



Internal Audit Review of Access to Statistical Data within IT Systems at Statistics New Zealand

Client	Statistics New Zealand
Document ID	STATS2015001
Author	Axenic Limited
Date Published	24 June 2015
Classification	In Confidence

Document Control

Revision History

Version	Date	Author	Description
1.0	24 June 2015	[REDACTED]	Final draft report

Release Approval

Approved for release to client	Signature	Date
[REDACTED]	[REDACTED]	24 June 2015

Distribution

Name	Role	Organisation
[REDACTED]	Internal Auditor	Statistics New Zealand
[REDACTED]	Chief Technology Officer	Statistics New Zealand
[REDACTED]	Manager Standards and Design	Statistics New Zealand
[REDACTED]	Security Manager	Statistics New Zealand
[REDACTED]	Manager Information Management	Statistics New Zealand

Document acceptance

Accepted by	Signature	Date
[REDACTED]		

Copyright © Axenic Ltd 2015. This document contains proprietary information and is provided to Statistics New Zealand for internal use only. It may not be reproduced or disclosed to anyone except for employees of the Statistics New Zealand without obtaining written permission from Axenic Ltd. The recipient by retaining and using this document agrees to the above restrictions and shall protect the document and information contained in it from loss, theft and misuse.

This document has been prepared at the request of the Statistics New Zealand in accordance with the terms of the contract between Axenic and Statistics New Zealand. Other than our responsibility to the Statistics New Zealand, neither Axenic nor any member or employee of Axenic undertakes responsibility arising in any way from reliance placed by a third party on this document. Any reliance placed is that party's sole responsibility.

Unless expressly stated otherwise, the document templates and methods used to complete this document are the pre-existing intellectual property of Axenic Ltd.

Table of Contents

Section 1. Overview	5
1.1. Background	5
1.2. Executive Summary	5
1.3. High Level Summary	8
1.4. High Level Findings in Relation to the PSR	9
Section 2. Audit Plan	16
2.1. Purpose of the Engagement	16
2.2. Audit Scope	16
2.3. Audit Objectives	16
2.4. Audit Criteria	16
2.5. Audit Processes and Methods	16
2.6. SNZ Project Manager	17
2.7. Auditors	17
2.8. Auditees	17
2.9. Audit Process	18
Section 3. Audit Findings	19
3.1. Audit Finding Ratings	19
3.2. Detailed Audit Plan and Assessment Findings	20
Section 4. Audit Appendices	33
4.1. Appendix A - Reference Documentation Provided	33
4.2. Appendix B - Audit Schedule	40
4.3. Appendix C - Audit Interviews	41

Section 1. Overview

1.1. Background

Statistics New Zealand (SNZ) collects data from respondents to surveys and other sources. The information collected can include personal information or be commercially sensitive or confidential and must be appropriately protected from unauthorised access and disclosure.

Its statistical analysts have access to both respondent and intermediate data as well as statistical output data prior to publication. Other staff including IT administrators, developers, publishing assistants and statistical methodologists may have access to the collected data and outputs.

SNZ has concern that instances of statistical data may have been copied or moved to unauthorised or insecure locations within SNZ's ICT environment for the convenience of staff. This belief is supported by the knowledge that data are not consistently classified and managed.

The lack of appropriate information management within Statistics exposes it to a number of risks including:

- possible disclosure of respondent data;
- loss of access to collected data in the event of a disaster;
- damage to its reputation due to inaccurate statistical output;
- damage to its reputation as a responsible data custodian; and
- fraud through unauthorised use of data and statistical outputs.

1.2. Executive Summary

This audit has been undertaken by Axenic Limited to review the information management framework, policies and practices at SNZ, in relation to access to statistical data within IT systems. 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 and the findings are presented with reference to the New Zealand Protective Security Requirements (PSR)¹.

[Redacted text block]

[Redacted text block]

¹ <http://www.protectivesecurity.govt.nz/>

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted content]

1.3.High Level Summary

Figure 1 and Table 1 below present the summary of audit findings in relation to the number of mandatory requirements of the Protective Security Requirements (PSR²) policy framework, to enable Statistics New Zealand to understand its performance against this compulsory government framework.



Figure 1 - Overview of PSR ratings

Figure 1 above provides a visual representation of the overall findings against the 29 requirements of the PSR. Note that requirements beyond the scope of this review are shown in grey.

² <http://www.protectivesecurity.govt.nz/>

1.4.High Level Findings in Relation to the PSR

Table 1 - High level findings in relation to PSR

PSR requirement	Description	Rating	High level findings	Reference
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

PSR requirement	Description	Rating	High level findings	Reference
[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]	[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]	[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]	

Section 2. Audit Plan

2.1. Purpose of the Engagement

Statistics New Zealand (SNZ) engaged Axenic Limited to perform a review of its information management framework, policies and practices, in order to assure the Government Statistician and Chief Executive of SNZ that it has appropriate frameworks and controls in place to manage access to statistical information by its staff and others.

2.2. Audit Scope

The scope of this audit plan included:

- The information management framework - policies, practices and procedures;
- The staff and contractors of SNZ - statistical analysts, IT administrators, developers, publishing assistants and statistical methodologists; and
- SNZ's ICT environment.

2.3. Audit Objectives

The objective of this audit was to examine SNZ's information management framework, policies and practices and evaluate:

- The application and effectiveness of the SNZ information management framework as it applies to statistical data;
- The ownership and custodianship of statistical data;
- Policies and practices for managing of statistical data and information;
- Staff awareness of policies and procedures for managing statistical data and information;
- Tools to facilitate effective management of statistical data and information; and
- Lifecycle management of statistical data and information.

2.4. Audit Criteria

This audit referenced the following standards, frameworks or requirements:

- SNZ's own information management framework, policies, and practices;
- ISO/IEC 27001:2013; and
- New Zealand Protective Security Requirements (PSR) and Information Security Manual (NZISM) 2015 v2.3.

2.5. Audit Processes and Methods

Documentation reviews

Documentation reviews were 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,
- certification and accreditation documentation,
- custodian lists; and
- organisational charts.

A full list of documents used in support of this review is detailed in Section 4 Audit Appendices.

Interviews

These were conducted on site at SNZ premises in Wellington, and included; random sampling, role/responsibility specific interview questionnaires and discussions. All interviewees are identified in section 2.8 Auditees.

Observations

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

2.6.SNZ Project Manager

- [REDACTED]

2.7.Auditors

Axenic Quality Assurance and Oversight

- [REDACTED]

Lead Auditor(s)

- [REDACTED]
- [REDACTED]

Auditors

- [REDACTED]

2.8.Auditees

The following table lists the identified roles or functions that were interviewed for this audit.

Table 2 - Auditee table

Role	Name
Manager Information Management	[REDACTED]
Manager Security Office / Information Technology Security Manager	[REDACTED]
HR Manager	[REDACTED]
Manager IT Operations and Services	[REDACTED]
Asset Manager - IT	[REDACTED]
User Access Manager	[REDACTED]
Manager Service Delivery	[REDACTED]
Manager Supplier Relationships - IT	[REDACTED]
Internal Auditor	[REDACTED]
Digital Publishing Manager	[REDACTED]

Role	Name
Statistical Analyst	
Service Delivery Consultant	
Manager – National Accounts	
Manager – Balance of Payments, Trade & Business Infrastructure	
Senior Advisor – Organisation Strategy & Performance	
DGS & DCE Customer Strategy & Delivery	

2.9. Audit Process

This audit process was based on the guidelines for auditing management systems ISO/IEC 19011:2011 and ISO/IEC 27007. The stages for this audit were as follows:

Phase 1

- Initiation: Including review of relevant documentation, confirmation of drivers and areas of concern for the audit to address; and
- Planning: Including the audit plan, interview questionnaire, agreement of approach, scope and timing for phase 2.

Phase 2

- Audit execution: Including consolidating the audit findings and drafting the audit report;
- Presentation of the draft audit report: Including meeting with SNZ stakeholders to discuss the findings; and
- Completion of the finalised report, plus assistance to achieve appropriate SNZ sign off.

Section 3. Audit Findings

3.1. Audit Finding Ratings

The findings of this audit were categorised into one of four ratings:

Table 3 - Audit findings and rating scale

Rating	Description
Effective	This indicates that there is clear intent to meet the standard, the means to support the control objectives have been implemented and appear to be effective .
Partially Effective	This indicates that there is some intent to meet the standard, the means to support the control objectives are partially implemented or are partially effective .
Not Effective	This indicates that there is no clear intent to meet the standard, or no means implemented to support the control objectives, or the means are not effective .
Not Reviewed / Out of Scope	This indicates that the control has not been reviewed or is out of scope.

3.2. Detailed Audit Plan and Assessment Findings

Table 4 - Detailed audit plan and assessment findings

ID	Title	Assessment Plan	Comments	Rating	Findings	ISO/IEC 27001:2013 Annex A Controls
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

ID	Title	Assessment Plan	Comments	Rating	Findings	ISO/IEC 27001:2013 Annex A Controls
		• [REDACTED]	[REDACTED]			
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

ID	Title	Assessment Plan	Comments	Rating	Findings	ISO/IEC 27001:2013 Annex A Controls
		<ul style="list-style-type: none"> • [REDACTED] 	[REDACTED]			
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]		[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]		[REDACTED]	[REDACTED]

ID	Title	Assessment Plan	Comments	Rating	Findings	ISO/IEC 27001:2013 Annex A Controls
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

ID	Title	Assessment Plan	Comments	Rating	Findings	ISO/IEC 27001:2013 Annex A Controls
			<ul style="list-style-type: none"> [REDACTED] 			
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]		[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]		[REDACTED]	[REDACTED]

ID	Title	Assessment Plan	Comments	Rating	Findings	ISO/IEC 27001:2013 Annex A Controls
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

ID	Title	Assessment Plan	Comments	Rating	Findings	ISO/IEC 27001:2013 Annex A Controls
		[REDACTED]	[REDACTED]			
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]		[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]		[REDACTED]	[REDACTED]

ID	Title	Assessment Plan	Comments	Rating	Findings	ISO/IEC 27001:2013 Annex A Controls
		<ul style="list-style-type: none"> [Redacted] 				
[Redacted]	[Redacted]	<ul style="list-style-type: none"> [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] 	<ul style="list-style-type: none"> [Redacted] [Redacted] [Redacted] 		[Redacted]	[Redacted]
[Redacted]	[Redacted]	<ul style="list-style-type: none"> [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] 	<ul style="list-style-type: none"> [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] 		[Redacted]	[Redacted]
[Redacted]	[Redacted]	<ul style="list-style-type: none"> [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] 	<ul style="list-style-type: none"> [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] 		[Redacted]	[Redacted]

ID	Title	Assessment Plan	Comments	Rating	Findings	ISO/IEC 27001:2013 Annex A Controls
		<ul style="list-style-type: none"> [REDACTED] 	[REDACTED]			
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]		[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]		[REDACTED]	[REDACTED]

ID	Title	Assessment Plan	Comments	Rating	Findings	ISO/IEC 27001:2013 Annex A Controls
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

ID	Title	Assessment Plan	Comments	Rating	Findings	ISO/IEC 27001:2013 Annex A Controls
		<ul style="list-style-type: none"> [Redacted] 				[Redacted]
[Redacted]	[Redacted]	<ul style="list-style-type: none"> [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] 	<ul style="list-style-type: none"> [Redacted] [Redacted] 	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	<ul style="list-style-type: none"> [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] 	<ul style="list-style-type: none"> [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] 	[Redacted]	[Redacted]	[Redacted]

ID	Title	Assessment Plan	Comments	Rating	Findings	ISO/IEC 27001:2013 Annex A Controls
			<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] 		[REDACTED]	
[REDACTED]	[REDACTED]	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] 	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] 		[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] 	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] 		[REDACTED]	[REDACTED]

ID	Title	Assessment Plan	Comments	Rating	Findings	ISO/IEC 27001:2013 Annex A Controls
SNZ27	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Section 4. Audit Appendices

4.1. Appendix A - Reference Documentation Provided

Table 5 - Reference and evidence documents provided

Item	Title of document or item	Description	Owner	Provided by	Version	Date last updated
1.	Statistics New Zealand Code of Conduct Aug 2009	SNZ Code of Conduct	Unclear	V.C.	None	March 2014
2.	Statistics NZ Access to statistical and corporate data is provided on a need to do the job bases Policy	Statistics NZ Access to statistical and corporate data is provided on a need to do the job bases Policy	Security Office	V.C.	None	22/04/2014
3.	Access to and use of our IT environment is provided on a need to do the job basis Policy	Access to and use of our IT environment is provided on a need to do the job basis Policy	Security Office	V.C.	None	13/05/2014
4.	Statistics NZ User Access to IT Systems and Data Policy	Statistics NZ User Access to IT Systems and Data Policy	CIO, IT Solutions	V.C.	None	17/08/2012
5.	Security and IT Policies_June 2011.	Summary of Security Policies from the Corporate Policies database.	Unclear	V.C.	None	Created 15/08/2012
6.	Statistics NZ Custodian Role and Guidance	Document identifier W1250349.3	Unclear	V.C.	None	Unclear
7.	Statistics NZ Data Integration Policy	Data Integration Policy	Information Management	V.C.	None	25/09/2012
8.	Statistics NZ Information and Data Management Policy	Information and Data Management Policy	Information Management	V.C.	None	07/03/2013

Item	Title of document or item	Description	Owner	Provided by	Version	Date last updated
9.	Statistics NZ Microdata Access Policy	Microdata Access Policy	Manager Client Services and Liaison Collections and Dissemination Group, Integrated Data Division	V.C.	None	05/10/2009
10.	Statistics NZ Policy for the Release of Statistics	Policy for the Release of Statistics	Product Development and Publishing Manager, Collections and Dissemination Group	V.C.	None	09/05/2012
11.	Statistics NZ Policy for the Retention and Preservation of Statistical Data	Policy for the Retention and Preservation of Statistical Data	Information Management	V.C.	None	Under review, due 13/05/2015
12.	Statistics NZ Security Handbook for Managers and Supervisors	Security Handbook for Managers and Supervisors	Security Office	V.C.	None	30/11/2007
13.	Statistics NZ Security Policies Framework	Statistics NZ Security Policies Framework	Security Office	V.C.	None	22/04/2014
14.	Stats ToR - 29-05-2015 11-17	Terms of Reference – upon which the Statement of Work was based.		V.C.	Draft	May/June 2015
15.	Remote Working - Casual Temporary and Emergency Situations Policy	Remote Working – Casual, Temporary and Emergency Situations	Head of Human Resources	V.C.	None	04/11/2013

Item	Title of document or item	Description	Owner	Provided by	Version	Date last updated
16.	Remote Working - Permanent Policy	Remote Working - Permanent Policy	Head of Human Resources	V.C.	None	04/11/2013
17.	Remote Working - Permanent Guidelines	Remote Working - Permanent Guidelines	Manager Human Resources	V.C.	None	07/10/2013
18.	Supporting SNZ documentation V0 2 LE.docx Sec-1 IPSCG 30 April 2015 Minutes Final.docx Sec-2 IPSCG 18 March 2015 Minutes Draft.doc Sec-3 IPSCG 5 February 2015 Minutes Draft.doc Sec-4a Security and Privacy Incident Report IPSaC GG April 2015.docx Sec-4b Security and Privacy Incident Report IPSaC GG March 2015.docx Sec-4c Security Incident Report IPSaC GG Feb 2015.docx Sec-5a Monthly report - Security - May 2015.xlsx Sec-5b Monthly report - Security - Apr 2015.xlsx Sec-5c Monthly report - Security - Mar 2015.xlsx	Requested evidence documents	Information Security Technology Manager	L.E.	Various	Various

Item	Title of document or item	Description	Owner	Provided by	Version	Date last updated
	<p>Sec-6 Certification and Accreditation - Check Point Capsule Workspace - Containerised.docx</p> <p>Sec-7 Security - Process Diagram - System Certification and Accreditation.pdf</p> <p>Sec-8a GCIO Review_Risk Assessment Process - Information Security.pdf</p> <p>Sec-8b GCIO Review_Risk Assessment Process - Risk Assessment Report Template.pdf</p> <p>Sec-8c GCIO Review_Risk Assessment Process - Risk Assessment Report Template.doc</p> <p>Sec-8d GCIO Review_Risk Workshop Guidelines.doc</p> <p>Sec-8e Stats NZ Security Risk Assessment Template.docx</p> <p>Sec-9 Guidelines for Classifying Official Information.pdf</p> <p>Sec-10 Security Newsletter May 2015.pdf</p> <p>Sec-11 Security - Process Diagram - Security Privacy Incident Management.pdf</p> <p>Sec-12 IPSCGG Terms of Reference.doc</p>					

Item	Title of document or item	Description	Owner	Provided by	Version	Date last updated
	Sec-13a Examples of intranet notices to staff on innovation.pdf Sec-13b A4 Strategy poster.pdf Sec-13c Strategic Refresh Narrative .ppt					
19.	Supporting SNZ documentation V0.5 TB and AJ.docx IM-1 Custodian COP_Terms of Reference.docx IM-2 Custodian COP_Comms Planv3.docx IM-3 Consultation with Data Custodians.pdf IM-4 Evidence of review of policies etc.pdf IM-5 Data Management Maturity Assessment.pptx IM-6a Mapping New RM standard May 2014 to Audit Self-Assessment 2012-13 list.docx IM-6b RM Standard Archives NZ May 2014 - Matrix 2015.xlsx IM-7 IM induction process for new starters.docx IM-8 Screenshots of Ako course.docx IM-9a EMAIL A Induction email to contractors and casuals.doc	Requested evidence documents	Manager Information Management	T.B. & A.J.	n/a	n/a

Item	Title of document or item	Description	Owner	Provided by	Version	Date last updated
	IM-9b EMAIL B Induction face to face introduction email.docx IM-9c EMAIL C Induction face to face follow up email.docx IM-10 IM induction record of attendees 2015.xlsx IM-11 Custodian list for COP.xlsx IM-12a Custodial Times May 2015.pdf IM-12b Custodial Times March 2015.pdf IM-12c Custodial Times Feb 2015.pdf IM-13 Example of guidance pack.pdf IM-14 Library brochure - final.pdf IM-15 Data Disposal Process - Sybase databases appraisal and sentencing.pdf IM-16 Record of Disposal Actions - Standalone Sybase Databases - Destruction.pdf IM-17 2013.11.20 - Statistics New Zealand - Census 2013 - 1001079 - FFN - Certificate of Destruction - listing.pdf IM-18 Information Management KPIs.docx					

Item	Title of document or item	Description	Owner	Provided by	Version	Date last updated
	IM-19 Defining Statistics NZ top level Data Management landscape.docx IM-20 Blueprint for Data Management at Statistics New Zealand 3rd version.docx					
20.	Supporting SNZ documentation V0 4 DH.docx	Requested evidence documents	Manager User Access Management	D.H.	n/a	n/a
21.	IT Asset Register Version 3 [01-03-06]_ Retiring Physical Asset.pdf ITS Org Chart.docx Review meeting - Q4 2014 - Q1 2015.pdf STATS NZ Monthly Mobile Report April 2015.pdf Service Review April 2015.pdf Stats_Quarterly Report - 1 Jan-31 Mar 2015_FINAL.PDF WAN Usage Calculations April 2015.xlsx idi-extn-pia-2nd-ed.pdf	Requested evidence documents	Manager – Service Planning and Performance	B.B.	n/a	n/a

4.2. Appendix B - Audit Schedule

Table 6 - Audit schedule

Date	Stage	Activity
2015-06-08	Opening meetings	Present and finalise the audit plan
2015-06-09	Audit execution	Interviews - See proposed audit interview plan below
2015-06-10	Audit execution	Interviews - See proposed audit interview plan below
2015-06-11	Audit execution	Documentation review
2015-06-12	Audit execution	Site visit for observations Documentation review
2015-06-15	Audit execution	Interviews Documentation review
2015-06-16	Audit execution	Interviews Documentation review Consolidating audit findings
2015-06-17	Audit execution	Drafting audit report
2015-06-18	Audit execution	Drafting audit report
2015-06-19	Audit reporting	Drafting audit report
2015-06-22/23	Finalise report	Quality assurance Draft audit report delivery for review
2015-06-25	Finalise report	Receive and incorporate review feedback
2015-06-26	Closing meeting	Delivery and signoff of final report

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

Any evidence that could not be provided within this timeframe may have been excluded from the findings and audit report.

4.3. Appendix C - Audit Interviews

The following table presents the interviews conducted that were scheduled by SNZ (Victoria Craig), in order to meet auditing requirements. The table references the detailed audit plan in section 3.2 above.

Table 7 - Audit interviews

Time and priority	Assessor	Reference	Activity	Auditee(s)
1 hour Priority 1	[REDACTED]	SNZ02, SNZ03, SNZ06, SNZ07, SNZ10, SNZ11, SNZ12, SNZ13, SNZ14, SNZ15, SNZ16, SNZ17, SNZ18, SNZ19, SNZ20, SNZ21, SNZ22, SNZ24, SNZ25, SNZ26, SNZ27.	Interview Manager Security Office / Information Technology Security Manager about: <ul style="list-style-type: none"> • Organisation of information security; • Asset Management; • Access Control; • Cryptography; • Physical and Environmental Security • Operations Security; • Communications Security; • System acquisition, development and maintenance; • Information security incident management; • Information security aspects of business continuity; and • Compliance. 	[REDACTED]
1 hour Priority 2	[REDACTED]	SNZ01, SNZ03, SNZ04, SNZ06, SNZ07, SNZ17.	Interview Manager Information Management about: <ul style="list-style-type: none"> • Security Policies; • Organisation of information security; • Human Resource Security; • Asset Management; and • Operations Security. 	[REDACTED]
1 hour	[REDACTED]	SNZ08,	Interview Manager Service Delivery about:	[REDACTED]

Time and priority	Assessor	Reference	Activity	Auditee(s)
Priority 2	[REDACTED]	SNZ09, SNZ10, SNZ11, SNZ12, SNZ14, SNZ15, SNZ16, SNZ17, SNZ18, SNZ19, SNZ20, SNZ22, SNZ24, SNZ25.	<ul style="list-style-type: none"> • Access Control; • Cryptography; • Physical and environmental security; • Operations Security; • System acquisition, development and maintenance • Information security incident management; and • Information security aspects of business continuity. 	
30 minutes Priority 2	[REDACTED]	SNZ08, SNZ09, SNZ10, SNZ11, SNZ12, SNZ14, SNZ15, SNZ16, SNZ17, SNZ18, SNZ19, SNZ20, SNZ22, SNZ24, SNZ25.	Interview Manager IT Operations and Services about: <ul style="list-style-type: none"> • Access Control; • Cryptography; • Physical and environmental security; • Operations Security; • System acquisition, development and maintenance • Information security incident management; and • Information security aspects of business continuity. 	[REDACTED]
30 minutes Priority 3	[REDACTED]	SNZ05, SNZ07, SNZ23, SNZ25.	Interview Asset Manager IT about: <ul style="list-style-type: none"> • Asset Management; and • Information security aspects of Business Continuity. • Supplier Relationships. 	[REDACTED]

Time and priority	Assessor	Reference	Activity	Auditee(s)
30 minutes Priority 3	[REDACTED]	SNZ26, SNZ27.	Interview Internal Auditor about: <ul style="list-style-type: none"> • Compliance. 	[REDACTED]
30 minutes Priority 3	[REDACTED]	SNZ01.	Interview with DGS&DCE Customer Strategy & Delivery about: <ul style="list-style-type: none"> • Leadership and commitment • Policy • Resources • Monitoring, measurement, analysis and evaluation. 	[REDACTED]
30 minutes Priority 3	[REDACTED]	All	Interview with Balance & Payments, Trade & Business Infrastructure Manager about: <ul style="list-style-type: none"> • Leadership and commitment • Access control • Policy • Resources • Incident Management. 	[REDACTED]
30 minutes Priority 3	[REDACTED]	All	Interview with National Accounts Manager about: <ul style="list-style-type: none"> • Leadership and commitment • Access control • Policy • Resources • Incident Management • Business Continuity • Risk Management. 	[REDACTED]