New Zealand Core Database Access Panel

Core Database Compliance Internal Audit Report

January 2024

Distribution	Take action	Secure action	Information	Reviewed prior to release
Dave Paul, Data and Information Manager, NZAEL	✓			
Mike Jonkers, Head of Digital Technologies, DairyNZ	✓	✓		✓
Robyn Marsh, Chief Financial Officer & General Manager Corporate Services, NZCDAP		✓		✓
Robert Anderson, Chairman, NZCDAP			✓	

Building a better working world

Contents

1. Executive summary

1.1 Background

The core database compliance ("compliance") internal audit for New Zealand Core Database Access Panel ("NZCDAP" or the "Panel") has been completed in accordance with the Engagement Letter dated 24 August 2023.

Ernst & Young Limited ("EY") has been engaged by NZCDAP to meet your obligations under Section 27(1) of the Dairy Industry (Herd Testing and New Zealand Dairy Core Database) Regulations 2001 (the "Regulations"), which states: "the Access Panel must appoint an auditor to audit LIC's and the manager of the core database's compliance with Part 2 and this Part no later than 31 May in each year and may reappoint that auditor".

The New Zealand core database is maintained and managed by DairyNZ's Digital Technologies team in conjunction with the Dairy Industry Good Animal Database ("DIGAD") Manager who sits under DairyNZ's subsidiary, New Zealand Animal Evaluation Limited ("NZAEL"). All IT and operational processes of the core database are owned and managed by DairyNZ.

The scope of the compliance internal audit focused on the operational and IT controls that DairyNZ have in place to meet the requirements of parts 2 and 3 of the Dairy Industry (Herd Testing and the New Zealand Dairy Core Database) Regulations 2001. Our procedures covered testing of controls and transactions from the period beginning 1 January 2022 and ending 31 May 2023.

Refer to Appendix A for the objectives, scope and work performed for this compliance internal audit.

1.2 General comment

DairyNZ have been managing the core database since 2014 and have established a standard approach for processing applications to access and supply data from the core database. DairyNZ understands the requirements and the compliance that the Regulations demand.

We have also conducted a follow-up on the findings and observations from the 2022 compliance internal audit. Please refer to Appendix C for details. We found that all the issues observed are fully remediated, however, during the existing audit period we have noted two findings and one process improvement remained primarily due to staff changes within the Digital Operations team. Presently, new processes are being formulated and integrated across IT General and Operational controls to address these issues.

Our observations in relation to each of the compliance internal audit objectives (objectives in bold) are detailed below.

Evaluate the operation of the IT general controls (system controls) that DairyNZ had developed and implemented, to verify the security and integrity of data within the DairyNZ versions of the core database.

The core data is stored in SQL database that is hosted in the cloud and managed by the DairyNZ Digital Technologies team. All changes in the SQL database such as patches or upgrades were implemented locally by the DairyNZ Digital Operations team.

DairyNZ use a single sign-on user authentication service which permits a user to use one set of login credentials to access the core database. For the testing of authentication settings, we inspected the password settings on the network layer and noted that DairyNZ sets up the password settings in line with the company policy. We found the overall security settings follow good practice to prevent unauthorised access although there is room for improvement over the current minimum password length setting.

Our testing of user access management covered privileged access rights to the database, user creation, and termination of accounts. Due to staff changes within the scope period, there have been some inconsistencies in the processes applied particularly regarding the documentation of the approval for users requiring database access and a privileged account that was found that was not controlled and restricted. DairyNZ may need to revisit the actual process in place to ensure that the process and controls are consistently executed as designed. A periodic review of users may need to be considered to address the risks associated with, inappropriate privileged access rights granted to users, and creation of users with no supporting approval.

In relation to backup and recovery procedures, we found that the core database was backed up, replicated and stored on a regular basis. We randomly selected a sample of dates during the compliance internal audit scope period and observed that backups had been successfully created and restored. This supports our assessment that core data is retained and readily retrievable.

Evaluate the processes utilised by DairyNZ to verify their compliance with Part 2 and Part 3 of the Dairy Industry (Herd Testing and New Zealand Dairy Core Database) Regulations 2001.

We assessed DairyNZ's compliance with the obligations stated in Parts 2 and 3 of the Dairy Industry Regulations (2001) per the terms and conditions set by the Panel. This assessment did not identify any exceptions relating to compliance with Parts 2 and 3 of the Dairy Industry Regulations (2001).

To assess whether the core database fields were correctly populated, we obtained a random sample of 25 herds with more than one animal recorded. We obtained a list of all active cattle currently recorded for these herds. From these active cattle we randomly tested 25 animals to determine whether all required fields were populated as expected and found no exceptions.

To determine whether the application processes were followed, we tested all the applications to access data from the core database during the scope period and found no exceptions. We noted that there is a documented and established process governing application processing to restrict access to data in the core database. The process requires Panel approval and covers pricing methodology and proper delivery of the information. Please refer to Appendix B for the summary of our assessment of compliance with Part 2 and Part 3 of the Regulations.

1.3 Significant and high[1] observations

In accordance with the scope and objectives outlined in Appendix A, we noted no Significant or High rated observations.

Details of observations from this compliance internal audit are contained in the 'Findings and observations' section of this report.

1.4 Conclusion

As per Part 3 (28) (4) of the Dairy Industry (Herd Testing and New Zealand Dairy Core Database) Regulations 2001, we have had access to the accounting records and other documents and obtained all the information and explanations that we have required to perform our compliance internal audit.

Based on our compliance internal audit procedures performed we have not identified any evidence to indicate that DairyNZ is contravening Parts 2 and 3 of the Dairy Industry (Herd Testing and New Zealand Dairy Core Database) Regulations 2001.

Ernst & Young Limited
Paul Roberts
Partner – Consulting

[1] Definitions of Significant, High, Medium and Low rated observations and Improvement ideas are contained on page 3.

The following rating system has been used to identify the significance of the observations.

Rating	Definition
Significant	Serious control weakness requiring immediate NZCDAP CFO & Secretary/Chairman, DairyNZ Board/CEO attention and immediate management resolution.
High	Serious control weakness requiring immediate senior management attention.
Medium	Existing controls that need improvement for effectiveness, requiring management's attention.
Low	Minor control or efficiency issues.
Improvement idea	An observation or idea for management to consider, to improve a process or control.

Inherent Limitations

In the performance of our internal audit, we have undertaken tests of selected controls and transactions as appropriate to the circumstances of our internal audit. The concept of selective testing, which involves judgement regarding both the number of transactions to be audited and the controls to be tested, has been generally accepted as a valid and sufficient basis for an auditor to express a view on the internal controls in operation. Occasions may arise where the nature of the controls, the lack of controls or the circumstances of the internal audit require us to undertake alternative audit procedures. The decision to test, or not to test controls is made by us solely at our discretion.

Because of the inherent limitations in any system of internal control or accounting system, errors, fraud, or irregularities may occur and not be detected. The nature and size of the operations may prevent optimum segregation of duties being achieved. In addition, projections of any assessments provided on internal control relating to future periods (beyond the date of the audit fieldwork) are subject to the risk that the internal controls may become inadequate due to changes in conditions, or that the level of compliance with control procedures may deteriorate or weaken.

Our internal audit fieldwork was completed on 16 November 2023. Our findings are expressed as at that date. We have no responsibility to update this report for events or circumstances occurring after that date.

Third party reliance

This report has been prepared at the request of DairyNZ and NZCDAP in connection with our engagement to perform internal audit services. This report is solely for the benefit of DairyNZ and NZCDAP for the purpose set out in this report and is not to be used for any other purpose or distributed to any other party or relied upon by any other party without Ernst & Young Limited's prior written consent.

Other than our responsibility to the Board and Management of DairyNZ and NZCDAP, neither Ernst & Young Limited nor any officer or employee of Ernst & Young Limited undertakes any responsibility or liability arising in any way to any third party, including but not limited to DairyNZ and NZCDAP, external auditor, in respect of this report.

2. Findings and observations – IT general controls

2.1 New accounts created without supporting ticket

Finding **Rating:** Medium

During the scope period, seven new accounts were created, of which three did not have a supporting request ticket validating their database access. These users are part of the Digital Operations team, and their database access was granted as part of their job descriptions. The accounts are as follows:

#	Account Name	Name	Position	Hire date
1	ADM-OlaO	Ola Oloruntoba	Systems Engineer	17/01/2022
2	atpusernzael	System Account for DEFEND iCE Security Partner	N/A	23/02/2022
3	ADM-ScottF	Scott Fitzgerald	Digital Operations Lead	20/03/2023

We note that the risk of unauthorised access has been mitigated by the implementation of periodic user access right reviews during the scope period. These reviews involve a thorough evaluation of the appropriateness of access for each of the users, thereby ensuring enhanced scrutiny and control over user privileges.

Root cause

- Personnel changes within the Digital Technology team and several oversights by management. The required access for these users, integral to their job responsibilities, was granted without strictly following the established procedural steps for access creation, which involves approval and proper documentation of requests.

Effect

- The lack of a thorough approval process before creating accounts heightens the risk of granting unauthorised access to the NZAEL environment. This can potentially result in the initiation of unauthorised transactions, posing a threat to the overall security of data and systems.

Recommendation

1. DairyNZ should establish a documented procedure governing user access management. It should include the process in requesting, approving, and granting of access to DairyNZ IT environment.

Management comments

Comments	Person responsible	Due date
As noted in the finding, the risk has been mitigated and it was assumed that because the Digital Operations Team provided day to day support to the NZAEL infrastructure, new staff who joined the team 'inherited' the access as part of their role. Moving forward, all access requests, including Digital Staff, will be included in the established access request process to ensure explicit approval is obtained from NZAEL. Documentation will be updated to reflect this. It is important to note that a new staff member (Sean Yarrell) joined the Digital team on 15/01/2024, and the assumed process was applied again due to only	Mike Jonkers, DairyNZ, Head of Digital Technologies	January 2024

Comments	Person responsible	Due date
receiving the draft findings report during that same week. A retrospective ticket has been logged in the system to confirm approval from NZAEL.		

2.2 Potential inappropriate user access in SQL database

Finding **Rating:** Medium

We observed that the privileged 'SQL Services (SQLADMIN)' account password has not been adequately secured. The associated password for this account has not been stored securely in a digital password vault. Additionally, neither the Digital Operations Team nor the Business Intelligence Team seems to be aware of the location or method of password storage, indicating a gap in account security protocols.

Root cause

- The root cause of this issue is a deficiency in management's accountability regarding the supervision of privileged accounts and a communication gap between the Digital Operations Team and the Business Intelligence Team.

Effect

- Failing to store shared account passwords in a secure digital password vault not only jeopardises the security of the information contained in those accounts but also increases the risk of unauthorised access, making it easier for malicious actors to compromise sensitive data.

Recommendation

1. We recommend that management takes proactive measures to appropriately identify the accountable owner of the privileged account. Additionally, the credentials for this account should be securely stored using a reliable password management tool or a password vault. These tools offer a safe, centralised, and encrypted location for storing complex and unique passwords for shared accounts, thereby enhancing overall account security.

Management comments

Comments	Person responsible	Due date
Investigations are underway to identify the 'owner' of the SQLADMIN account and what the account is used for. If the account is no longer required, it will be removed. If it is still required, processes using the account will need to be identified with the view of the password being reset. Once reset (if possible), the credentials will be stored in DairyNZ's secure password vault.	Mike Jonkers, DairyNZ, Head of Digital Technologies	March 2024

2.3 Password configuration needs to be updated

Finding **Rating: Improvement idea**

We observed that one password parameter configuration within the DIGAD network, specifically the 'Minimum password length: 8', does not align with DairyNZ's Password Policy, which recommends a length of 16. We note that DairyNZ's approach is in alignment with the good security practice guidelines set by the National Institute of Standards and Technology ("NIST") for password configuration.

Root cause

- The root cause of this process improvement lies in the fact that the current password configuration for DIGAD does not align with the framework that DairyNZ use, and the current good security practices recommended by NIST.

Effect

- This misalignment could potentially facilitate unauthorised access, and subsequent misuse of privileged accounts, undermining the overall IT security infrastructure.

Recommendation

1. We recommend that management take the necessary steps to update the existing DIGAD's password configuration to reflect what was documented in the DairyNZ password policy. It is critical that the current configuration be reviewed and realigned, ensuring it aligns with up-to-date good security practices in password security to maintain a strong, effective IT security.

Management comments

Comments	Person responsible	Due date
Management notes that the 8-character password length is assigned in the DIGAD Group Policy and to access DIGAD internally, staff will need to first login to DairyNZ's environment using a 16-character passphrase. Investigations will be performed on the impact of changing DIGAD passwords to adhere to DairyNZ's 16-character password policy. If alignment is practical and preferred, then the DIGAD group policy in AD will be updated accordingly and passwords will be changed.	Dave Paul, Business Intelligence Specialist	May 2024

Appendix A Objectives, scope, and work performed.

Objectives

The objectives of this compliance internal audit were to:

- Evaluate the operation of the IT general controls (system controls) that DairyNZ have developed and implemented, to verify the security and integrity of data within the DairyNZ version of the core database.
- Evaluate the processes utilised by DairyNZ to verify the level of compliance with the Regulations.

Scope

Similar to prior years, the scope of this compliance internal audit focused on the operational and the IT controls that DairyNZ have in place to meet the requirements of parts 2 and 3 of Dairy Industry (Herd Testing and New Zealand Dairy Core Database) Regulations 2001.

Our sample testing of controls and transactions were drawn from the period beginning 1 January 2022 and ending 31 May 2023.

Out of Scope

This compliance internal audit did not include the following:

- Any assessment of particular system changes deployed to the DairyNZ IT environment.
- Any assessment over IT controls of the DairyNZ's systems outside the core database.
- Any assessment of fraud prevention and detection controls beyond the operational and IT controls related to management of core database.

Work performed

In the execution of the IT control testing, we performed the following:

- Performed a walkthrough to ascertain whether any changes had occurred to the core database IT Processes.
- If changes had occurred, we performed tests to assess if the controls over such changes were operating effectively and efficiently.
- Followed-up on the issues and management action plans that were raised in the last compliance internal audit to determine whether previously identified matters have been appropriately resolved.

In the execution of operational control testing, we performed the following:

- Held discussions with key personnel to ascertain whether any changes had occurred in the process for handling Confidential and Non-Confidential applications and the process for handling data access internally, for their own use.
- Obtained the pricing methodology and compared the reasonability of measurable inputs to similar costs in the market and compared back to actual costs of DairyNZ.
- Tested completed applications (Confidential and Non-Confidential) to assess the accuracy of the application process controls.
- Conducted interviews with process owners to gain an understanding of the process followed by the applicants in making the applications and identifying any issues or concerns with the process.
- Tested a sample of applications to assess whether a formal request was completed and appropriately authorised, and whether the Regulations or Panel rulings were adhered to.
- Followed-up on the issues and management action plans that were raised in the last compliance internal audit, to determine whether previously identified matters have been appropriately resolved.

Appendix B Key regulatory compliance

Below is a summary of our assessment of compliance with Part 2 and Part 3 of the Regulations:

Compliance with Dairy Industry (Herd Testing And New Zealand Dairy Core Database) Regulations 2001		
Legislation		
Clause	**Description**	**Compliance**
Part 2		
12	Neither LIC nor the manager of the core database may enter into exclusive arrangements for access to data in the core database.	✓
17	An application for access to information in the core database must be— (a) made in the manner required by the Access Panel; and (b) accompanied by a fee of $200 (which is inclusive of goods and services tax).	✓
18 (1)	The Access Panel must grant an application for access to data in the core database only if it is satisfied that to do so is likely to be beneficial to the New Zealand dairy industry.	✓
18 (2)	If the Access Panel is not satisfied that granting an application for access to data in the core database is likely to be beneficial to the New Zealand dairy industry, the Access Panel may grant an application for access to data in the core database only if the Access Panel is satisfied that to do so would not be harmful to the New Zealand dairy industry.	✓
19 (1)	The Access Panel may set terms and conditions (excluding the manager of the core database's charges) on which data in the core database must be made available, including the form in which it must be made available and the time limits within which it must be made available.	✓
19 (2)	LIC or the manager of the core database may require an applicant for access to the data in the core database to execute an agreement with LIC or the manager (as the case may be) before access is granted.	✓
19 (3)	An agreement required by LIC or the manager of the core database under subclause (2) must contain the terms and conditions set by the Access Panel under subclause (1).	✓
22 (1)	The manager of the core database must retain the following information in electronic form:	
22 (1)(a)	all data provided to LIC under the Herd Testing Regulations 1958 and held by LIC in electronic form at the commencement of these regulations; and	✓
22 (1)(b)	all data provided to LIC after the commencement of these regulations under the Herd Testing Regulations 1958; and	✓
22 (1)(c)	all data provided to LIC or to the manager under these regulations.	✓
22 (2)	The manager of the core database must retain the data so that it is readily retrievable.	✓
24 (1)	Neither LIC nor the manager of the core database may make data in the core database available except—	
24 (1)(a)	in accordance with a decision or determination of the Access Panel; or	✓
24 (1)(b)	to the owner or person in charge of the dairy herd to which the data relates; or	✓
24 (1)(c)	to a person authorised to receive the data by the owner or person in charge of the dairy herd to which the data relates.	✓
24 (2)	A person referred to in subclause (1)(b) or (c) may request the manager of the core database to provide data in the core database, and the entity concerned must provide the requested data subject to payment of any reasonable charge for access set by that entity.	✓
24(3)	Subclause (1) does not prevent LIC from using data in the core database for the purposes of its own business. However, if LIC proposes to use data in any partnership or joint venture or other arrangement with any other person, subclause (1) applies to access to the information for that purpose.	✓

Compliance with Dairy Industry (Herd Testing And New Zealand Dairy Core Database) Regulations 2001		
Legislation		
Clause	**Description**	**Compliance**
Part 2		
25(1)	LIC and the manager of the core database must keep confidential, and must not disclose to any other person,–	
25(1)(a)	any information contained in an application to the Access Panel in relation to the supply of data in the core database:	✓
25(1)(b)	the fact that an application has been made:	✓
25(1)(c)	the fact that any data in the core database has been made available as a result of an application.	✓
25(2)	In subclause (1), any other person includes any person who is both–	
25(2)(a)	a director, employee, contractor, or associated person of LIC or of the manager; and	✓
25(2)(b)	a person involved in any activity of LIC's or of the manager's, other than the operation of the database of which the core database forms a part.	✓
25(3)	Subclause (1) applies subject to any agreement that an applicant may reach with LIC or the manager of the core database in relation to their application.	✓
Part 3		
26(1)	The manager of the core database must publish the manager's–	
26(1)(a)	procedures for complying with decisions of the Access Panel, including maximum time periods for the provision of data; and	✓
26(1)(b)	procedures for complying with regulation 25; and	✓
26(1))c)	pricing methodology or methodologies used to set charges for access to data in the core database (including charges that the manager makes to businesses it owns for access to that data), and the prices resulting from applying those methodologies.	✓
26(2)	The manager of the core database must publish the information required by subclause (1) as soon as practicable after 1 June in each year.	✓
26(3)	The manager of the core database must ensure that the manager makes available, in the following ways, information that the manager is required by these regulations to publish:	
26(3)a	by making copies of the information available for inspection, during ordinary office hours, at the manager's office; and	✓
26(3)b	by providing the information to a person who requests it, in whichever of the following ways the person prefers:	
	(i) by post, or	✓
	(ii) for collection, during ordinary office hours, from the manager's office.	✓
29(1)	Information supplied to the chief executive under section 66(1) or (2) of the Act must be verified by statutory declaration in the form specified in Schedule 6.	✓
29(2)	The statutory declaration referred to in subclause (1) must be made by a director or officer of LIC or by a director or an officer of the manager of the core database, whichever is appropriate in the circumstances.	✓
Legend:		
✓	Complies, No observations noted.	
✓*	Complies, with observation noted. Please refer to list of findings and observations	

Appendix C 2022 Compliance internal audit follow-up

We followed-up findings from the 2022 compliance internal audit and the results are below.

2022 finding	2022 Management's response	2023 status
IT Controls		
ITC 01 - New users created without approval As part of our testing, we assessed whether the users created during the scope period were supported by a service ticket showing that the access is approved, and if their access rights are aligned with approved request. We noted that out of 25 new user samples we tested: ► 11 were not supported by an approval hence we cannot determine whether they have been approved by the business prior to creation. ► Three were created prior to approval and their request were logged after the creation of the account.	The observation and its potential impact have been understood. Will improve current process as per recommendation.	This finding is closed. However, access granting control remains ineffective due to the finding noted above. Please see finding 2.1 for more details of the finding.
ITC 02 - Terminated employee access not deactivated in a timely manner We tested whether the access of 166 terminated employees during the compliance internal audit scope period have been revoked in a timely manner. We noted one user who accessed the network post termination date, although the account was Disabled at the time of testing.	The observation and its potential impact have been understood. A further analysis of the user noted as exception will be performed to determine whether the account was used inappropriately. Will improve current process as per recommendation.	This finding is closed.
ITC 03 – Inappropriate privileged access in SQL database We assessed the privileged users in the SQL database and noted the following users that no longer require privileged access rights, hence, were determined as inappropriate. We were informed that DairyNZ will review these users and update their access rights accordingly.	The observation and its potential impact have been understood. Users noted as exception will be reviewed, and access rights/permissions will be updated accordingly. Will improve current process as per recommendation.	This finding is closed. However, privileged access control remains ineffective due to the finding noted above. Please see finding 2.2 for more details of the finding.

2022 finding	2022 Management's response	2023 status
ITC 04 – Change testing documentation could be improved DairyNZ has a process that requires a change to be logged in the service ticketing tool (Freshservice), tested, and approved prior to deployment to the production environment. We noted that none of the five change samples we tested had evidence of testing performed.	The observation and its potential impact have been understood. Will improve the current process as per recommendation.	This finding is closed. We obtained a sample of change and noted that evidence of testing is attached and included in the process.
ITC 05 – Idle session setting on network layer We noted that the core SQL database utilises the Active Directory user credentials for authenticating users. We performed testing on the password settings on the network layer and noted that it could be improved by activating the idle session timeout. Good practice suggests that computer session should be locked after a period of inactivity.	The observation and its potential impact have been understood Current process will be improved as per recommendation.	This finding is closed.

2022 finding	2022 Management's response	2023 status
Operational Controls		
OC 01 - Inconsistent process implementation The regulation mentions that NZCDAP, being the core database manager, should not make the data in the core database available except in accordance with a decision or determination of the Access Panel. Currently, DairyNZ does not have a process in place to determine whether a data extract should be charged or not. And if it should not, there is currently no criteria to guide that decision. It is also unknown who in DairyNZ could make that call. We noted the following applications from our testing, that though they have been approved by the Access Panel, the data extract was not charged. ► AP87 - data extract was determined as support of a DIGAD project, hence, there was no charge made. ► AP120 - there was no fee charged for the data extract as per instruction of a manager in NZAEL. ► AP121 - the data extract was used for a project's proof of concept, however, although there was a movement of data, the data itself was not used and has not been persisted, hence, there was no fee charged. ► AP122 - was paid internally by the Strategy and Investment Leader and was determined to be an internal job, hence no formal invoice was created. Also, we noted that administration fee and base programming fee have been waived.	There are no instances where a data extract is not required to go through an application process. We do not release data unless approved by the Core Data Access Panel. The $200 fee to process the application has always been charged. We will review the process documentation to ensure it reflects current practice.	This finding is closed. We confirmed that the process documentation reflects current practice.

2022 finding	2022 Management's response	2023 status
OC 02 - Inconsistent charging of fees A customer is charged with a programming fee that includes a base programming fee per approved data extract and any additional fee which is at an hourly rate. We noted that from the samples that we tested that the base programming fee is only charged once per application request, and it is the minimum that will be charged for any programming effort. Out of the 12 data extracts during the compliance internal audit scope period, four did not have the base programming fee charged as they were already charged in 2018 when the programming was completed. However, for one sample (AP100), we cannot determine whether a base programming fee was charged. In addition, the regulation mentions that an application will be accompanied by a fee of $200. We noted in our testing that there was no administration fee charged for reruns as it is only charged upon application. Instead, customers were charged with rerun fees. However, this was not specified in the documented procedure nor in the New Zealand Gazette for DairyNZ Limited's Procedure for Complying with Decisions of the Panel (Gazette). During our testing we noted that for the AP100 application we cannot determine based on the information provided whether an administration fee was included in the amount charged to the customer.	For AP100 the administration fee and the base programming fee should have been charged in 2018. Unfortunately, we do not have the itemised invoice charges. The fee schedule in the Gazette mentions the Additional Extracts fee of $500. On the invoice we call this a Rerun fee. Except for the fact that we do not have the itemised invoice from 2018, there have been no issues with charging the appropriate fees. The risk associated with this has been understood and I do not believe additional documentation or checks are needed.	This finding is closed.
OC 03 - Missing panel approval for contract renewal The Panel approval document for AP79 was issued in June 2017 with three years validity. We noted that data was provided to the customer in March 2020 and whilst the decision was still valid, we noted that the agreement with the customer had been renewed. However, there was no formal Panel decision supporting its renewal. We noted that the documented process does not specify the process for contract renewal. However, the expectation is to have an updated Panel approval if the customer continues to access the core data.	We received an email from David Evans confirming that the panel had approved the extension request. We believe that is sufficient and no changes are required. As mentioned under 3.1, we will review the process documentation to ensure it reflects current practice.	This finding is closed. We did not note any contract renewal in our scope period this year.

2022 finding	2022 Management's response	2023 status
OC 04 - Outdated documented procedures DairyNZ has a Gazette to guide the public as well as an internal procedure (AP – Manage Approved Access Panel Applications document) used by the DIGAD administrator in applying for a core data extract. We noted that these two documents contain conflicting information regarding the base programming fee charge. In addition, we noted that the AP – Manage Approved Access Panel Applications document requires a Data Transfer Agreement approved by the NZAEL Manager and signed by the customer. However, we noted that this requirement has been removed and Data Transfer Agreement is no longer obtained, instead the client agrees to the manner of data transfer when the customer agrees with the price. We were informed that the documented application process is yet to be updated to reflect this change.	We have changed the documentation to reflect that the base programming charge is $600 per approved data extract.	This finding is closed. We inspected the updated Gazette and noted that the fee is now $600 per the approved data extract.

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

ey.com