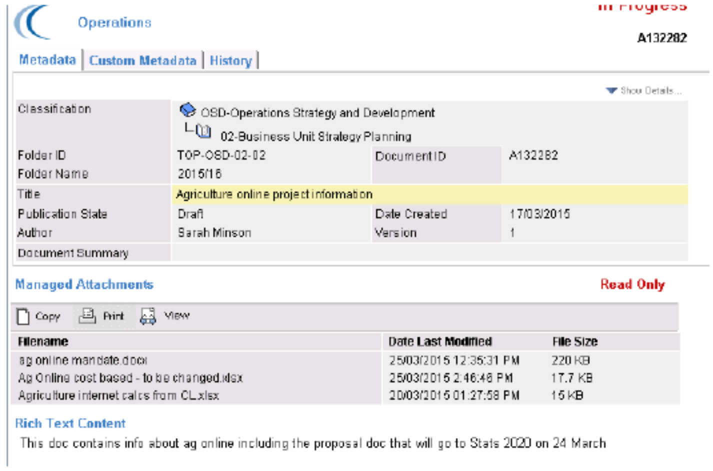
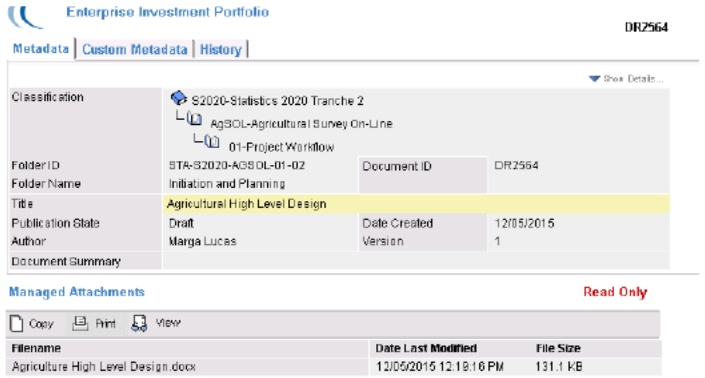
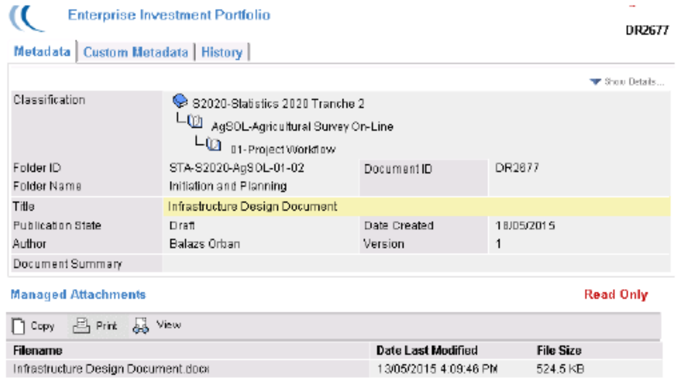
Evidence number	Evidence requested	Title of document(s) provided as supporting evidence	SNZ response email	Axenic comments (Italics quoted from evidence)	Acceptability	Recommendations
				SSC&A document states a cloud based risk assessment is not required as the Cloud Service CWP is an all of government service hosted in the government IaaS.		
2.	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
3.	Security architecture review document	SNZ response email	Refer Security Architecture Review section of the System Security Certificate: The system design was reviewed by the Security Architect with the following observations: *I have reviewed the architecture and implementation documentation, and have also reviewed the separate Software*	The security architecture of the solution was reviewed by the SNZ Security Architect and found to be complete, as stated in the C&A document. This was assessed to meet the appropriate level of assurance against SNZ risk appetite and minimum security controls by the SM in the SSC&A document.	No. Approval not verified by authorised signoff of SSC&A.	• Ensure a System (Security) Architecture review exists for all Certification and Accreditation activities (as it is assessed as part of the Certification process).

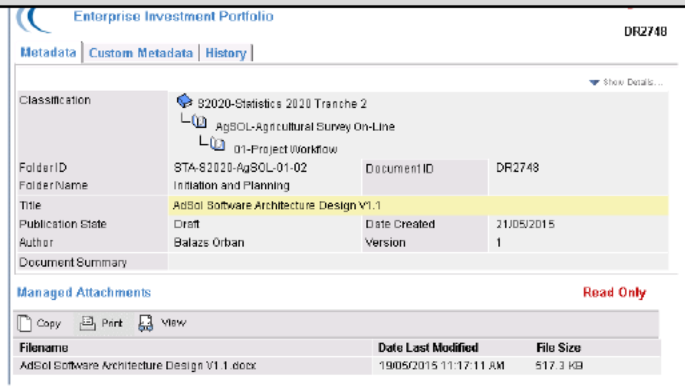
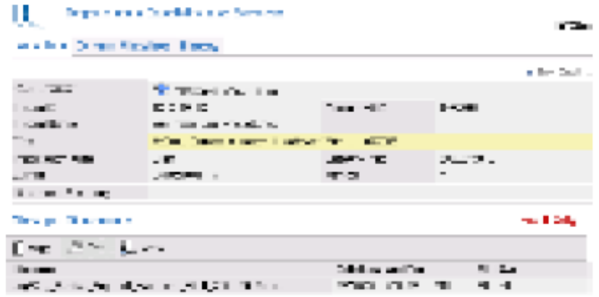
Evidence number	Evidence requested	Title of document(s) provided as supporting evidence	SNZ response email	Axenic comments (Italics quoted from evidence)	Acceptability	Recommendations
			Architecture Design document. In addition I have been involved with the project from vendor solution assessment, through risk assessment and solution architecture design. *My assessment is that the architecture of the solution and its implementation is appropriate for securing the information classification being managed.* --- [redacted] Kaihoahoa Haumarutanga / Hoahoanga Hinonga / Tatauranga Aotearoa Security Architect | Enterprise Architecture			• Ensure that this review is appropriately documented if required and also stored.
4.	Privacy impact assessment (if the system contains private data)	SNZ response email	Refer PIA section of the System Security certificate. Combined with security risk assessment as system. The Statistics NZ Privacy Officer reviewed this decision along with the survey contents and agreed with the panel that a separate PIA was not required.	Classification rating was In Confidence, according to the SNZ RA (which used SIGS classification guidelines which have been superseded as of PSR release of December 2014, although scale remains the same). PIA was determined to not be necessary as a separate risk assessment by the SNZ Privacy Officer, as no completed survey forms were being stored outside SNZ. SM agreed with this decision in the SSC&A.	No. Approval not verified by authorised signoff of the SSC&A or RA.	• Ensure the decision whether or not to conduct a PIA is made by a Privacy professional, and is formally agreed and recorded/stored. • Ensure that a PIA is conducted whenever a system contains private data. This is required by the Certification process.
5.	Security risk assessment and remediation plan (approved/signed copies)	Risk Assessment - AgSOL - Agricultural Survey Online.docx CWP - ICT Risk Assessment – FINAL.docx CWP - Security Risk Management Plan FINAL.docx	Attached, also refer to CWP ICT risk assessment and remediation plan.	SNZ RA provided, dated May 2015, unsigned by SM or Business Owner. Risk rating matrix differs from the SNZ Risk rating tool and Risk Assessment process documentation. Leads to risks being rated at levels inconsistent with the organisation scale. The Business Owner is identified in the SSC as being responsible for ensuring all identified controls are managed and remain in place during the life of the system, however the risks do not appear to have been entered into a risk register for the project/system or ICT operations risk register.	No. Approval not verified by authorised signoff	• Ensure that a consistent risk rating matrix is used in all risk assessments. • Ensure that risk assessments are appropriately signed off and recorded/stored. • Ensure all identified residual risks which are outside SNZ appetite, after control effectiveness has been verified, are centrally recorded/stored to enable appropriate management. This is required by the Certification process.
6.	System classification (including information classification)	SNZ response email	IN-CONFIDENCE	Classification rating was stated as In Confidence, according to the SNZ RA.	No. Approval not verified by authorised signoff of the RA.	• Ensure that information classifications are consistently applied for all SNZ data. • Ensure that all project documentation has a consistent description and classification of the data involved. This is required by the Certification process. • Ensure that a consistent data classification policy is in use at SNZ.
7.	Risk acceptance and any exemptions required	SNZ response email	Business owner sign-off of system security certificate.	The RA has not undergone formal signoff, and acceptance of the risks by the business owner has not been provided. Business owner may also be incorrect as Sarah Minson was not identified in the authorisation table, and above the risk table, an incorrect initiative was identified (Azure / Single Sign On).	No. Approval not verified by authorised signoff of the SSC&A or RA.	• Ensure there is appropriate Business Owner risk ownership. This can be done by ensuring the Business Owner has signed off the RA, SSC&A and SSC. • Ensure the appropriate Business Owner is identified in the centrally managed risk register.

Evidence number	Evidence requested	Title of document(s) provided as supporting evidence	SNZ response email	Axenic comments (Italics quoted from evidence)	Acceptability	Recommendations
						• Ensure any exemptions to SNZ policy are appropriately signed off, recorded, and managed. This is required by the Certification process.
8.	Excerpt of risks entered in to the ICT operations risk register for the project/system	SNZ response email	Does not exist.	Although 5 risks were identified in the Security and Privacy Risk assessment in May 2015, it appears that as the residual ratings were not entered into the ICT operations risk register for the project/system, even though one of the residual ratings remained High (R4). This means that the risks identified are not able to be easily reassessed if the environment changes, or should current controls become less effective. The result is that the SSC could be misleading as the effectiveness of the current controls has not been validated and so the risk ratings may be more or less than assessed. This could also negatively impact recertification activities if the control effectiveness is not based on the inherent risk rating.	No.	• Ensure all identified residual risks which are outside SNZ appetite, after control effectiveness has been verified, are centrally recorded/stored to enable appropriate management. • Ensure the appropriate business owner is identified in the centrally managed risk register. • Ensure that the residual risks have appropriate security controls (with owners identified), to ensure ratings are accurate over time.
9.	[redacted]	[redacted]	[redacted] 	[redacted]	[redacted]	[redacted]
10.	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
11.	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Evidence number	Evidence requested	Title of document(s) provided as supporting evidence	SNZ response email	Axenic comments (Italics quoted from evidence)	Acceptability	Recommendations
				[redacted]		[redacted]es are appropriately stored.
12.	GCIO cloud considerations – Completed responses and evaluation from SNZ on these responses	SNZ response email	Does not exist. Reliance placed on DIA certification of the common web platform.	DIA certification of CWP was not provided, though the SSC&A states that this document has been reviewed by SNZ. SSC&A document was not signed, and GCIO cloud considerations was deemed not required. However, Agencies must complete the GCIO Cloud Risk Assessment Tool and Endorsement for all-of-government cloud services[4] (e.g. common capabilities).	No. Approval not verified by authorised signoff of the SSC&A.	• Complete consistent documentation, such as the GCIO Cloud Computing Information Security and Privacy Considerations document, for all cloud related activities/projects. This includes AoG common capabilities. • Ensure that the responses are evaluated as to suitability to SNZ. • Ensure that this formal document is appropriately signed off and stored.
13.	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
14.	Endorsement form sent to ICTAssurance (approved/signed copy)	SNZ response email	Does not exist.	SSC&A document states that this is not required. However, Agencies must complete the GCIO Cloud Risk Assessment Tool and Endorsement for all-of-government cloud services.	No.	• Ensure that there is a process for completing and sending Endorsement forms to ICTAssurance. This would follow on from the Accreditation process. • Ensure that this formal document is appropriately signed off and stored.

[4] ICT Govt NZ site FAQ page, Q4. https://www.ict.govt.nz/guidance-and-resources/information-management/requirements-for-cloud-computing/faqs-for-cloud-risk-assessment/#Cloud

Evidence number	Evidence requested	Title of document(s) provided as supporting evidence	SNZ response email	Axenic comments (Italics quoted from evidence)	Acceptability	Recommendations
15.	Business case – (approved/signed copy)	SNZ response email	 Operations In Progress A132282 Metadata | Custom Metadata | History | Show Details... Classification: OSD-Operations Strategy and Development 02-Business Unit Strategy Planning Folder ID: TOP-OSD-02-02 — Document ID: A132282 Folder Name: 2015/16 Title: Agriculture online project information Publication State: Draft — Date Created: 17/03/2015 Author: Sarah Minson — Version: 1 Document Summary: Managed Attachments — Read Only Copy Print View Filename — Date Last Modified — File Size ag online mandate.docx — 25/03/2015 12:35:31 PM — 220 KB Ag Online cost based - to be changed.xlsx — 25/03/2015 2:46:48 PM — 17.7 KB Agriculture internet calcs from CL.xlsx — 20/03/2015 01:27:58 PM — 15 KB Rich Text Content This doc contains info about ag online including the proposal doc that will go to Stats 2020 on 24 March	Screen shot shows that a business case document appears to exist at SNZ. Content of this document is unknown. Approval is assumed due to project and contracts going ahead with Silverstripe and DIA (confirmed via list of agencies using CWP on the ICT.govt website).	Yes. However, approval was not verified by authorised signoff of the business case..	• Ensure that a formal business case document is appropriately signed off and stored (as it is a required artefact of the SSC).
16.	Design and configuration documentation – (approved/signed copy)	SNZ response email	 Enterprise Investment Portfolio DR2564 Metadata | Custom Metadata | History | Show Details... Classification: S2020-Statistics 2020 Tranche 2 AgSOL-Agricultural Survey On-Line 01-Project Workflow Folder ID: STA-S2020-AGSOL-01-02 — Document ID: DR2564 Folder Name: Initiation and Planning Title: Agricultural High Level Design Publication State: Draft — Date Created: 12/05/2015 Author: Marga Lucas — Version: 1 Document Summary: Managed Attachments — Read Only Copy Print View Filename — Date Last Modified — File Size Agriculture High Level Design.docx — 12/05/2015 12:19:16 PM — 131.1 KB  Enterprise Investment Portfolio DR2677 Metadata | Custom Metadata | History | Show Details... Classification: S2020-Statistics 2020 Tranche 2 AgSOL-Agricultural Survey On-Line 01-Project Workflow Folder ID: STA-S2020-AgSOL-01-02 — Document ID: DR2677 Folder Name: Initiation and Planning Title: Infrastructure Design Document Publication State: Draft — Date Created: 18/05/2015 Author: Balazs Orban — Version: 1 Document Summary: Managed Attachments — Read Only Copy Print View Filename — Date Last Modified — File Size Infrastructure Design Document.docx — 13/05/2015 4:09:46 PM — 524.5 KB	Screen shots appear to show three Architecture documents last updated in May 2015: High level design, Infrastructure design and Software Architecture Design. These documents were not provided as evidence, so their status (draft, final) and approval is unconfirmed.	No. Although the architecture documents appear to exist, their content and authorisation is unconfirmed.	• Ensure that a formal design and configuration document is appropriately signed off and stored (as it is a required artefact of the SSC). Exception is when there are no SNZ specific design components required or not deemed as required by the Security team.

Evidence number	Evidence requested	Title of document(s) provided as supporting evidence	SNZ response email	Axenic comments (Italics quoted from evidence)	Acceptability	Recommendations
			 Enterprise Investment Portfolio DR2748 Metadata | Custom Metadata | History Show Details... Classification: S2020-Statistics 2020 Tranche 2 / AgSOL-Agricultural Survey On-Line / 01-Project Workflow Folder ID: STA-S2020-AgSOL-01-02 Document ID: DR2748 Folder Name: Initiation and Planning Title: AdSol Software Architecture Design V1.1 Publication State: Draft Date Created: 21/05/2015 Author: Balazs Orban Version: 1 Document Summary Managed Attachments Read Only Copy Print View Filename: AdSol Software Architecture Design V1.1.docx Date Last Modified: 19/05/2015 11:17:11 AM File Size: 517.3 KB			
17.	NZISM controls compliance - (all applicable controls and how compliance rating was determined)	NZISM v2.3 Compliance – AgSOL.xlsx	Attached.	Spreadsheet provided summarizing the NZISM controls which are deemed relevant for this initiative. All relevant tabs and NZISM controls have been summarised to the SSC&A, in the NZISM Controls Compliance section, and the section marked as complete.	No. Approval not verified by authorised signoff of SSC&A.	• Ensure all applicable security controls from the SNZ RA are mapped to NZISM security controls to measure NZISM compliance. • Ensure the document which maps security controls to NZISM compliance is appropriately signed off and stored (e.g. in a RA, Controls catalogue).
18.	Standard Operating Procedures	SNZ response email		The screen shot of the handover document for AgSOL shows that this document was last modified 28/5/2015. The SSC&A indicates that the SOPs have not been evidenced or reviewed. Although the handover document exists, it lacked support and delivery requirement detail.	No. The Certification process states Standard Operation Procedures will always be measured, completed and documented prior to the audit phase.	• Ensure that standard operating procedures are documented, appropriately signed off and stored (as it is a required artefact of the SSC and Certification process).
19.	Incident response plan (including service management relationship information)	SNZ response email	SNZ standard incident management process - http://tematapihi.stats.govt.nz/articles_landing_pages/Security/Reporting%20a%20Security%20Incident.aspx	SSC&A NZISM Controls Compliance section, Chapter 7: IS Incidents, is deemed to be not relevant, and is not showing in this section at all. The SSC&A Incident Response (IRP) section appears to not have been completed, as the standard SNZ Incident Management Process will be used. The RA states that there is a current control for Incident reporting & response plan which is supposed to include vendor responsibilities, however no details of how this would be achieved were provided as evidence.	No. Approval not verified by authorised signoff of SSC&A.	• Ensure that an incident response plan is documented, appropriately signed off and stored (as it is included within the SSC&A).
20.	Disaster recovery plan	SNZ response email	Does not exist	The SSC&A Disaster Recovery section states there is no formal DR or BC plan. The fall-back position is stated as using paper based surveys and responses.	No. Approval not verified by authorised signoff of SSC&A.	• Ensure that a disaster recovery plan is documented, appropriately signed off and stored (as it is included within the SSC&A).
21.	System security plan	SNZ response email	Does not exist	Not evidenced. This is a NZISM requirement for all systems to be covered, either separately or within a higher level SecPlan (5.1.8.C.01).	No.	• Ensure the system / service is covered in a System Security Plan, either separately or at a higher level (as it is a required artefact of the SSC).

4.3 Audit plan

This audit was separated into three major phases, and several sub-stages of activities, which are summarised here.

Phase 1

- Initiation

  Opening meeting(s) with SNZ project manager [redacted].

  Reviewing of relevant documentation which details SNZ's cloud adoption practices. Including but not limited to: policies, standards, guidelines, processes and procedures, risk management framework and process, risk assessment process, certification and accreditation process, security practices and processes executed during a project's lifecycle, staff awareness and training.

  Identification of stakeholders to interview as part of Phase 2.

- Planning

  Development of a plan to complete the audit of SNZ's cloud adoption processes and practices based on the information provided in the initiation.

  The plan will allow for examination to follow a structured approach, covering: application and effectiveness of SNZ practices for adopting cloud services (including risk assessment, risk management, certification and accreditation), responsibilities for sign off/approvals, staff awareness, sampling of up to four representative projects for adherence to agency processes.

  Development of interview questionnaires for auditees.

  Agreement with SNZ project management to present and agree the approach, scope and timing of the audit work programme for Phase 2.

Phase 2

- Process review

  Review of the intent and implementation of the practices and procedures identified during Phase 1.

  Including: organising and conducting interviews with the identified auditees, collecting information and evidence on actual practices on risk assessment and certification and accreditation.

  Analysis of responses and evidence to assess intent and implementation of SNZ cloud service practices.

  Consideration of the role SNZ's security team in the cloud adoption process.

  Documentation of findings with reference to GCIO and PSR guidance and requirements, and make recommendations for uplift if required.

  Present this draft report to Internal Audit and the CTO for feedback. Incorporate feedback as required and appropriate.

Phase 3

- Project review

Conduct a review of up to four sample representative projects, selected at random by the Auditors and agreed with SNZ, to ascertain the effectiveness of SNZ cloud service implementation practices, and identify any gaps/weaknesses in these practices.

Document the findings and make recommendations for capability uplift if required.

Incorporate these findings into the existing draft report from Phase 2.

Present this updated draft report to Internal Audit and the CTO for feedback. Incorporate feedback as required and appropriate.

Project close

- Project close

  Axenic Limited representatives will meet with SNZ stakeholders to discuss the findings for sign-off of the report.

Table 9 SNZ audit schedule

Time allocation	Stage	Date	Activity
Phase 1 (~3 days)	Initiation	23 May 2016	Opening meeting: V.C., J.S, L.Z., K.F. Identification of stakeholders for Phase 2. Documentation request provided to SNZ, with due date 25 May.
	Initiation	26-27 May 2016	All documentation requested for review which has been provided, is reviewed.
	Planning	30-31 May 2016	Creation of audit plan. Creation of interview questionnaires for stakeholders identified.
	Planning	1 June 2016	Sharing of audit plan with SNZ to obtain agreement to agree approach, scope and timing of Phase 2.
Phase 2 (~9 days)	Process review	1 -2 June 2016	SNZ stakeholder interviews organised by V.C. Interviews conducted by Auditors. Analysis of responses and evidence provided. Internal QA of report.
	Process review	7-13 June 2016	Interviews conducted by Auditors.
	Process review	7-14 June 2016	Consolidation and analysis of responses and evidence provided. Internal QA of report.
	Process review	16 June 2016	Report draft shared. Updated draft report shared with V.C. and C.B for feedback. Due back to Axenic no later than 17 June 2016.

Phase 3 (~5 days)	Project review	15 June 2016	Sample projects selected by Auditors for review, agreed by SNZ. Evidence of SNZ implementation practices being followed for each project to be provided to Axenic by CoB 17 June 2016.
	Project review	17 -20 June 2016	Sample (up to) 4 projects reviewed. Feedback from draft report incorporated as appropriate. Internal QA of report.
	Project review	22 June 2016	Report draft shared. Updated draft report shared with V.C. and C.B for feedback. Due back to Axenic CoB 23 June for incorporation.
	Project close	23-24 June 2016	Finalising of report. Presentation of updated draft report and findings from Axenic to SNZ identified stakeholders for sign-off.

Please note that the actual dates within the audit schedule were dependent upon the prerequisite activities and evidence being available and provided.

Any evidence which was not able to be provided within this timeframe may have been excluded from the findings of the audit report.

4.4 Audit interview plan

The following table presents the interview plan that was conducted and scheduled by SNZ (V.C.), in order to meet auditing requirements. This included creating calendar appointments that align to the audit schedule and booking facilities (such as meeting rooms, video conferencing etc.). The table references the detailed audit findings set out in section 3.13.2.

Table 10 Audit interview plan

Estimated time required	Assessor	Reference	Activity	Auditee(s)
2 hours	L.Z. K.F.	SNZ01 SNZ02 SNZ05 SNZ08 SNZ09 SNZ10 SNZ15 SNZ17 SNZ20 SNZ22	Interview Chief Technology Officer (CTO/CISO) about: • Security policies and Risk Management • Organisation of information security and privacy • Asset management • Access control responsibilities • Access control – System and application access control • Cryptography • Operations security – Information systems audit • System acquisition, development and maintenance	[redacted]

Estimated time required	Assessor	Reference	Activity	Auditee(s)
			- Information security aspects of business continuity - Compliance – Information security reviews	
2 hours	L.Z. K.F.	SNZ01 SNZ02 SNZ04 SNZ05 SNZ08 SNZ09 SNZ10 SNZ11 SNZ12 SNZ13 SNZ14 SNZ15 SNZ16 SNZ17 SNZ18 SNZ19 SNZ20 SNZ21 SNZ22	Interview Security Manager (ITSM) about: - Security policies and Risk Management - Organisation of information security and privacy - Asset management - Access control responsibilities - Access control – System and application access control - Cryptography - Operations security - Operational procedures and responsibilities - Operations security – Backup - Operations security – Logging and monitoring - Operations security – Technical vulnerability management - Operations security – Information systems audit - Communications security - System acquisition, development and maintenance - Supplier relationships - Information security incident management - Information security aspects of business continuity - Compliance – Legal and contractual - Compliance – Information security reviews	[redacted]
30 minutes	L.Z. K.F.	SNZ01 SNZ02	Interview DCE Organisational Capability & Services (CSO/Chief Privacy Officer) about: - Security policies and Risk Management - Organisation of information security and privacy	[redacted]
1 hour	L.Z. K.F.	SNZ01 SNZ04 SNZ07 SNZ16	Interview Manager Information Management and/or Senior Manager Standards and Design (MIM) about: - Security policies and Risk Management - Asset management - Access control – User access management	[redacted]

Estimated time required	Assessor	Reference	Activity	Auditee(s)
			• Communications security	
1 hour	L.Z. K.F.	SNZ02 SNZ09 SNZ11 SNZ17 SNZ22	Interview Director Enterprise Programme Office (EPO) about: • Organisation of information security and privacy • Access control - System and application access control • Operations security - Operational procedures and responsibilities • System acquisition, development and maintenance • Compliance – Information security reviews	[redacted]
30 minutes	L.Z. K.F.	SNZ03 SNZ08	Interview Chief People Officer (HR) about: • Human resource security • Access control responsibilities	[redacted]
1 hour	L.Z. K.F.	SNZ01 SNZ15 SNZ21	Interview Risk Manager (RM) about: • Security policies and Risk Management • Operations security – Information systems audit • Compliance – Legal and contractual	[redacted]
2 hours	L.Z. K.F.	SNZ09 SNZ10 SNZ11 SNZ12 SNZ13 SNZ14 SNZ18 SNZ19 SNZ20 SNZ21	Interview Senior Manager IT Operations (IT Ops & Svcs) about: • Access control - System and application access control • Cryptography • Operations security - Operational procedures and responsibilities • Operations security – Backup • Operations security – Logging and monitoring • Operations security – Technical vulnerability management • Supplier relationships • Information security incident management • Information security aspects of business continuity • Compliance – Legal and contractual	[redacted]
2 hours	L.Z. K.F.	SNZ05 SNZ11 SNZ14 SNZ16 SNZ17	Interview Manager IT Sourcing and Supply (IT AM/SR) about: • Asset management • Operations security - Operational procedures and responsibilities	[redacted]

Estimated time required	Assessor	Reference	Activity	Auditee(s)
		SNZ18 SNZ19 SNZ21	• Operations security – Technical vulnerability management • Communications security • System acquisition, development and maintenance • Supplier relationships • Information security incident management • Compliance – Legal and contractual	
30 minutes	L.Z. K.F.	SNZ06 SNZ07 SNZ13	Interview Manager Service Delivery (UAM) about: • Access control and Business requirements • Access control – User access management • Operations security – Logging and monitoring	[redacted]
30 minutes	L.Z.	SNZ16 SNZ18 SNZ21	Interview Legal Counsel (LC) about: • Communications security • Supplier relationships • Compliance – Legal and contractual	[redacted]
30 minutes	L.Z. K.F.	SNZ18 SNZ19	Interview the Privacy Officer (PO) about: • Supplier relationships • Information security incident management	[redacted]
30 minutes	L.Z. K.F.	SNZ06 SNZ07 SNZ12 SNZ22	Interview the Senior Manager Operations Strategy and Development (ECP – Salesforce) about: • Access control and Business requirements • Access control • Operations security – Backup • Compliance – Information security reviews	[redacted]
30 minutes	L.Z. K.F.	SNZ12 SNZ15 SNZ22	Interview the Programme Manager Data Processes and Infrastructure (ECP – PM) about: • Operations security – Backup • Operations security – Information systems audit • Compliance – Information security reviews	[redacted]

This page has been intentionally left blank.