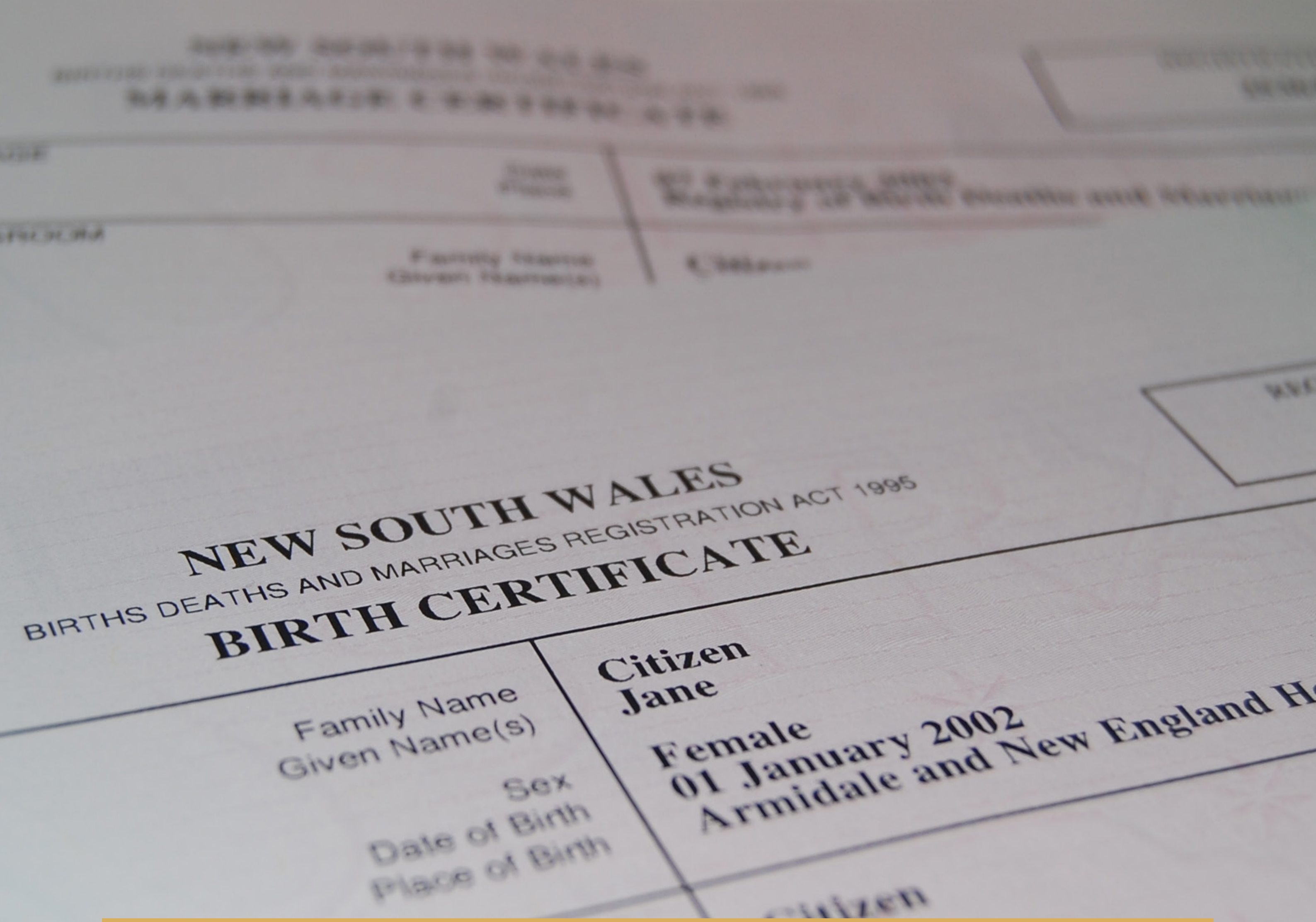


NEW SOUTH WALES

BIRTHS DEATHS AND MARRIAGES REGISTRATION ACT 1995

BIRTH CERTIFICATE

Family Name	Citizen
Given Name(s)	Jane
Sex	Female
Date of Birth	01 January 2002
Place of Birth	Armidale and New England H

PERFORMANCE AUDIT

7 APRIL 2020

Integrity of data in the Births, Deaths and Marriages Register

NEW SOUTH WALES AUDITOR-GENERAL'S REPORT

audit office
OF NEW SOUTH WALES

THE ROLE OF THE AUDITOR-GENERAL

The roles and responsibilities of the Auditor-General, and hence the Audit Office, are set out in the *Public Finance and Audit Act 1983* and the *Local Government Act 1993.*

We conduct financial or 'attest' audits of State public sector and local government entities' financial statements. We also audit the Total State Sector Accounts, a consolidation of all agencies' accounts.

Financial audits are designed to add credibility to financial statements, enhancing their value to end-users. Also, the existence of such audits provides a constant stimulus to entities to ensure sound financial management.

Following a financial audit the Audit Office issues a variety of reports to entities and reports periodically to parliament. In combination these reports give opinions on the truth and fairness of financial statements, and comment on entity compliance with certain laws, regulations and government directives. They may comment on financial prudence, probity and waste, and recommend operational improvements.

We also conduct performance audits. These examine whether an entity is carrying out its activities effectively and doing so economically and efficiently and in compliance with relevant laws. Audits may cover all or parts of an entity's operations, or consider particular issues across a number of entities.

As well as financial and performance audits, the Auditor-General carries out special reviews and compliance engagements.

Performance audits are reported separately, with all other audits included in one of the regular volumes of the Auditor-General's Reports to Parliament – Financial Audits.

Cover image: © NSW Registry of Births, Deaths and Marriages 2020. Supplied and permitted for use under Creative Commons Attribution-ShareAlike 3.0 Unported Licence. Full terms at https:// creativecommons.org/licenses/by-sa/3.0/deed.en

AUDITOR-GENERAL
ORTA RECENS QUAM PURA NITES
NEW SOUTH WALES

GPO Box 12
Sydney NSW 2001

The Legislative Assembly
Parliament House
Sydney NSW 2000

The Legislative Council
Parliament House
Sydney NSW 2000

In accordance with section 38E of the *Public Finance and Audit Act 1983*, I present a report titled **'Integrity of data in the Births, Deaths and Marriages Register'.**

Margaret Crawford
Auditor-General
7 April 2020

contents

Integrity of data in the Births, Deaths and Marriages Register

Section one – Integrity of data in the Births, Deaths and Marriages Register

Executive summary 1

Introduction 4

Maintaining the integrity of the Register 6

Preventing unauthorised access and misuse 8

Section two – Appendices

Appendix one – Response from agency 15

Appendix two – About the audit 18

Appendix three – Performance auditing 20

Section one

Integrity of data in the Births, Deaths and Marriages Register

Executive summary

The NSW Registry of Births Deaths and Marriages (BD&M) is responsible for maintaining registers of births, deaths and marriages in New South Wales. BD&M is also responsible for registering adoptions, changes of name, changes of sex and relationships. These records are collectively referred to as 'the Register'. The *Births, Deaths and Marriages Registration Act 1995* (the BD&M Act) makes the Registrar (the head of BD&M) responsible for maintaining the integrity of the Register and preventing fraud associated with the Register. Maintaining the integrity of the information held in the Register is important as it is used to confirm people's identity. Unauthorised access to, or misuse of the information in the Register can lead to fraud or identity theft. For these reasons it is important that there are sufficient controls in place to protect the information.

BD&M staff access, add to and amend the Register through the LifeLink application. While BD&M is part of the Department of Customer Service, the Department of Communities and Justice (DCJ) manages the databases that contain the Register and sit behind LifeLink and is responsible for the security of these databases.

This audit assessed whether BD&M has effective controls in place to ensure the integrity of data in the Births, Deaths and Marriages Register, and to prevent unauthorised access and misuse. It addressed the following:

- Are relevant process and IT controls in place and effective to ensure the integrity of data in the Register and the authenticity of records and documents?
- Are security controls in place and effective to prevent unauthorised access to, and modification of, data in the Register?

Conclusion

BD&M has processes and controls in place to ensure that the information entered in the Register is accurate and that amendments to the Register are validated. BD&M also has controls in place to prevent and detect unauthorised access to, and activity in the Register. However, there are significant gaps in these controls. Addressing these gaps is necessary to ensure the integrity of the information in the Register.

BD&M has detailed procedures for all registrations and amendments to the Register, which include processes for entering, assessing and checking the validity and adequacy of source documents. Where BD&M staff have directly input all the data and for amendments to the Register, a second person is required to check all information that has been input before an event can be registered or an amendment can be made. BD&M carries out regular internal audits of all registration processes to check whether procedures are being followed and to address non-compliance where required.

BD&M authorises access to the Register and carries out regular access reviews to ensure that users are current and have the appropriate level of access. There are audit trails of all user activity, but BD&M does not routinely monitor these. At the time of the audit, BD&M also did not monitor activity by privileged users who could make unauthorised changes to the Register. Not monitoring this activity created a risk that unauthorised activity in the Register would not be detected.

BD&M has no direct oversight of the database environment which houses the Register and relies on DCJ's management of a third-party vendor to provide the assurance it needs over database security. The vendor operates an Information Security Management System that complies with international standards, but neither BD&M nor DCJ has undertaken independent assurance of the effectiveness of the vendor's IT controls.

1. Key findings

BD&M has processes in place to ensure that the information entered in the Register is accurate and that amendments to the Register are validated

BD&M has detailed procedures for all registrations which include processes for entering, assessing and checking the validity and adequacy of source documents. Where BD&M staff have directly input all the data, LifeLink requires a second staff member to approve the registration before it is entered on the Register. BD&M also requires documentation from two separate sources for birth and death registrations.

BD&M validates and authorises all requests for amendments to the Register and there is segregation of duties to ensure that the same officer cannot both create and apply an amendment. BD&M carries out regular internal audits of all registration processes to check whether procedures are being followed and to identify and address non-compliance.

BD&M authorises access to the Register and regularly reviews this access

BD&M has processes in place to authorise internal and third-party access to the Register, including Service NSW call centre staff and users who submit information via eRegistry. This authorisation process ensures that users are provided with the appropriate level of access. BD&M carry out regular user access reviews to ensure that the list of users is current and that users have the appropriate levels of access.

There are insufficient controls to prevent the distribution of information in the Register

There are currently insufficient restrictions placed on the ability of staff to export and distribute information from LifeLink. This increases the risk of unauthorised access to, and misuse of LifeLink data and creates the risk that information may be sent to unauthorised third parties.

Four staff members of BD&M can use specialised software to generate reports of data from the Register as part of their role in BD&M. There is an audit trail of this activity but at the time of the audit, BD&M was not reviewing this. BD&M has since commenced routine audits to address this.

BD&M does not actively monitor user activity in the Register

BD&M maintains audit trails of all activity in the Register but does not routinely monitor these to identify unusual activity or fraud by users including activity by Service NSW staff who have read-only access to the Register. At the time of this audit, BD&M also did not monitor audit trails of privileged user activity in the Register, but it has now commenced routine audits to address this. It is particularly important to monitor activity by privileged users because they have access to amend records and can enable unauthorised access to the Register.

BD&M does not have sufficient assurance over the effectiveness of database security controls

BD&M has no direct oversight of the database environment and relies on DCJ's management of a third-party vendor to provide the assurance it needs over database security. The vendor operates an Information Security Management System that is certified against international standards, but neither BD&M nor DCJ has undertaken independent assurance of the effectiveness of the vendor's general IT controls.

There are gaps in controls to prevent and detect unauthorised access to the databases and servers

Neither BD&M nor DCJ is regularly reviewing users who have access to the databases and related servers that sit behind the Register. They are also not monitoring user activity in these databases and servers. Passwords that individuals use to access the databases and servers are not configured in line with DCJ's policy on required password settings. This creates the risk of unauthorised access or changes to the Register that are not identified.

2. Recommendations

As a matter of urgency, the Department of Customer Service should ensure that the Registry of Births Deaths and Marriages:

1. works with the Department of Communities and Justice to ensure that passwords for users authorised to access the databases and servers comply with the Department of Communities and Justice's policy on password settings.

By July 2020, the Department of Customer Service should ensure that the Registry of Births Deaths and Marriages:

2. routinely monitors:
   - privileged user activity in the Register
   - other user activity in the Register including activity outside normal office hours
   - reporting software user activity
3. restricts the ability of LifeLink users to export and distribute information from the Register outside of legitimate actions required for their role
4. updates the Service Partnership Agreement with Service NSW to include monitoring of Service NSW staff activity in the Register
5. performs regular fraud detection audits for eRegistry users
6. works with the Department of Communities and Justice to ensure that:
   - there are regular access reviews of users of the databases and servers that sit behind the Register
   - there is regular monitoring of activity of users who have access to the databases and servers that sit behind the Register
   - there are regular audits to provide independent assurance that database security controls operate effectively
7. clarifies and formalises responsibilities with the Department of Communities and Justice in relation to the management of database security

By December 2020, the Department of Customer Service should ensure that the Registry of Births Deaths and Marriages:

8. undertakes a risk-based analysis of the impact of gaps in the controls to prevent unauthorised user activity on the historical integrity of data in the Register
9. implements remediating action stemming from recommendation eight.

1. Introduction

1.1 The NSW Registry of Births Deaths and Marriages

The NSW Registry of Births Deaths and Marriages (BD&M) was created in 1856 to establish and maintain accurate registers of births, deaths and marriages in NSW. These are collectively referred to as 'the Register'. The responsibilities of BD&M are set out in the *Births, Deaths and Marriages Registration Act 1995* (the BD&M Act), the *Births, Deaths and Marriages Registration Regulation 2017*, the *Relationships Register Act 2010* and the Commonwealth *Marriage Act 1961*. The legislation sets out requirements for the registration of the following life events:

- births
- deaths
- marriages
- adoptions
- changes of name
- changes of sex
- relationships.

BD&M also produces certificates relating to these registrations. The general functions of the BD&M Registrar (the head of BD&M), as set out in the BD&M Act, include:

- establishing and maintaining the Register
- maintaining the integrity of information in the Register and preventing identity fraud associated with the Register and the information extracted from the Register
- administering the registration system and ensuring that it operates efficiently, effectively and economically.

The Register is accessed, added to and amended through the LifeLink application. Most BD&M staff use LifeLink as part of their day-to-day work.

1.2 Third party interactions with the Register

BD&M moved from the former Department of Justice to the Department of Customer Service (DCS) on 1 July 2019 as part of the Machinery of Government changes. The Department of Communities and Justice (DCJ) manages the databases that sit behind LifeLink and contain all the data in the Register. This means that DCJ manages the controls which protect the databases from unauthorised access. While DCJ is responsible for managing the databases, a third-party vendor hosts the databases on their servers.

In line with the BD&M Act, the Registrar has also authorised a number of other organisations to have access to the Register. The Service NSW call centre receives enquiries from members of the public regarding the progress of their BD&M certificate applications and registration processes. Allocated staff have read-only access to LifeLink to enable them to respond to these enquiries.

BD&M authorises midwives and other hospital staff, funeral directors and marriage celebrants to have access to eRegistry; an online portal that enables them to upload registration and supporting documentation relating to birth, death and marriage registrations.

1.3 About the Audit

This audit assessed the effectiveness of controls in place to ensure the integrity of data in the Births, Deaths and Marriages Register, and to prevent unauthorised access and misuse.

We addressed the audit objective with the following audit criteria:

1. Security controls are in place and effective to prevent unauthorised access to, and modification of, data in the Register.
2. Process and IT controls are in place and effective to ensure the integrity of data in the Register and the authenticity of records and documents.

More information about the audit approach can be found in Appendix two.

2. Maintaining the integrity of the Register

2.1 Verification of information entered in the Register

BD&M has controls in place to ensure that life events are registered accurately

Maintaining the integrity of the Register and preventing fraud associated with the Register are key roles of the Registrar. This means that controls must be in place to ensure that only legitimate events are registered, and that they are registered accurately. BD&M has a range of controls in place to ensure that this occurs.

BD&M has detailed procedures for all of the registration processes including birth, death, marriage, change of name, change of sex and relationship registrations. These include processes for entering, assessing and checking the validity and adequacy of source documents. Where BD&M staff have directly input all the data, LifeLink requires a second staff member to approve the registration before it is entered on the Register. This segregation of duties reduces the risk of error or fraud by BD&M staff members.

In addition to these controls, BD&M also has controls to verify the identity of individuals who have submitted information. Third parties using eRegistry must use the login credentials provided by BD&M. Other parties, for example the parents of a newborn, are required to submit identification documents with their registration. BD&M checks these against state and national databases to ensure that they are legitimate. These controls seek to minimise the risk that unauthorised individuals are submitting information.

BD&M requires two sources of documentation for birth and death registrations, but the same party submits both death registration documents

Before BD&M registers a birth or death, matching information is required from two separate forms of documentation. This reduces the risk of fraud by requiring verification from two sources. Exhibit 1 indicates the forms of documentation required to register these events.

Exhibit 1: Documentation required for birth and death registrations

Event	Document one	Document two
Birth	Notice of Birth	Birth Registration Statement
Death	One of: • Medical Certificate Cause of Death • Medical Certificate Cause of Perinatal Death • Coroner's Notice of Particulars.	Death Registration Statement

Source: Audit Office analysis of BD&M processes.

For birth registrations, the Birth Registration Statement is completed by both parents and submitted with their identity documentation, usually online. Midwives and hospital staff submit the Notice of Birth using eRegistry. Where all information is provided online and the two sources of information match then the birth will automatically register with no involvement of BD&M staff. If the information does not match, BD&M staff are responsible for checking source documentation to identify and correct any errors and approve the birth registration.

For death registrations, BD&M requires two documents: a Death Registration Statement (DRS) and one of the certificates listed in Exhibit 1. Funeral directors complete and submit the DRS. The other certificate is entered into LifeLink by BD&M staff and when this information matches the information in the DRS, the death is registered.

Rather than requiring the DRS and the Medical Certificate to be lodged separately, BD&M allows funeral directors to lodge both documents. This has the potential to weaken this control as both documents are submitted from the same source. BD&M mitigate this risk by limiting the distribution of the blank Medical Certificate forms to authorised healthcare practitioners and requiring that these practitioners include their Australian Health Practitioner Regulation Agency registration number.

2.2 Authorising amendments to the Register and auditing processes

BD&M validates and authorises requests for amendments to the Register

In order to ensure the integrity of information in the Register, it is important that any changes that are made once an event is registered are valid and authorised. As with registrations, BD&M has procedures in place to ensure that requests received for amendments to the Register are validated and authorised. Requests for amendments must be made in writing by a person entitled to receive a certificate of the event and they are required to provide proof of identification. All amendments are completed in two stages (creation and approval) and there is segregation of duties to ensure that the same officer cannot create and approve an amendment.

BD&M carries out regular internal audits to ensure that policies and procedures relating to data integrity are being followed

BD&M carry out routine audits of a sample of birth, marriage and death registrations as well as change of name, change of sex, relationship and adoption registrations. They also carry out routine audits of proof of identity checks for registrations. These audits are carried out to check that the registration process conforms with internal procedures and is compliant with legislation. The audits involve checking the validity of source documents and ensuring that identification procedures have been followed. BD&M also carry out audits of a sample of amendments made to the Register. Audits are carried out by staff who are not responsible for implementing the process being audited.

Audit reports contain findings, non-conformances, areas of concern, strengths, opportunities for improvement and recommendations. Audit results are shared with the relevant operational manager and signed by the auditor, the auditee and their Divisional Manager. Operational managers report on the corrective actions undertaken in response to the recommendations and corrective actions are entered into a database and implementation of these actions is monitored.

3. Preventing unauthorised access and misuse

3.1 Authorising user access

BD&M authorises and regularly reviews access to the Register

BD&M has approval processes in place to ensure that staff are provided with the appropriate level of access to the Register through LifeLink. This includes all levels of access for BD&M staff, as well as Service NSW call centre staff who require read-only access. Levels of access are restricted depending on the assigned role of the staff member. Roles with associated permissions are built into LifeLink. BD&M has processes in place to approve changes to staff access and to disable access if staff resign or are going on leave for longer than four weeks.

BD&M routinely audits LifeLink user access for both BD&M and Service NSW staff to confirm whether staff members are assigned the appropriate level of access and to ensure that access has been disabled where required. BD&M policy is that access is removed on an employee's last day or when staff are due to take at least four weeks of leave. The audits check that this policy has been followed.

During the audit period there were 12 staff members who left BD&M and there were two instances where LifeLink access was not removed on the staff member's last working day. For these staff, user access was removed three and five days later. In this case the two staff members did not access the system after their last working day.

BD&M authorises third party access to eRegistry

BD&M authorises access for third parties, such as marriage celebrants, funeral directors and midwives, to upload information to eRegistry. BD&M regularly checks the currency of eRegistry users for some, but not all of these users. This means that some of the registration details may be out-of-date and may include users who no longer require this access.

In addition to developing a process to ensure the currency of all eRegistry users, BD&M could monitor user access to identify third party users who have not logged in for an extended period and then remove their access. This would increase BD&M's assurance over the currency of eRegistry users.

3.2 Identifying and preventing unauthorised access and misuse

LifeLink logs user activity through audit trails, but BD&M does not monitor these

LifeLink logs audit trails of all user activity. These audit trails cannot be amended or deleted. BD&M only monitors these audit trails when they have been alerted to some unusual activity or potential fraud. BD&M does not carry out routine monitoring of audit trails to ensure that users are only accessing records that are required for their work or to identify any unusual or suspicious activity. BD&M also does not carry out routine monitoring of Service NSW staff activity in the Register to ensure that they are only accessing records required for their work.

BD&M previously monitored user activity in LifeLink outside of normal office hours through a third-party application. Each day, a list of users accessing LifeLink outside normal office hours was sent to relevant staff in BD&M for checking. However, BD&M has not been receiving these reports since January 2019 as the third-party application has not been functioning correctly. BD&M can monitor staff activity outside normal office hours using audit trails. At the time of the audit, BD&M was not doing this, but it has now commenced routine audits to address this.

At the time of the audit, BD&M did not monitor activity of privileged users in LifeLink

Privileged users are users who have a high level of access to key systems, such as granting or modifying system access to other accounts. There are nine accounts with privileged user access to LifeLink. Privileged user access to LifeLink is authorised using the same process as general users and there is no separate, independent review of privileged user access.

There is a risk that privileged users could carry out unauthorised activity in the Register such as creating an unauthorised registration or amendment, or providing unauthorised access to another user. This has the potential to be used for fraudulent purposes. At the time of the audit, BD&M did not monitor audit trails for privileged users to identify unauthorised activity but it has now commenced routine audits to address this.

BD&M has alerts on high profile and sensitive records to identify users viewing these records

BD&M has placed visible alerts on high profile and sensitive records to maintain the confidentiality and privacy of those individuals. If staff access these records, the staff member receives an alert and the Identity Security Division (ISD) receives an automatic email to identify who has accessed the record. ISD then follows up this access with the employee's manager to understand whether there was an acceptable reason for accessing the record or whether the access was unauthorised. BD&M has also placed silent alerts on very sensitive records and if staff access these records an email is sent to the relevant Assistant Registrar to follow up.

There are insufficient controls to prevent the distribution of information in the Register

There are currently insufficient restrictions placed on the ability of staff to export and distribute information from LifeLink. Although some BD&M staff are required to export and distribute information as part of their regular duties, it is important to have controls in place to mitigate the risk of unauthorised access to and misuse of information from the Register.

Four members of staff can also use specialised software to generate reports of data from the Register as part of their role in BD&M. These staff can download a range of data from the Register to generate these reports and then distribute this data. There is an audit trail of this activity but at the time of the audit, BD&M was not reviewing this. BD&M has since commenced routine audits to address this.

It is necessary for some BD&M staff to have the ability to export and send data from the Register in order to respond to data requests from research and statistical organisations.

BD&M has not renewed its Memorandum of Understanding with Service NSW since 2016

Some Service NSW call centre staff have read-only access to LifeLink and can view any record in the system. They can also download and print information obtained through the search function in LifeLink. This means that there is the potential for unauthorised access or misuse of records. These Service NSW staff receive training from Service NSW and BD&M around the appropriate use of the LifeLink system and sign a confidentiality agreement which stipulates that they will not access information or records for any purpose other than in the course of their duties. Service NSW has its own quality assurance processes to monitor staff performance on calls.

Since 2014, BD&M manages its relationship with Service NSW through a Memorandum of Understanding (MoU). BD&M has not renewed its MoU with Service NSW since 2016. This MoU does not contain any requirements for the audit of user access or monitoring and reporting of Service NSW user activity in LifeLink.

BD&M has not performed fraud detection audits for eRegistry users

BD&M has not performed fraud detection audits of applicants or other third parties who submit registration information through eRegistry (i.e. midwives, funeral directors and marriage celebrants). Audits could analyse activity by individual eRegistry users to identify any unusual activity, for example, an unusually high number of registrations or unusual patterns in registration activity. BD&M could also carry out regular analysis and reporting to identify addresses where multiple birth certificates have been sent to identify potential fraud.

BD&M restricts access to its buildings including to certificate paper and the certificate printing room

Access to BD&M offices requires a security pass, with access to the certificate printing room and certificate paper storage requiring further authorisation. Physical access to certificate paper and the certificate printing room is restricted to those staff who require access for their job.

ISD carry out routine audits of security access. These audits examine all active access cards and ensure that staff have the correct access assigned to them and that access is removed in a timely manner when it is no longer required. They use an automatically generated report from the security access system to identify active access cards.

Certificate paper could be used to produce fraudulent documents. BD&M has policies in place and systems within LifeLink to track certificate paper. Each sheet of certificate paper has a serial number that is tracked and when certificates are printed they are scanned to ensure that the registration record in LifeLink is attached to a serial number. ISD checks the use of the certificate paper at the end of each day to ensure that all paper is accounted for. ISD also carries out routine certificate waste paper audits to ensure that certificate paper has been disposed of in line with the relevant policy.

3.3 Database security

There are no reviews of user access or monitoring of user activity in the databases and servers that sit behind the Register

The databases and servers that contain the information in the Register are hosted at a third-party vendor site. Some vendor staff and DCJ IT staff have access to the databases and servers. Neither BD&M nor DCJ, which manages the vendor, performs regular reviews of users who have this access to ensure that they are current and have a valid need to access the databases.

There are audit trails of all user activity in the databases. However, this activity is not regularly reported or reviewed by BD&M or DCJ.

BD&M does not have sufficient assurance that database security controls are effective

The vendor that hosts the LifeLink databases and the relevant servers operates an Information Security Management System that is certified against international standards. The vendor provides DCJ with the certificate for this compliance, which is intended to provide assurance that the vendor is implementing IT controls according to the standard. However, this does not provide sufficient assurance that the implemented controls are working effectively. Neither BD&M nor DCJ have performed independent audits of the vendor's IT controls to ensure they are working effectively and the vendor does not provide independent audit assurance over their existing IT controls.

While DCJ is presently responsible for managing the relationship with the vendor, there is no formal agreement between BD&M and DCJ outlining this arrangement. A more formal relationship could ensure that BD&M receives the necessary assurance over database security controls until management of the database security transitions to DCS. There is no current timeline for transitioning the database management from DCJ to DCS.

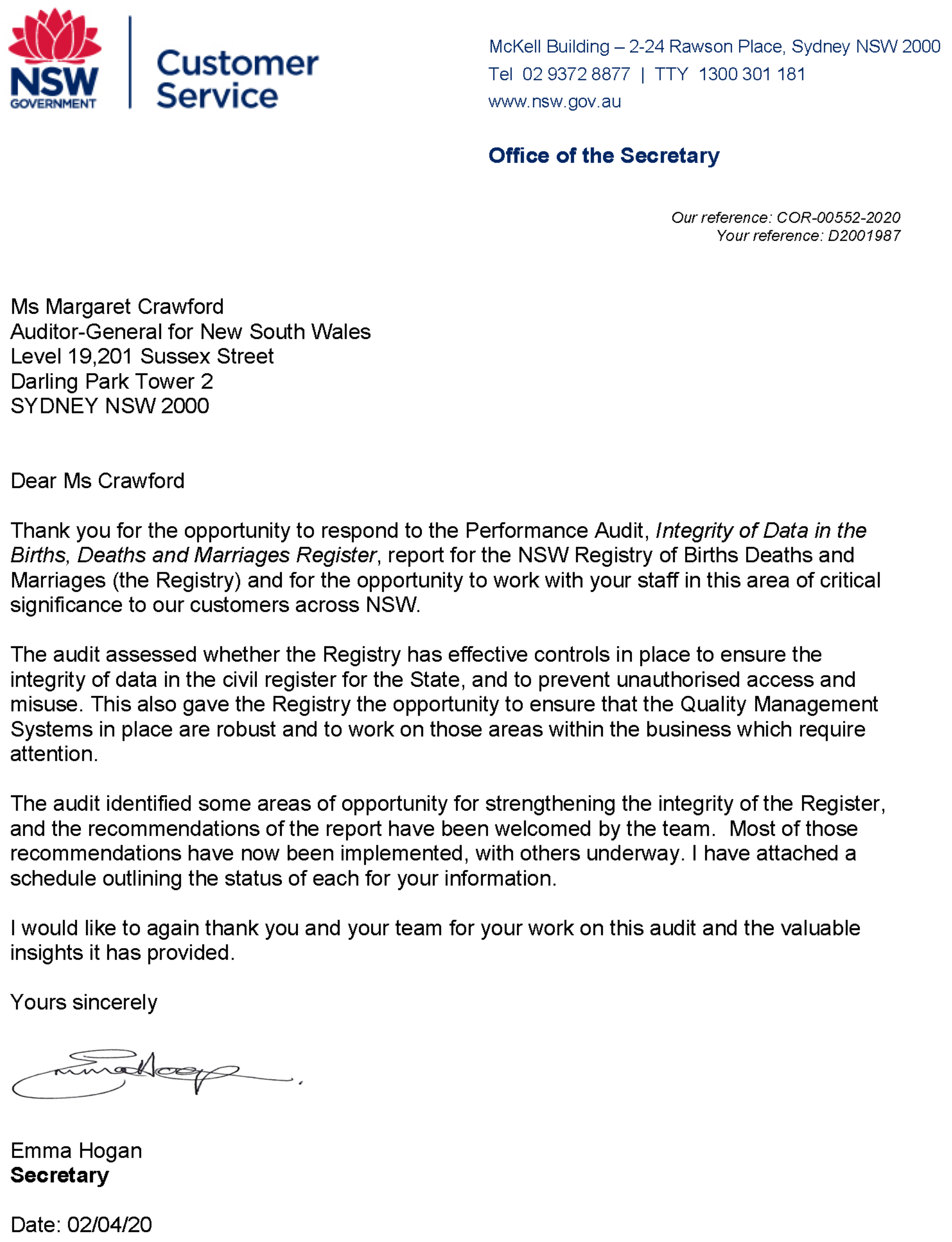
Database and relevant server password settings do not comply with DCJ's documented password policy

Individuals authorised to access the LifeLink databases and relevant servers require a user name and password. The current passwords being used to access the databases and servers are not compliant with DCJ's documented password policy.

Section two

Appendices

Appendix one – Response from agency



NSW GOVERNMENT | Customer Service

McKell Building – 2-24 Rawson Place, Sydney NSW 2000
Tel 02 9372 8877 | TTY 1300 301 181
www.nsw.gov.au

Office of the Secretary

Our reference: COR-00552-2020
Your reference: D2001987

Ms Margaret Crawford
Auditor-General for New South Wales
Level 19,201 Sussex Street
Darling Park Tower 2
SYDNEY NSW 2000

Dear Ms Crawford

Thank you for the opportunity to respond to the Performance Audit, *Integrity of Data in the Births, Deaths and Marriages Register*, report for the NSW Registry of Births Deaths and Marriages (the Registry) and for the opportunity to work with your staff in this area of critical significance to our customers across NSW.

The audit assessed whether the Registry has effective controls in place to ensure the integrity of data in the civil register for the State, and to prevent unauthorised access and misuse. This also gave the Registry the opportunity to ensure that the Quality Management Systems in place are robust and to work on those areas within the business which require attention.

The audit identified some areas of opportunity for strengthening the integrity of the Register, and the recommendations of the report have been welcomed by the team. Most of those recommendations have now been implemented, with others underway. I have attached a schedule outlining the status of each for your information.

I would like to again thank you and your team for your work on this audit and the valuable insights it has provided.

Yours sincerely

Emma Hogan
Secretary

Date: 02/04/20

Status of recommendations

Recommendation 1: As a matter of urgency, the Department of Customer Service (DCS) should ensure that the Registry of Births Deaths & Marriages (the Registry) works with the Department of Communities and Justice (DCJ) to ensure that passwords for users authorised to access the databases and servers comply with the Department of Communities and Justice's policy on password settings.

> **Response**: Accepted. The DCJ Chief Information Security Officer is facilitating the implementation of the DCS Password Policy to ensure compliance for all authorised users. It will be completed before 30 April 2020.

Recommendation 2: By July 2020, the Department of Customer Service should ensure that the Registry of Births Deaths & Marriages routinely monitors: privileged user activity in the Register, other user activity in the Register, including activity outside normal office hours, reporting software user activity.

> **Response**: Accepted. The Registrar has commenced regular Privileged Access User Activity Audits and After-Hours Access Audits through the internal audit program.

Recommendation 3: By July 2020, the Department of Customer Service should ensure that the Registry of Births Deaths & Marriages restricts the ability of LifeLink users to export and distribute information from the Register outside of legitimate actions required for their role.

> **Response**: Accepted. Information protection arrangements are being put in place to restrict the extraction, printing and emailing of LifeLink information outside of the LifeLink system, by July 2020.

Recommendation 4: By July 2020, the Department of Customer Service should ensure that the Registry of Births Deaths & Marriages updates the Service Partnership Agreement with Service NSW to include monitoring of Service NSW staff activity in the Register.

> **Response**: Accepted. Work is underway to update the Service Partnership Agreement. Action to be completed by end of July 2020.

Recommendation 5: By July 2020, the Department of Customer Service should ensure that the Registry of Births Deaths & Marriages performs regular fraud detection audits for eRegistry users.

> **Response**: Accepted. Regular fraud detection audits for eRegistry users have commenced.

Recommendation 6: By July 2020, the Department of Customer Service should ensure that the Registry of Births Deaths & Marriages works with the Department of Communities and Justice to ensure that there are regular access reviews of users of the databases and servers that sit behind the Register, there is regular monitoring of activity of users who have access to the databases and servers that sit behind the Register, there are regular audits to provide independent assurance that database security controls operate effectively.

> **Response**: Accepted. An access review process is being developed jointly by the Registry, DCJ and DCS. In addition, new database security controls will be implemented, with an external audit undertaken to independently confirm the effectiveness of security controls. Action to be completed by end of July 2020.

Recommendation 7: By July 2020, the Department of Customer Service should ensure that the Registry of Births Deaths & Marriages clarifies and formalises responsibilities with the Department of Communities and Justice in relation to the management of database security.

> **Response**: Accepted. RACI matrix is developed, and roles and responsibilities have been clearly identified. Action complete.

Recommendation 8: By December 2020, the Department of Customer Service should ensure that the Registry of Births Deaths and Marriages undertakes a risk-based analysis of the impact of gaps in the controls to prevent unauthorised user activity on the historical integrity of data in the Register.

> **Response**: Accepted. The Registry will undertake risk analyses within the required timeframe and determine action plan required to mitigate the risks identified through the analysis. Action to be completed by end of December 2020.

Recommendation 9: By December 2020, the Department of Customer Service should ensure that the Registry of Births Deaths and Marriages implements remediating action stemming from recommendation eight.

> **Response**: Accepted. The Registry will implement the action plan that is determined from response to recommendation 8. Action to be completed by end of December 2020.

Appendix two – About the audit

Audit objective

This audit assessed the effectiveness of controls in place to ensure the integrity of data in the Births, Deaths and Marriages Register, and to prevent unauthorised access and misuse.

Audit criteria

We addressed the audit objective with the following audit criteria:

1. Security controls are in place and effective to prevent unauthorised access to, and modification of, data in the Register.
2. Process and IT controls are in place and effective to ensure the integrity of data in the Register and the authenticity of records and documents.

Audit scope and focus

In assessing the criteria, we checked the following aspects:

1. Security controls are in place and effective to prevent unauthorised access to, and modification of, data in the Register.
   a) database security (including third party access, hardening and patching of the operating system and database management system and network/perimeter security)
   b) managing user access for privileged accounts and general users with edit access through the applications
   c) managing third party interfaces and access
   d) password complexity/enforced lockout
   e) physical security over infrastructure.
2. Process and IT controls are in place and effective to ensure the integrity of data in the Register and the authenticity of records and documents.
   a) enforcement of segregation of duties
   b) retention and review of audit trails or alerting
   c) input validation and data governance
   d) effective handling and processing of supporting evidence inwards and outwards
   e) controls over modification to data and outputs (e.g. birth certificates, identity check requests) including validating the authenticity of records and documents.

Audit exclusions

The audit did not:

- examine the overall effectiveness, efficiency and/or economy of the Registry's operations
- question the merits of government policy objectives.

Audit approach

Our procedures included:

1. interviewing a range of Registry staff including the Registrar, Senior Managers overseeing relevant controls and processes and staff responsible for implementing relevant controls and processes
2. examining relevant policies, procedures and training material which relate to the controls to be tested through the audit as well as recent reviews or internal audits undertaken by the Department
3. walkthroughs of the processes and controls to be tested through the audit.

The audit approach was complemented by quality assurance processes within the Audit Office to ensure compliance with professional standards.

Audit methodology

Our performance audit methodology is designed to satisfy Australian Audit Standard ASAE 3500 Performance Engagements and other professional standards. The standards require the audit team to comply with relevant ethical requirements and plan and perform the audit to obtain reasonable assurance and draw a conclusion on the audit objective. Our processes have also been designed to comply with requirements specified in the *Public Finance and Audit Act 1983* and the *Local Government Act 1993*.

Acknowledgements

We gratefully acknowledge the co-operation and assistance provided by staff at the NSW Registry of Births Deaths and Marriages and the Department of Communities and Justice.

Audit cost

The total cost of the audit is $218,000.

Appendix three – Performance auditing

What are performance audits?

Performance audits determine whether State or local government entities carry out their activities effectively, and do so economically and efficiently and in compliance with all relevant laws.

The activities examined by a performance audit may include a government program, all or part of an audited entity, or more than one entity. They can also consider particular issues which affect the whole public sector and/or the whole local government sector. They cannot question the merits of government policy objectives.

The Auditor-General’s mandate to undertake performance audits is set out in section 38B of the *Public Finance and Audit Act 1983* for State government entities, and in section 421D of the *Local Government Act 1993* for local government entities.

Why do we conduct performance audits?

Performance audits provide independent assurance to the NSW Parliament and the public.

Through their recommendations, performance audits seek to improve the value for money the community receives from government services.

Performance audits are selected at the discretion of the Auditor-General who seeks input from parliamentarians, State and local government entities, other interested stakeholders and Audit Office research.

How are performance audits selected?

When selecting and scoping topics, we aim to choose topics that reflect the interests of parliament in holding the government to account. Performance audits are selected at the discretion of the Auditor-General based on our own research, suggestions from the public, and consultation with parliamentarians, agency heads and key government stakeholders. Our three-year performance audit program is published on the website and is reviewed annually to ensure it continues to address significant issues of interest to parliament, aligns with government priorities, and reflects contemporary thinking on public sector management. Our program is sufficiently flexible to allow us to respond readily to any emerging issues.

What happens during the phases of a performance audit?

Performance audits have three key phases: planning, fieldwork and report writing.

During the planning phase, the audit team develops an understanding of the audit topic and responsible entities and defines the objective and scope of the audit.

The planning phase also identifies the audit criteria. These are standards of performance against which the audited entity, program or activities are assessed. Criteria may be based on relevant legislation, internal policies and procedures, industry standards, best practice, government targets, benchmarks or published guidelines.

At the completion of fieldwork, the audit team meets with management representatives to discuss all significant matters arising out of the audit. Following this, a draft performance audit report is prepared.

The audit team then meets with management representatives to check that facts presented in the draft report are accurate and to seek input in developing practical recommendations on areas of improvement.

A final report is then provided to the head of the audited entity who is invited to formally respond to the report. The report presented to the NSW Parliament includes any response from the head of the audited entity. The relevant minister and the Treasurer are also provided with a copy of the final report. In performance audits that involve multiple entities, there may be responses from more than one audited entity or from a nominated coordinating entity.

Who checks to see if recommendations have been implemented?

After the report is presented to the NSW Parliament, it is usual for the entity's audit committee to monitor progress with the implementation of recommendations.

In addition, it is the practice of Parliament's Public Accounts Committee to conduct reviews or hold inquiries into matters raised in performance audit reports. The reviews and inquiries are usually held 12 months after the report received by the NSW Parliament. These reports are available on the NSW Parliament website.

Who audits the auditors?

Our performance audits are subject to internal and external quality reviews against relevant Australian and international standards.

The Public Accounts Committee appoints an independent reviewer to report on compliance with auditing practices and standards every four years. The reviewer's report is presented to the NSW Parliament and available on its website.

Periodic peer reviews by other Audit Offices test our activities against relevant standards and better practice.

Each audit is subject to internal review prior to its release.

Who pays for performance audits?

No fee is charged for performance audits. Our performance audit services are funded by the NSW Parliament.

Further information and copies of reports

For further information, including copies of performance audit reports and a list of audits currently in-progress, please see our website www.audit.n.gov.au or contact us on 02 9275 7100.

Professional people with purpose

OUR VISION

Our insights inform and challenge government to improve outcomes for citizens.

OUR PURPOSE

To help parliament hold government accountable for its use of public resources.

OUR VALUES

Pride in purpose

Curious and open-minded

Valuing people

Contagious integrity

Courage (even when it's uncomfortable)

auditoffice
OF NEW SOUTH WALES

audit.nsw.gov.au

Level 19, Darling Park Tower 2
201 Sussex Street
Sydney NSW 2000 Australia

PHONE +61 2 9275 7100
FAX +61 2 9275 7200

mail@audit.nsw.gov.au

Office hours: 8.30am-5.00pm

auditoffice
OF NEW SOUTH WALES

audit.nsw.gov.au