



Accreditation Audit Tool: Information provider

Legal entity name:

Trading name:

Physical address of audit /
registered business address:

NAIT Location Number:

Audit key contact name
and title:

Audit key contact email:

Auditor(s) name and title:

Date(s) of audit:

Type of Organisation:	Sale Yard	Meat Processor	Farm Management Stock Agent	Farm Management Software Provider
	Farm Management	Transportation Provider		
Type of audit:	Re-accreditation application	Mid-point performance audit	Periodic accreditation audit	
On-site / remote audit	On-site audit	Remote audit		
Information provider activities (record all that apply):	Carrying out animal registration obligations of PICA	Providing animals movement declaration		
	Providing information to NAIT Organisation	Providing notification when NAIT animals die, lost or exported live		
	Registering a person as a PICA or PICA delegate			

✓ Pre-Audit Checklist for Applicant

Audit logistics confirmed.

Audit key contact established, and support staff organised for audit.

NAIT records are up to date, and system available for review.

Policies and Procedures described in Standard(s), NAIT Act and regulations available for review.

Clear and accurate records available for review.

Training records for staff and contractors available for review.

Health and safety induction system for visitors*.

Biosecurity induction system for visitors*.

Health and safety: facilities, yards, sheds, pens, ramps in good condition. No holes, rough edges, protrusions that could cause injury*.

**Only applicable to on-site audits.*



NAIT is an OSPRI programme



ospri.co.nz



0800 482 463

Contents

Glossary and audit framework	3	Section C: Policies and procedures	11	Section E: Business continuity	22
Audit executive summary	4	C01: Quality management	11	E01: Business continuity plan	22
Section A: Facilities, resources and capability	5	C02: Document and data management	12	E02: Business continuity communication plan	22
A01: Accredited organisation application and administration	5	C03: Contract/supplier management	14		
A02: Facility	5	C04: Staff responsibility and appointment	14		
A03: Equipment	6	C05: Staff training	15		
Section B: Collection and submission of NAIT data	7	C06: Internal audit	16		
B01: Interface with NAIT Database	7	C07: Complaints	16		
B02: Electronic data submission and data quality	7	C08: information provider's obligations	17		
B03: Provision of information to PICAs	9	Section D: Data management systems	19		
B04: Data upload failures	10	D01: Information management	19		
B05: Incorrect data	10	D02: NAIT System terms of use	19		
		D03: Data privacy	20		
		D04: Information system back up	20		
		D05: Information system recovery	21		
		D06: IT incident resolution	21		
		D07: Data upload failures and errors	21		

Glossary and audit framework

Glossary

Identification System: A system approved under section 50(1) of the Biosecurity Act 1993, or section 15 of the NAIT Act 2012.

NAIT: National Animal Identification and Tracing

NAIT Act: National Animal Identification and Tracing Act 2012.

NAIT Device: An animal identification device manufactured or supplied in accordance with standards issued.

NAIT Location: As defined in section 5 of the NAIT Act. A place where one or more NAIT animals are kept or held, and which has been registered with and issued with a location identifier by the NAIT organisation.

NAIT Organisation: The organisation designated under the NAIT Act 2012 to implement and operate the national animal identification and tracing scheme.

NAIT Number: The number allocated by the NAIT organisation to identify a particular property where the animals are held.

OSPRI: Operational Solutions for Primary Industries

PICA: A natural person in day-to-day charge of a NAIT animal.

PICA Delegate: A natural person who is nominated and registered, under sections 26 and 27 of the NAIT ACT, to undertake specified procedures and obligations on behalf of a PICA.


Audit Framework

- During the audit each audit criterion is assigned a provisional level of attainment by the auditor:

Level of attainment

FA  Fully Attained

OFI  Opportunity for Improvement

NC  Non-Conformance

NA  Not Applicable

- Audit criterion that are **NC** are assigned a provisional risk level by the auditor.

Level of risk

C  Critical

M  Moderate

L  Other

- Any critical/moderate non-conformances evidence will need to be provided to the audit agencies to review for conformance against the NAIT standards.
- For **Other** risk audit non-conformances, your organisation should take actions to remediate the non-conformances. Evidence to demonstrate these non-conformances are adequately resolved may be reviewed at the next planned audit

Note: Whilst this audit tool references specific sections of the NAIT Standard(s) and NAIT legislation. Accredited organisations should ensure they are aware of their obligations under the entire NAIT Act, regulations and standards which may be sampled during Accreditation audits.

Audit executive summary (this section summarizes the findings from your Audit)

Summary:

Total non-conformances:

Number of critical non-conformances:

Number of other non-conformances:

Number of moderate non-conformances:

Number of opportunities for improvement:

Auditors signed and dated:

Auditors signed and dated:

Section A: Facilities, resources and capability

A01: Accredited organisation application and administration

Criteria	Attainment	Risk	Audit summary and findings
A01-01 Information provider users are registered in the NAIT database (for accredited information provider undergoing an audit). [Section 4.2.1 of IP Standard]	Fully Attained Opportunity for Improvement Non-Conformance Not Applicable	Critical Moderate Other	
A01-02 Contracted Information provider functions on behalf of PICA client(s) align to the requirements in the NAIT Act. [S28 NAIT Act 2012]	Fully Attained Opportunity for Improvement Non-Conformance Not Applicable	Critical Moderate Other	

A02: Facility

A02-01 Suitable IT Security and data privacy policy and procedures are in place to manage NAIT Data. [Section 4.12 of IP Standard]	Fully Attained Opportunity for Improvement Non-Conformance Not Applicable	Critical Moderate Other	
--	--	-------------------------------	--

A03: Equipment

A03-01	Applicants must possess (own, lease or outsource) appropriate equipment for the functions and duties they perform.	Fully Attained	Critical
		Opportunity for Improvement	Moderate
		Non-Conformance	Other
		Not Applicable	
	This includes computer hardware and software capable of processing and submitting NAIT data within the timeframes.		
	prescribed by regulation 10 of the NAIT (Obligations and Exemptions) Regulations 2012.		
	[Section 4.1 of IP Standard]		
A03-02	Applicants must prove that they can upload data to the NAIT information system, in the required format and otherwise in accordance with this standard.	Fully Attained	Critical
		Opportunity for Improvement	Moderate
		Non-Conformance	Other
		Not Applicable	
	[Section 4.10 of IP Standard]		

Section B: Collection and submission of NAIT data

B01: Interface with NAIT Database

Criteria	Attainment	Risk	Audit summary and findings
B01-01 Documented policies and procedures are in place that enable staff to meet the information provider's obligations and obligations of the PICA's they contract with, under the NAIT ACT. [Section 4.3 of IP Standard]	Fully Attained Opportunity for Improvement Non-Conformance Not Applicable	Critical Moderate Other	
B01-02 If a NAIT standard governing accreditation of third-party software is in force and applies to the information provider. (for example, where that information provider wishes to use a common systems interface to connect to the NAIT information system), they comply with that standard. [Section 5.1 to 5.4 IP Standard]	Fully Attained Opportunity for Improvement Non-Conformance Not Applicable	Critical Moderate Other	

B02: Electronic data submission and data quality

B02-01 Information providers must take reasonable steps to ensure that data received from PICAs is correct and complete before it is transferred to the NAIT information system. [Section 5.9 of IP Standard]	Fully Attained Opportunity for Improvement Non-Conformance Not Applicable	Critical Moderate Other	
---	--	-------------------------------	--

B02-02	<p>Information provider must be able to demonstrate that they are able to achieve an operational level of data transfer quality and accuracy without error or omission. This means that in all instances of data transfer to the NAIT organisation the information transferred is both complete and correctly transferred.</p> <p>For example: animal exit declarations, and animal movement declarations, registration of NAIT Devices to NAIT Animals.</p> <p>[Section 5.8 of IP Standard]</p>	<p>Fully Attained</p> <p>Opportunity for Improvement</p> <p>Non-Conformance</p> <p>Not Applicable</p>	<p>Critical</p> <p>Moderate</p> <p>Other</p>
B02-03	<p>Information provider must be able to demonstrate that where they link into and access the NAIT information system for the purposes of submitting data that they do not compromise the integrity of the data in the NAIT information system or operation of the NAIT information system.</p> <p>[Section 5.7 of IP Standard]</p>	<p>Fully Attained</p> <p>Opportunity for Improvement</p> <p>Non-Conformance</p> <p>Not Applicable</p>	<p>Critical</p> <p>Moderate</p> <p>Other</p>
B02-04	<p>Information provider must notify PICAs in advance when they know ahead of time that they will be unable to provide their usual services: for example, when they will not be able to submit data on a PICA's behalf.</p> <p>[Section 5.10 of IP Standard]</p>	<p>Fully Attained</p> <p>Opportunity for Improvement</p> <p>Non-Conformance</p> <p>Not Applicable</p>	<p>Critical</p> <p>Moderate</p> <p>Other</p>

B02-05	Information provider must retain an electronic copy of all data entered in the NAIT information system, regardless of how the data is submitted, for 3 years. [Section 5.6 of IP Standard]	Fully Attained	Critical
		Opportunity for Improvement	Moderate
		Non-Conformance	Other
		Not Applicable	

B03: Provision of information to PICAs

B03-01	<p>When a receiving PICA requests an information provider to provide the NAIT number and sub-region of the sending PICA, the information provider must provide that information in a timely manner.</p> <p>When a sending PICA requests an information provider to provide the NAIT number and sub-region of the receiving PICA, the information provider must provide that information in a timely manner.</p> <p>In clauses 6.8–6.9 of this standard, “in a timely manner” means within the legal timeframes for the PICA’s provision of that information to the NAIT organisation, if applicable, and in any other event no later than 7 days after the request.</p> <p>[Section 6.7 to 6.9 of IP Standard]</p>	Fully Attained	Critical
		Opportunity for Improvement	Moderate
		Non-Conformance	Other
		Not Applicable	

B04: Data upload failures

B04-01	Where there is a failure in the process of uploading data to the NAIT information system, the information provider must immediately notify the NAIT organisation's contact center of the upload failure. To avoid doubt, this only applies where the failure cannot be rectified within the timeframes required by the NAIT Act. [Section 5.12 of IP Standard]	Fully Attained	Critical
		Opportunity for Improvement	Moderate
		Non-Conformance	Other
		Not Applicable	
B04-02	Information provider must resolve any data upload failures or errors within 48 hours of being notified of the failure or error, regardless of how or by whom the notification is made. [Section 5.12 to 5.14 of IP Standard]	Fully Attained	Critical
		Opportunity for Improvement	Moderate
		Non-Conformance	Other
		Not Applicable	

B05: Incorrect data

B05-01	Where a PICA advises the information provider of incorrectly recorded data, the information provider must take reasonable steps to resolve the issue within 48 hours. [Section 5.15 of IP Standard]	Fully Attained	Critical
		Opportunity for Improvement	Moderate
		Non-Conformance	Other
		Not Applicable	

B05-02	If the information provider is unable to resolve the issue, it must notify the PICA and the NAIT organisation that the incorrect data cannot be rectified within five business days. [Section 5.16 of IP Standard]	Fully Attained	Critical
		Opportunity for Improvement	Moderate
		Non-Conformance	Other
		Not Applicable	
B05-03	Where an information provider is informed of or identifies an incorrectly recorded movement and has not been informed of this movement by the PICA, the information provider must inform the PICA of the incorrect movement within 48 hours, as well as whether the issue has been resolved. [Section 5.17 of IP Standard]	Fully Attained	Critical
		Opportunity for Improvement	Moderate
		Non-Conformance	Other
		Not Applicable	

Section C: Policies and procedures

C01: Quality management

Criteria	Attainment	Risk	Audit summary and findings
C01-01 Satisfactory policies and procedures that describe the quality management system are available for review. [Section 4.12.3 of IP Standard]	Fully Attained	Critical	
	Opportunity for Improvement	Moderate	
	Non-Conformance	Other	
	Not Applicable		

C02: Document and data management

C02-01	<p>Satisfactory policies and procedures that describe the data management system are available for review.</p> <p>[Section 4.11 of IP Standard]</p>	<p>Fully Attained</p> <p>Opportunity for Improvement</p> <p>Non-Conformance</p> <p>Not Applicable</p>	<p>Critical</p> <p>Moderate</p> <p>Other</p>
C02-02	<p>Satisfactory policies and procedures exist for managing the NAIT data that they handle.</p> <p>Specifically, the policies and procedures ensure that the data is collected, held and used in compliance with New Zealand laws.</p> <p>[Section 4.11.1 of IP Standard]</p>	<p>Fully Attained</p> <p>Opportunity for Improvement</p> <p>Non-Conformance</p> <p>Not Applicable</p>	<p>Critical</p> <p>Moderate</p> <p>Other</p>
C02-03	<p>Satisfactory policies and procedures exist for managing the NAIT data that they handle.</p> <p>Specifically, the policies and procedures ensure that the data is collected, held and used in accordance with any restrictions imposed on the data by the person who provided it.</p> <p>[Section 4.11.2 of IP Standard]</p>	<p>Fully Attained</p> <p>Opportunity for Improvement</p> <p>Non-Conformance</p> <p>Not Applicable</p>	<p>Critical</p> <p>Moderate</p> <p>Other</p>

C02-04	<p>Satisfactory policies and procedures exist for managing the NAIT data that they handle.</p> <p>Specifically, the policies and procedures ensure that the data is held safely and securely.</p> <p>[Section 4.11.3 of IP Standard]</p>	<p>Fully Attained</p> <p>Opportunity for Improvement</p> <p>Non-Conformance</p> <p>Not Applicable</p>	<p>Critical</p> <p>Moderate</p> <p>Other</p>
C02-05	<p>Satisfactory policies and procedures exist for managing the NAIT data that they handle.</p> <p>Specifically, the policies and procedures ensure that the data is stored so that it is readily accessible.</p> <p>[Section 4.11.4 of IP Standard]</p>	<p>Fully Attained</p> <p>Opportunity for Improvement</p> <p>Non-Conformance</p> <p>Not Applicable</p>	<p>Critical</p> <p>Moderate</p> <p>Other</p>
C02-06	<p>Satisfactory policies and procedures exist for managing the NAIT data that they handle.</p> <p>Specifically, the policies and procedures ensure that the data is able to be securely transferred to the NAIT organisation within the regulated timeframes.</p> <p>[Section 4.11.5 of IP Standard]</p>	<p>Fully Attained</p> <p>Opportunity for Improvement</p> <p>Non-Conformance</p> <p>Not Applicable</p>	<p>Critical</p> <p>Moderate</p> <p>Other</p>

C02-07	If a NAIT standard governing accreditation of third-party software is in force and applies to an Information Provider (for example, where that entity wishes to use a common systems interface to connect to the NAIT information system), they must comply with that standard. [Section 5.1 of IP Standard]	Fully Attained	Critical
		Opportunity for Improvement	Moderate
		Non-Conformance	Other
		Not Applicable	

C03: Contract/supplier management

C03-01	Satisfactory policies and procedures exist that describe contract management. [Section 4.12.1 of IP Standard]	Fully Attained	Critical
		Opportunity for Improvement	Moderate
		Non-Conformance	Other
		Not Applicable	

C04: Staff responsibility and appointment

C04-01	Sufficient staff are employed or contracted by the organisation and that their staff have the skills and experience to perform the functions and duties required of them. [Section 4.2 IP Standard]	Fully Attained	Critical
		Opportunity for Improvement	Moderate
		Non-Conformance	Other
		Not Applicable	

C05: Staff training

C05-01	<p>Policies and procedures exist that enable their staff to meet an information provider's obligations and the obligations of the PICA's they contract with, under the NAIT Act.</p> <p>[Section 4.3 of IP Standard]</p>	<p>Fully Attained</p> <p>Opportunity for Improvement</p> <p>Non-Conformance</p> <p>Not Applicable</p>	<p>Critical</p> <p>Moderate</p> <p>Other</p>
C05-02	<p>There is evidence of procedures for providing training and support where required, to all registered information provider users within the organisation.</p> <p>[Section 4.2.2 and 4.12.5 IP Standard]</p>	<p>Fully Attained</p> <p>Opportunity for Improvement</p> <p>Non-Conformance</p> <p>Not Applicable</p>	<p>Critical</p> <p>Moderate</p> <p>Other</p>
C05-03	<p>There is evidence of individual training records for all registered information provider users and these ensure all registered information provider users are aware of their obligations under the NAIT Act, the Privacy Act 2020 and the standard.</p> <p>[Section 4.2.3 and 4.2.4 IP Standard]</p>	<p>Fully Attained</p> <p>Opportunity for Improvement</p> <p>Non-Conformance</p> <p>Not Applicable</p>	<p>Critical</p> <p>Moderate</p> <p>Other</p>

C06: Internal audit

C06-01	Satisfactory policies and procedures exist that describe the internal audit system. [Section 4.12.3 of IP Standard]	Fully Attained	Critical
		Opportunity for Improvement	Moderate
		Non-Conformance	Other
		Not Applicable	

C07: Complaints

C07-01	A documented complaints management policy exists, and a complaints register is maintained and available for review. [Section 4.4 of IP Standard]	Fully Attained	Critical
		Opportunity for Improvement	Moderate
		Non-Conformance	Other
		Not Applicable	
C07-02	The complaints register a must detail the following: <ul style="list-style-type: none"> the nature of the complaint who made the complaint how the complaint was resolved who managed the complaint the date the complaint was received, and the date the complaint was resolved. [Section 4.4.1 to 4.4.6 of IP Standard]	Fully Attained	Critical
		Opportunity for Improvement	Moderate
		Non-Conformance	Other
		Not Applicable	

C07-03	<p>The complaints management policy and any associated procedures are published.</p> <p><i>For example, on the company's website, member's database, or in available in physical copies on demand.</i></p> <p>[Section 4.5 of IP Standard]</p>	<p>Fully Attained</p> <p>Opportunity for Improvement</p> <p>Non-Conformance</p> <p>Not Applicable</p>	<p>Critical</p> <p>Moderate</p> <p>Other</p>
C07-04	<p>The complaints management policy and any associated procedures are provided on request to any PICA.</p> <p>[Section 4.5 of IP Standard]</p>	<p>Fully Attained</p> <p>Opportunity for Improvement</p> <p>Non-Conformance</p> <p>Not Applicable</p>	<p>Critical</p> <p>Moderate</p> <p>Other</p>
C08: information provider's obligations			
C08-01	<p>The information provider has entered into a written contract with each PICA that specifies the functions and duties that the information provider will undertake on behalf of that PICA. This must be done before the information provider accesses that PICA's information or undertakes a function or duty on their behalf, at the latest.</p> <p>[Section 6.2 of IP Standard]</p>	<p>Fully Attained</p> <p>Opportunity for Improvement</p> <p>Non-Conformance</p> <p>Not Applicable</p>	<p>Critical</p> <p>Moderate</p> <p>Other</p>

C08-02	<p>The contract between a PICA and an Information Provider must be held for the duration of the relationship with a PICA.</p> <p>[Section 6.3 of IP Standard]</p>	<p>Fully Attained</p> <p>Opportunity for Improvement</p> <p>Non-Conformance</p> <p>Not Applicable</p>	<p>Critical</p> <p>Moderate</p> <p>Other</p>
C08-03	<p>The information provider must retain copies of all data, correspondence and records relating to the contractual relationship with the PICA for at least 3 years after the contract terminates.</p> <p>[Section 6.4 of IP Standard]</p>	<p>Fully Attained</p> <p>Opportunity for Improvement</p> <p>Non-Conformance</p> <p>Not Applicable</p>	<p>Critical</p> <p>Moderate</p> <p>Other</p>
C08-04	<p>The contract must be made available to the NAIT organisation or an approved audit agency upon written request during this (retention) period.</p> <p>[Section 6.5 of IP Standard]</p>	<p>Fully Attained</p> <p>Opportunity for Improvement</p> <p>Non-Conformance</p> <p>Not Applicable</p>	<p>Critical</p> <p>Moderate</p> <p>Other</p>

Section D: Data management systems

D01: Information management

Criteria	Attainment	Risk	Audit summary and findings
D01-01 Satisfactory policies and procedures that describe IT security and data privacy are available for review. [Section 4.12.2 of IP Standard]	Fully Attained Opportunity for Improvement Non-Conformance Not Applicable	Critical Moderate Other	

D02: NAIT System terms of use

D02-01 The policies and procedures for IT security and data privacy provide instructions on how to: <ul style="list-style-type: none"> take care of the NAIT Information System information provider logons and passwords avoid the improper use of logons. [Section 4.12.2, and 5.11 of IP Standard , NAIT System Terms of Use July 2015]	Fully Attained Opportunity for Improvement Non-Conformance Not Applicable	Critical Moderate Other	
--	--	-------------------------------	--

D03: Data privacy

D03-01	<p>The policies and procedures for IT security and data privacy provide instructions on:</p> <ul style="list-style-type: none"> • what to do when your password is compromised • what to do if you know or have reason to believe that there has been or is about to be fraudulent or other unlawful use of your logons. <p>[Section 4.12.2 and 5.11 of IP Standard, NAIT System Terms of Use July 2015]</p>	Fully Attained	Critical
		Opportunity for Improvement	Moderate
		Non-Conformance	Other
		Not Applicable	

D04: Information system back up

D04-01	<p>Applicants must ensure that they have a system back up and that records are securely held.</p> <p>[Section 4.8 and 4.12 of IP Standard]</p>	Fully Attained	Critical
		Opportunity for Improvement	Moderate
		Non-Conformance	Other
		Not Applicable	

D04-02	<p>Satisfactory policies and procedures that describe the system back-up are available for review.</p> <p>[Section 4.12.4 of IP Standard]</p>	Fully Attained	Critical
		Opportunity for Improvement	Moderate
		Non-Conformance	Other
		Not Applicable	

D05: Information system recovery

D05-01	Policies and procedures that describe the system recovery are available for review. [Section 4.12.4 of IP Standard]	Fully Attained	Critical
		Opportunity for Improvement	Moderate
		Non-Conformance	Other
		Not Applicable	

D06: IT incident resolution

D06-01	Satisfactory policies and procedures that describe IT incident resolution and are available for review. Incidents are an unplanned loss or disruption of the IT system, services, or functions. [Section 4.12.6 of IP Standard]	Fully Attained	Critical
		Opportunity for Improvement	Moderate
		Non-Conformance	Other
		Not Applicable	

D07: Data upload failures and errors

D07-01	The organisation has methods to identify when a data upload failure or error to the NAIT database has occurred. [Section 5.12 of IP Standard]	Fully Attained	Critical
		Opportunity for Improvement	Moderate
		Non-Conformance	Other
		Not Applicable	

Section E: Business continuity

E01: Business continuity plan

Criteria	Attainment	Risk	Audit summary and findings
E01-01 Applicants must have a business continuity plan that ensures they can continue to perform their NAIT functions and duties, within the timeframes prescribed by the National Animal Identification and Tracing (Obligations and Exemptions) Regulations 2012, in the event of a systems failure or other emergency. [Section 4.6 of IP Standard]	Fully Attained Opportunity for Improvement Non-Conformance Not Applicable	Critical Moderate Other	
E01-02 The business continuity plan must include procedures for: <ul style="list-style-type: none"> Restoring system capability without loss of data. Operating alternative systems during emergency. [Section 4.7.1 and 4.7.2 of IP Standard]	Fully Attained Opportunity for Improvement Non-Conformance Not Applicable	Critical Moderate Other	

E02: Business continuity communication plan

E02-01 The business continuity plan must include procedures for: <ul style="list-style-type: none"> Communication with the NAIT Organisation about the emergency within 24 hours of emergency detection. Communicating with PICAs about the emergency if required. [Section 4.7.3 and 4.7.4 of IP Standard]	Fully Attained Opportunity for Improvement Non-Conformance Not Applicable	Critical Moderate Other	
--	--	---------------------------------------	--