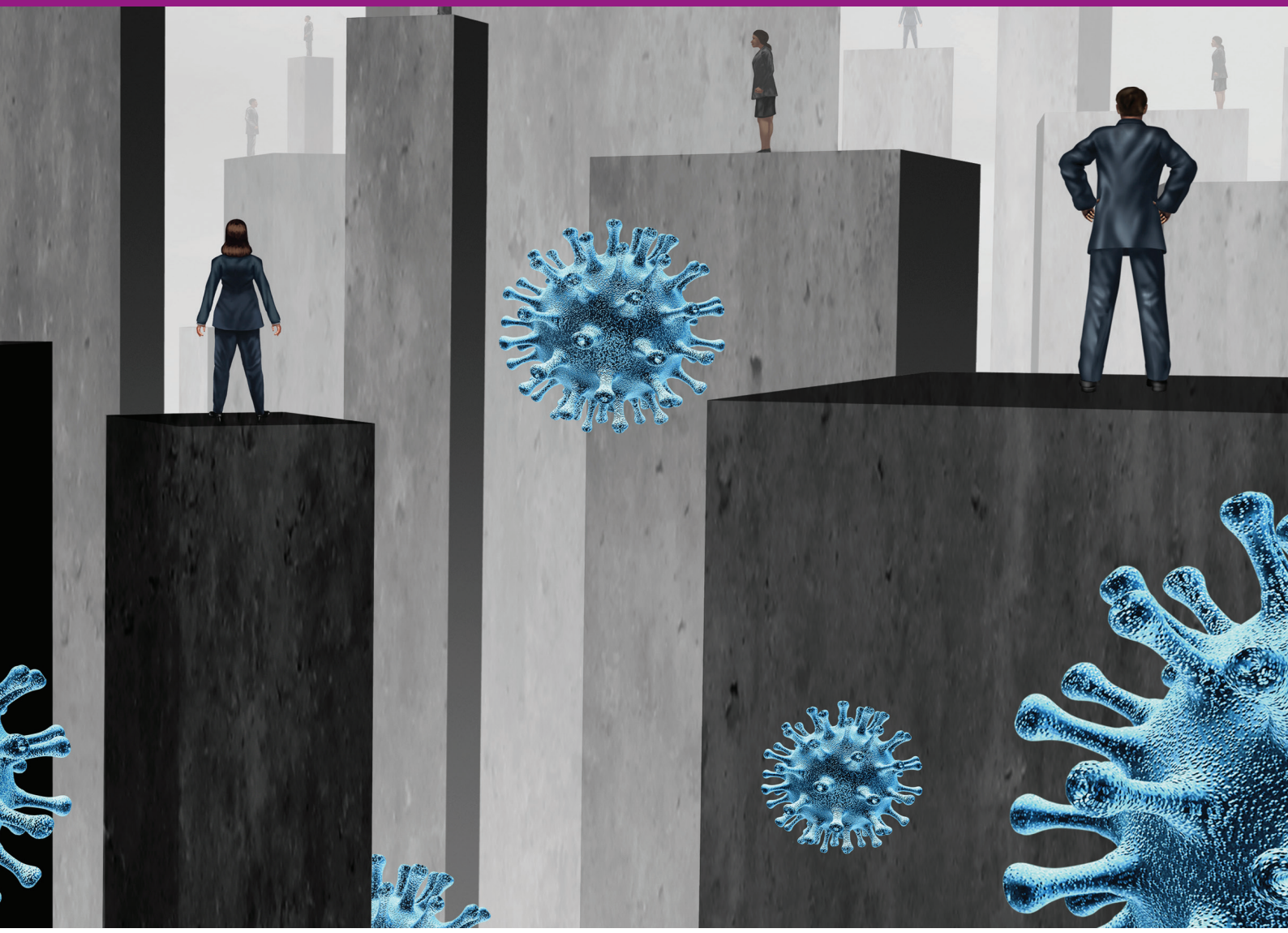
Report of the Auditor-General

Auditor-General's Department

Report 13 of 2021

COVID-SAfe Check-In review



Government of South Australia

[P.P.4ZB

Report of the Auditor-General

Report 13 of 2021

COVID-SAfe Check-In review

Tabled in the House of Assembly and ordered to be published, 12 October 2021

Second Session, Fifty-Fourth Parliament

By authority: S. Smith, Government Printer, South Australia

2021

The Auditor-General's Department acknowledges and respects Aboriginal people as the State's first people and nations, and recognises Aboriginal people as traditional owners and occupants of South Australian land and waters.

Auditor-General's
Department

www.audit.sa.gov.au

Enquiries about this report should be directed to:

Auditor-General
Auditor-General's Department
Level 9, 200 Victoria Square
Adelaide SA 5000

ISSN 0815-9157

Government of South Australia
Auditor-General's Department

Level 9
State Administration Centre
200 Victoria Square
Adelaide SA 5000
Tel +618 8226 9640
Fax +618 8226 9688
ABN 53 327 061 410
audgensa@audit.sa.gov.au
www.audit.sa.gov.au

30 September 2021

President
Legislative Council
Parliament House
ADELAIDE SA 5000

Speaker
House of Assembly
Parliament House
ADELAIDE SA 5000

Dear President and Speaker

Report of the Auditor-General: Report 13 of 2021 *COVID-SAfe Check-In review*

Under section 36(1)(a)(iii) of the *Public Finance and Audit Act 1987* (PFAA), I have conducted an review of the COVID-SAfe Check-In app.

Our objective was to conclude on the controls applied to manage people's contact details captured through the COVID-SAfe Check-In app for contact tracing purposes. This covered both the Department of Premier and Cabinet (DPC) and the Department for Health and Wellbeing's (SA Health) data management, protection and disposal arrangements.

I present to each of you my independent assurance report on the findings of the audit.

A copy of this report has also been provided to DPC, SA Health and the State Coordinator.

Content of the Report

The COVID-SAfe Check-In app was developed quickly and implemented in December 2020 within the existing mySA GOV app used for digital passes and licences. It has been vitally important for enhancing the State's COVID-19 contact tracing processes.

DPC and SA Health have different responsibilities and systems for data captured by the COVID-SAfe Check-In app. DPC developed the app and operates the system that manages all the data it captures. SA Health receives only a subset of the captured data and uses systems to manage specific COVID-19 contact tracing processes.

Overall, I concluded that reasonable controls were applied by DPC and SA Health to protect people's contact details obtained through the COVID-SAfe Check-In app. I note this is a point in time review and opinion. IT systems are subject to changing circumstances and the ongoing management of system changes and security is a key management responsibility.

For DPC, our testing found that the controls implemented to secure the data captured by the COVID-SAfe Check-In app were reasonable. This includes controls applied to the database and supporting IT environment.

For SA Health, some controls applied over its COVID management systems were reasonable. Other controls need strengthening to provide better security of people's contact details.

The key findings and positive observations supporting my opinion are summarised in section 1.3.

Acknowledgements

The audit team for this Report was Andrew Corrigan and Tyson Hancock.

We appreciate the cooperation and assistance given by staff of DPC, SA Health and State Coordinator and during the review.

Yours sincerely

Andrew Richardson
Auditor-General

Contents

1 Executive summary

1.1 Introduction

In early May 2020, the SA Government established a Transition Committee to help guide the State out of the COVID-19 health emergency and restore its social and economic health. The Transition Committee developed compliance rules, including the requirement for defined public activities to have COVID plans[1] and contact tracing records for the people attending them.

South Australia was able to relax some of the initial COVID-19 public health restrictions as 2020 progressed and the pandemic remained relatively under control here. To continue keeping the community safe, the Department of Health and Wellbeing (SA Health) sought to enhance the State's contact tracing processes so that in the event of an outbreak anyone at risk could be quickly identified. SA Health asked the Transition Committee to investigate ways to do this.

In October 2020 the COVID-SAfe Check-In project began, managed by the Department of the Premier and Cabinet (DPC). It aimed to develop a QR code app to identify people entering a business, venue, event or gathering operating under a COVID plan.

In November 2020, a suspected COVID-19 case was identified in the community. It was the start of what became the Parafield Cluster. SA Health urgently tried to perform contact tracing to understand the extent of the suspected outbreak. This triggered a six-day statewide lockdown, which was subsequently reduced to three days. It highlighted the need for more efficient and timely identification of contacts. The small team on the COVID-SAfe Check-In project continued working to quickly deliver a solution.

In December 2020 the project team's QR code check-in solution, the COVID-SAfe Check-In app, was released. It collects a user's name, phone number and date and time of visit when a QR code is scanned. Daily check-ins on the app recently exceeded two million.

As the global vaccine rollout progresses, continuing local economic and social activity while adhering to public health controls are community priorities. Introducing the COVID-SAfe Check-In app is one mechanism the SA Government is using to manage health risks and mitigate the risk of further economic downturn and disruption.

While the citizen information collected by the COVID-SAfe Check-In app is critical to its purpose, how the SA Government protects the privacy and security of this information is of keen public interest. We have a longstanding practice of reviewing and reporting on information system projects like this.

In December 2020, I received a letter from DPC asking me to conduct an examination of the COVID-SAfe Check-In project. It is important the community trusts and uses the app, so I exercised my *Public Finance and Audit Act 1987* discretion to review the project. We focused on DPC and SA Health's data management, protection and disposal arrangements.

Because responsibilities for the collected information exist in both agencies, this report has separate sections for overall governance, DPC and SA Health (refer to sections 4 to 7).

[1] A COVID Safe Plan or COVID Management Plan as prescribed under the Emergency Management (Public Activities No 27) (COVID-19) Direction 2021, issued 1 July 2021.

1.2 Conclusion

The COVID-SAfe Check-In app was developed quickly and implemented in December 2020 within the existing mySA GOV app used for digital passes and licences. It has been vitally important for enhancing the State's COVID-19 contact tracing processes.

DPC and SA Health have different responsibilities and systems for data captured by the COVID-SAfe Check-In app. DPC developed the app and operates the system that manages all the data it captures. SA Health receives only a subset of the captured data and uses systems to manage specific COVID-19 contact tracing processes.

Overall, I concluded that reasonable controls were applied by DPC and SA Health to protect people's contact details obtained through the COVID-SAfe Check-In app. I note this is a point in time review and opinion. IT systems are subject to changing circumstances and the ongoing management of system changes and security is a key management responsibility.

For DPC, our testing found that the controls implemented to secure the data captured by the COVID-SAfe Check-In app were reasonable. This includes controls applied to the database and supporting IT environment.

For SA Health, some controls applied over its COVID management systems were reasonable. Other controls need strengthening to provide better security.

The key findings and positive observations supporting my opinion are summarised in section 1.3 and include the following matters.

The South Australian Cyber Security Framework requires a clear asset owner to be assigned for the COVID-Safe systems. Formalising this will ensure clarity for managing the Check-In app and associated IT environments.

DPC has a regular process for destroying COVID-SAfe Check-In data older than 28 days from the production database. DPC regularly backs up the COVID-SAfe IT environment in line with responsible and vital practice for recovering critical systems in the event of a disaster or system failure. The backups are retained indefinitely and secured in line with DPC's accreditation for holding protected data. Backups hold contact data that is older than 28 days, but controls exist to prevent unauthorised restorations. DPC advised us that the restoration process would instantly remove data if it was over 28 days old. DPC also intends to destroy its backups when contact tracing in the State is no longer required.

Under directions issued under the *Emergency Management Act 2004* (EM Act), data extracted from the prescribed database and provided to SA Health by DPC for contact tracing purposes is information obtained under the *Health Care Act 2008* (Health Act). The Health Act makes detailed provisions for the protection and confidentiality of information. SA Health retains the data it receives indefinitely, in line with its responsibilities under the Health Act. For clarity of community messaging about the retention of data, it would be helpful if SA Health's public communications include information about this requirement, such as on websites and in digital media.

All findings received positive responses from the responsible agencies.

1.3 What we found

Our key findings and positive observations are summarised in figure 1.1 and more details are provided in sections 4 to 7.

Figure 1.1: Key findings and positive observations

Agency/Authority	Findings
State Coordinator (section 4)	The following key findings need attention: • There is no clear information asset owner of the COVID-SAfe Check-In app, database and supporting IT environment. • A strong information classification is used but not formally documented for the COVID-SAfe Check-In app and associated IT environment. • The State's end-to-end COVID-SAfe Check-In IT processes are not clearly and formally documented.
Department of the Premier and Cabinet (section 5)	We made the following positive observations: • There is a regular process for destroying COVID-SAfe Check-In data older than 28 days from the production database. • DPC followed good practice to develop and release the COVID-SAfe Check-In app quickly. • Encryption techniques are used to secure people's contact details. • User access management processes are industry best practice. • Physical security of the COVID-SAfe Check-In environment is industry best practice. • Security vetting occurs for users with access to the data. The following key findings need attention: • Backups of COVID-SAfe Check-In data are kept beyond 28 days of capture. Controls exist to prevent unauthorised restorations and DPC advised that the restoration process would instantly remove data if it was more than 28 days old. • Some components of the COVID-SAfe Check-In IT environment are not included in DPC's overarching Cyber Security Program. • A full risk assessment has not been performed to confirm the adequacy of end-to-end COVID-SAfe Check-In controls.

Agency/Authority	Findings
Department for Health and Wellbeing (section 6)	We made the following positive observations: • Sound change management processes were applied. • Security vetting and training is performed for users with access to the data. The following key findings need attention: • Data retention varies under the *Health Care Act 2008,* the EM Act and the State Records disposal determination. • No formal SA Health owner and information classification is assigned to the Contact Management Database (CMDB). • A full risk assessment has not been performed to confirm the adequacy of the end-to-end COVID management systems controls. • User access management practices need improvement. • Physical security could be improved. • A security impact assessment and penetration test has not been performed for the CMDB.
Department of the Premier and Cabinet and Department for Health and Wellbeing (section 7)	The following additional finding needs attention: • DPC's ICT and Digital Government Division and SA Health's COVID Operations unit are not included in their respective agency Information Security Management System (ISMS).[2]

1.4 What we recommended

Our key recommendations are summarised in figure 1.2.

Figure 1.2: Key recommendations

Agency/Authority	Recommendations
State Coordinator (section 4)	• Establish a clear asset owner for the COVID-SAfe Check-In app and associated IT environment. Once established, an information classification level should be formally assigned and documented. • Documentation describing the State's end-to-end COVID-SAfe Check-In IT processes should be finalised by the information custodians (DPC and SA Health) and approved by the relevant information asset owners.

[2] An ISMS aims to preserve the confidentiality, integrity and availability of information by applying a risk management process. ISMS implementation also gives stakeholders confidence that organisations have adequately managed risks and fully understand and appreciate agency assets/systems.

Agency/Authority	Recommendations
Department of the Premier and Cabinet (section 5)	• Update backup restoration policy and procedures to include the requirement for COVID-SAfe Check-In data older than 28 days to be immediately destroyed once a required restoration is complete. • Expand the scope of DPC's Cyber Security Program to ensure that it includes all components of the COVID-SAfe Check-In app and associated environment. • Perform a full risk assessment of the end-to-end COVID-SAfe Check-In controls.
Department for Health and Wellbeing (section 6)	• For clarity about retention of data received for contact tracing purposes, it would be helpful if public communications include advice of requirements of the Health Act. SA Health should also review the requirements of this Act against the EM Act and State Records' November 2020 disposal determination. • Ensure that the CMDB is identified, recorded and classified according to the South Australian Information Classification Scheme. • Perform a full risk assessment of the COVID management systems. • Address the user account exceptions identified and strengthen user access administration processes. • Re-locate the CMDB application server to an appropriately secured Digital Health managed on-premise server room.
Department of the Premier and Cabinet and Department for Health and Wellbeing (section 7)	• Review the current and future state Cyber Security Programs and security operating models to ensure they cover all primary agency functions.

1.5 Response to our recommendations

The State Coordinator, DPC and SA Health responded positively to our findings and recommendations.

The State Coordinator noted that the COVID-SAfe Check-In app was developed and implemented quickly in response to the rapidly evolving nature of the pandemic in November 2020, and that it has operated successfully since then.

Specific responses to our findings are provided in sections 4 to 7.

2 Background

On 28 January 2020, the Minister for Health and Wellbeing declared the human coronavirus with pandemic potential to be a controlled notifiable condition under the *South Australian Public Health Act 2011*. In mid-March 2020, SA Health declared that the threat of COVID-19 was a public health emergency under the Health Act.

On 22 March 2020 the State Coordinator (the South Australian Commissioner of Police) declared a major emergency under section 23(1) of the EM Act for the outbreak of COVID-19 in South Australia.

Certain directions were issued under sections 15, 16 and 18 of the EM Act to manage the State's COVID-19 response. This included limiting gatherings, and introducing social distancing. Businesses closed or operated under restrictions and workforces went home and stayed home for some months. Other widespread restrictions were implemented, to varying degrees.[3]

2.1 Contact tracing overview

Early in the pandemic the Commonwealth Government developed a COVIDsafe app[4] designed to help stop the spread of the virus across the country. State and Territory health authorities were also developing their own contact tracing processes. This included identifying all people suspected to have had close contact with a person infected with COVID-19.

Contact tracing records for defined public activities were first required under section 13(4) of Emergency Management (Public Activities) (COVID-19) Direction 2020 issued on 1 June 2020.

At the time of our review, Public Activities Direction 27[5] (Direction 27) was the current direction. Schedule 3(10) of Direction 27 defines contact tracing as:

> *… the process of identifying, assessing and managing persons who have been, or may have been, in contact with a person who has, or who may have, COVID-19.*

Schedule 3(10)(a-f) of Direction 27 then specifies several instances when there is a need to notify a person (or parent, guardian or carer of another person), determine locations where a person has visited and provide information and advice to impacted people.

---

[3] Auditor-General's Report 13 of 2020 *Annual Report for the year ended 30 June 2020* Part A: Executive summary included details of some key COVID-19 pandemic events that occurred in South Australia in 2019-20.

[4] The Commonwealth Government COVIDsafe app is separate from the COVID-SAfe Check-In app developed by DPC.

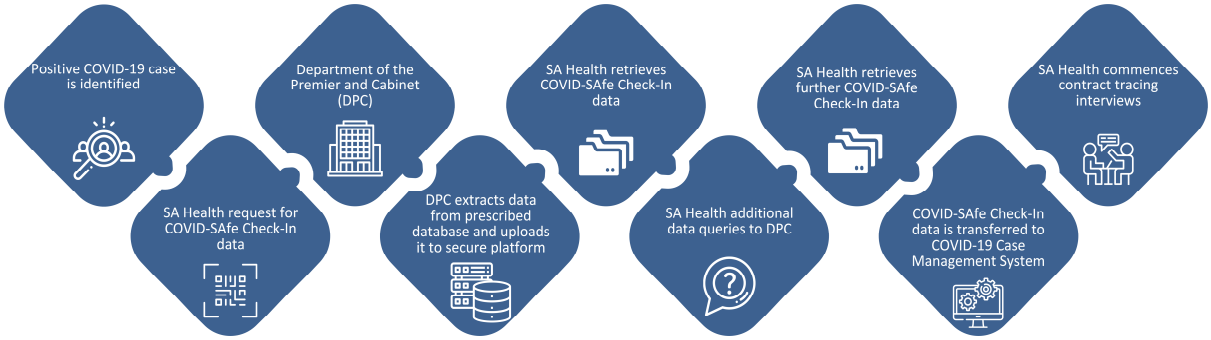
[5] Emergency Management (Public Activities No 27) (COVID-19) Direction 2021, issued 1 July 2021.

DPC developed the COVID-SAfe Check-In app to enhance the State's contact tracing processes. DPC and SA Health developed a process for SA Health's COVID Operations unit to request contact details captured through the app, when they are needed to manage an outbreak of COVID-19 in South Australia. Currently, SA Health's COVID Operations unit conducts an outbreak risk assessment before data requests are sent by email to DPC. The requested data is then transferred to SA Health through an encrypted portal.

The information requested by SA Health is a small subset of the information stored in DPC's prescribed database[6] (DPC's database), focused only on relevant points of interest.

This process and key roles and responsibilities are shown in figure 2.1.

Figure 2.1: COVID-19 contact tracing process



Schedule 3(7) of Direction 27 prescribes that:

> *Relevant contact details extracted from the prescribed database and provided to SA Health for contact tracing purposes is taken to be information obtained in connection with the operation of the* Health Care Act 2008 *and is protected under that Act.*[7]

Other than the standard COVID-19 contact tracing requests, SA Health advised us that it currently performs contact tracing for several other purposes to manage the COVID-19 pandemic.[8] These include:

- from a whole of population perspective, to determine the risk to the general community following a confirmed positive sample of wastewater that aligns with a high-risk public event
- statistical information on the number of people who check in to a particular high-risk event to determine the level of compliance of a business to its COVID-19 management plans and individuals using the COVID-SAfe Check-In app.

---

6 Schedule 3(10) of Direction 27 establishes DPC's prescribed database for storing contact details captured in an approved contact tracing system.

7 *Health Care Act 2008*, section 93—Confidentiality.

8 Schedule 3(6) of Direction 27 restricts the use of contact details collected to contact tracing in relation to COVID-19 and managing the COVID-19 pandemic.

SA Health stated that no personal identifying information is supplied to them from the COVID-SAfe Check-In app as part of these non-standard requests. We could not test this as the COVID-SAfe Check-In data retrieved by SA Health through the secure file transfer mechanism is deleted after three days.

In response to our inquiry, DPC indicated that it scrutinises SA Health's requests to ensure they only provide what is relevant for the situation and discusses these issues with SA Health as part of any non-standard request.

2.2 COVID-SAfe Check-In overview

2.2.1 The COVID-SAfe Check-In Project

The COVID-SAfe Check-In Project was authorised by the State Coordinator following a request from SA Health's COVID Operations unit to the Transition Committee[9] to enhance the State's COVID-19 contact tracing processes.

DPC managed the project, which involved a small team that started work in late-October 2020. The project was overseen by a Technical Advisory Group.[10]

The QR code check-in app (COVID-SAfe Check-In) was developed within the existing mySA GOV app, used for digital passes and licences. This app was selected by the project as it provided an interface that had previously been security tested and could be used to integrate QR scanning functionality. Creating a separate user interface would have taken more time.

The COVID-SAfe Check-In app was implemented on 1 December 2020. It is available for download on smart phones.

Users who have created a mySA GOV account have their digital passes, licencing and registration details retrieved from the Department for Infrastructure and Transport's licencing and registration system[11] and Consumer and Business Services' occupational licencing system.[12] These are separate interfaces to the COVID-SAfe Check-In and are shown in figure 2.2 below.

---

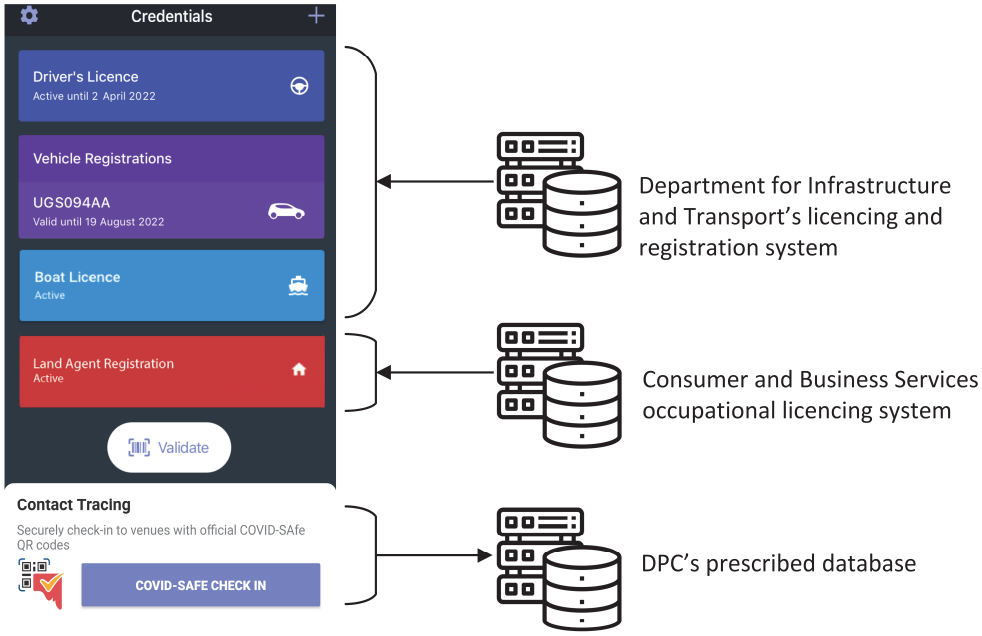
9 <https://www.premier.sa.gov.au/news/media-releases/news/sa-establishes-transition-team-to-manage-post-covid-19>, viewed 28 April 2021. The Transition Committee included key representatives from SA Health, DPC, South Australia Police, the Department of Treasury and Finance and the Department for Trade and Investment.

10 This group was established as a subcommittee of the Transition Committee. Its membership comprises DPC, SA Health, South Australia Police and the Department for Infrastructure and Transport. It provides a support and oversight role for digital COVID-19 solutions.

11 Examples include driver's licences and permits, motor vehicle registrations and boat licences.

12 Examples include licences for security and investigation agents, builders, plumbers, gas fitters, electricians and real estate agents.

Figure 2.2: Information flow for content on mySA GOV app

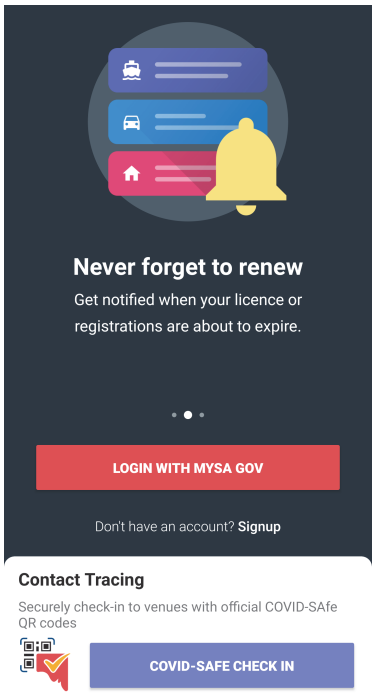


DPC manages the ongoing operations of the COVID-SAfe Check-In app, database and associated IT environment.

SA Health's COVID Operations unit implemented two COVID management systems. The COVID-19 Case Management System (CMS) was implemented to support COVID-19 case management and contact tracing processes. The Contact Management Database (CMDB) is a collection of applications and services supporting COVID contact management and other COVID operational processes.

The new QR code check-in feature appears at the bottom of the mySA GOV app, as shown in figure 2.3.

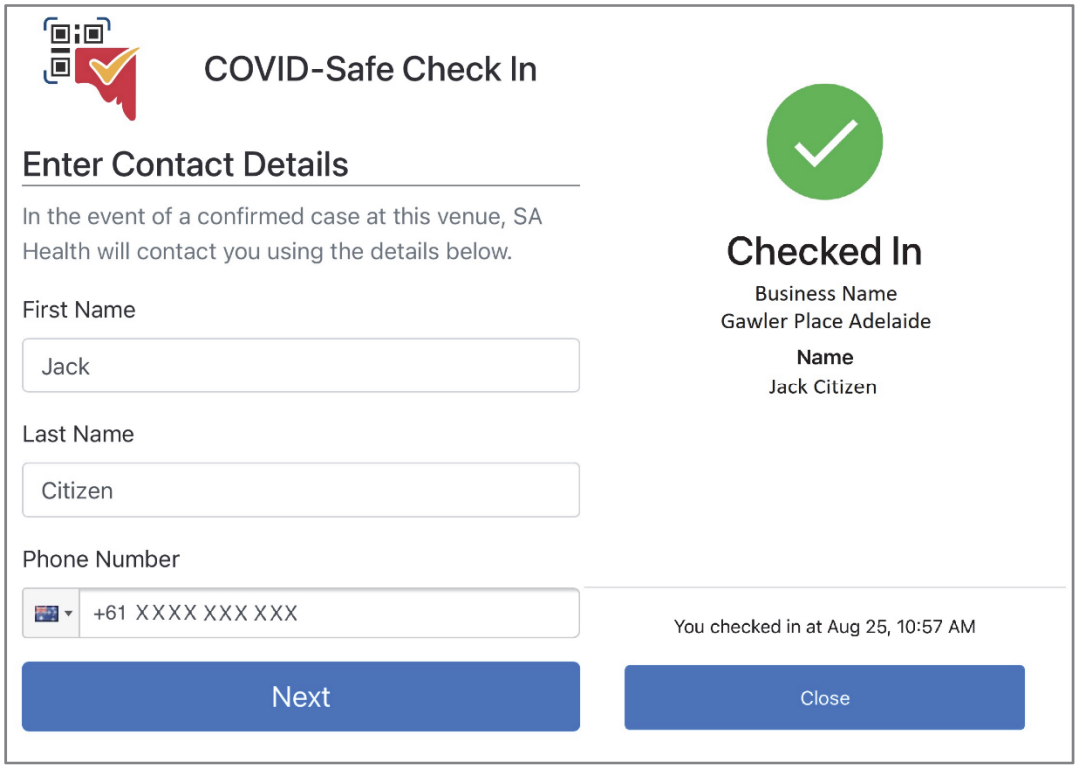
Figure 2.3: mySA GOV home screen with COVID-SAfe Check-In app



Users do not need to create an account to use the COVID-SAfe Check-In feature. To use it, users must enter their first name, last name and mobile phone number (see figure 2.4). This supports the essential contact tracing purpose of the app.

Users can also use a web version of the check-in with any QR code reader and do not have to use the mySA GOV app.

Figure 2.4: COVID-SAfe Check-In initial entry of contact details



2.2.2 Project challenges

2.2.2.1 The COVID-SAfe Check-In app was delivered quickly

The COVID-SAfe Check-In project commenced in late-October 2020 with a small team of DPC resources allocated. In mid-November 2020, a suspected COVID-19 case was identified in the community in the Adelaide metropolitan area. This triggered a six-day statewide lockdown, which was subsequently reduced to three days. Consequently, there was significant urgency to enhance the State's contact tracing capability.

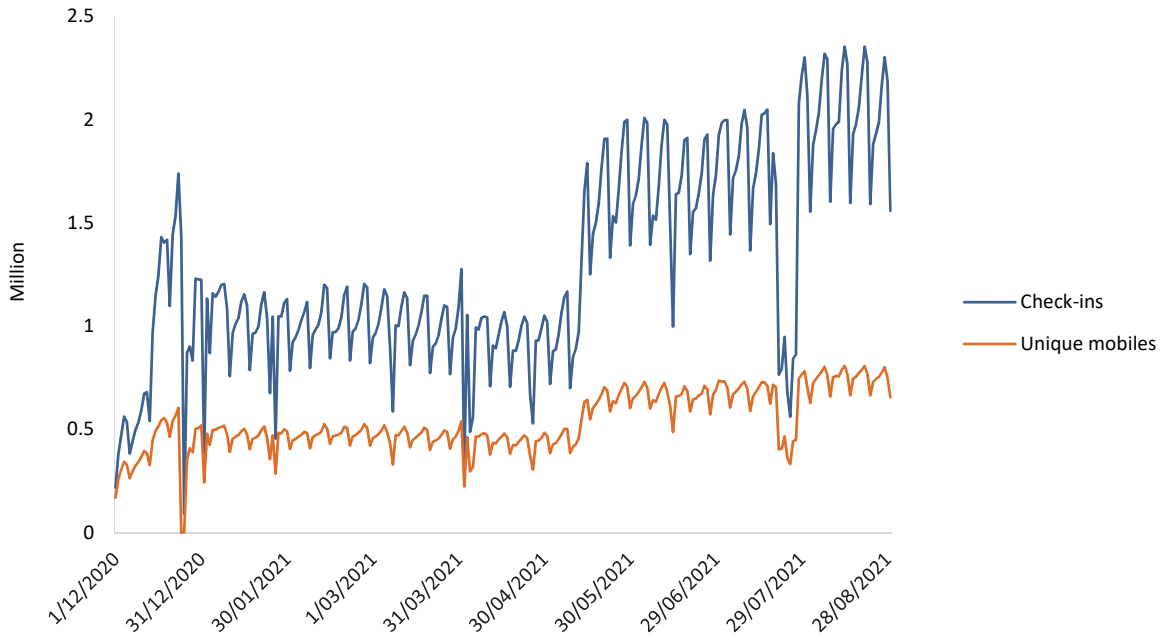
DPC advised us that although the project experienced challenges, the COVID-SAfe Check-In app was made available on 1 December 2020. At the time of our review, DPC indicated that there were few reported public complaints or issues with the app's performance.

2.2.2.2 Public use and risk of complacency

DPC advised us that initial public take-up of the COVID-SAfe Check-In app was acceptable and its ongoing use has been relatively stable (see figure 2.5).

We noted that in July 2021, daily check-ins were exceeding two million.

Figure 2.5: Total check-ins and unique mobile check-ins per day since inception



In reviewing the check-in data, we noted that check-ins appear to drop on weekends by an average of around 200 000, before climbing again on weekdays. DPC advised us that the volume of check-ins may be greater due to school and business check-ins on weekdays.

DPC further advised us that it does not perform any detailed analysis on the data other than acknowledging the general check-in patterns. The data is only interrogated when performing contact tracing or risk assessments.

DPC acknowledged that there is an ongoing risk of public complacency and/or forgetting to check in while there is no local community transmission. In mid-May 2021, South Australia Police (SAPOL) launched 'Operation Trace', intended to remind the public of their obligation to scan using the QR code check-in app when they enter a business or attend a public activity. SAPOL advised that it would use plain clothes police officers to ensure people are complying.[13] We noted that check-ins spiked after this announcement (as seen in figure 2.5) and have remained at this higher level.

In July 2021, an incident in Tailem Bend indicated that the COVID-SAfe Check-In app was not used by all people who attended contact tracing sites of interest. This suggests there was still a need for the public to increase its use of the app to enhance contact tracing.[14]

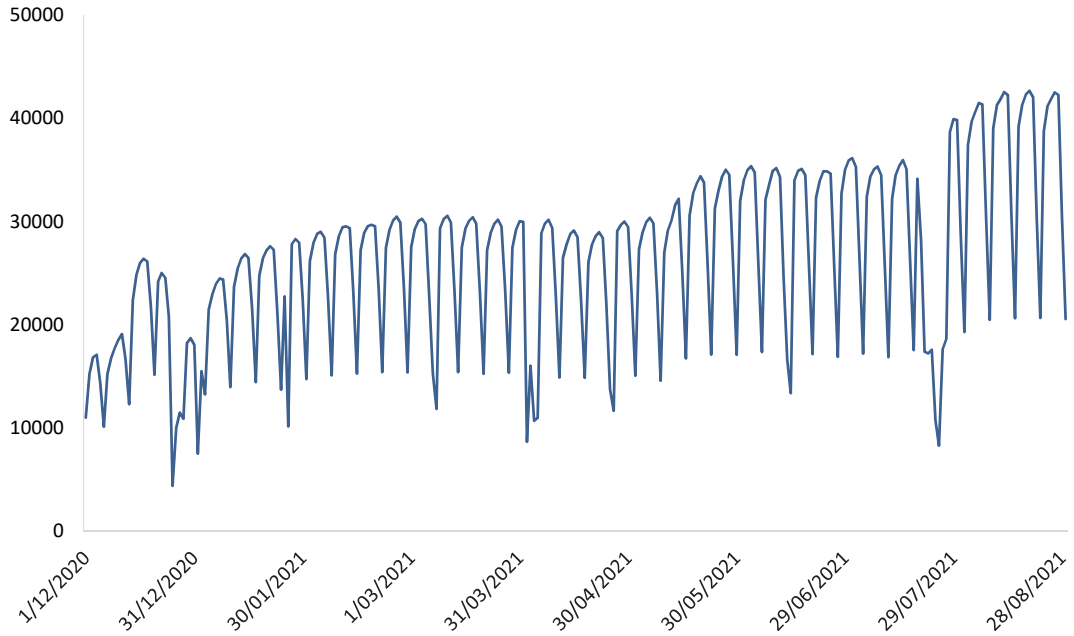
---

[13] <https://www.police.sa.gov.au/sa-police-news-assets/front-page-news/launch-of-operation-trace#.YK9AyY3is2w>, viewed 27 May 2021.

[14] On 15 July 2021, the State Coordinator advised the public that there had only been 25 QR code check-ins at the Tailem Bend locations during the time of concern, compared to 76 credit card transactions. <https://7news.com.au/lifestyle/health-wellbeing/sa-on-notice-over-potential-virus-cases-c-3404961>, viewed 2 August 2021.

Figure 2.6 shows the extent of businesses/organisations actively using the COVID-SAfe Check-In app.

Figure 2.6: COVID-SAfe active organisations per day since inception



We did not access any personal data to prepare these figures. At the time of this report this high-level check-in data was publicly available on an SA Government website.[15]

2.3 Relevant law and guidance

When the Commonwealth Government makes recommendations to the States about restriction guidelines relating to COVID-19, each State must then consider how to apply them. In South Australia, the State Coordinator is responsible for declaring an emergency and for managing and coordinating the response and recovery operations under the EM Act. After declaring a major emergency under section 23(1) of the EM Act, the State Coordinator must publish a Direction or requirement on a website within 24 hours under section 25 of the EM Act. Direction 27 was made under this provision.[16]

In 2020-21, several declarations and directions were made under the EM Act and the *South Australia Public Health Act 2011* that relate to the COVID-19 pandemic. Examples of these directions include:

- restrictions on public activities
- cross-border travel restrictions
- restricted access to residential aged care facilities
- exposure location testing requirements
- supervised quarantine

[15] <https://data.sa.gov.au/data/dataset/covid-safe-checkins/resource/a78b4b4f-834f-4e90-b38a-b3f12750bea5>, viewed 5 May 2021.

[16] The *COVID-19 Emergency Response Act 2020* modified section 25(3) of the EM Act to this effect.

- quarantine and testing for interstate arrivals
- isolation following diagnosis or close contact
- restrictions on the use of specific COVID-19 tests
- reporting on COVID-19 testing
- stay-at-home orders
- overseas travel self-quarantine.

Some declarations and directions were updated or withdrawn as the pandemic progressed.

2.3.1 Check-in and records requirements and penalties for non-compliance

2.3.1.1 Capturing information through an approved contact tracing system

Public Activities Direction 13[17] under the EM Act was updated at the start of December 2020 to coincide with the introduction of approved contact tracing systems and records management. This was to enforce the requirement for the public to use the approved contact tracing system (COVID-SAfe Check-In app)[18] to capture the contact details of a person who has entered a business/place/activity.[19]

At the time of our review Schedule 3(1) of Direction 27 required:

> *(a) an approved contact tracing system is enabled at the place so as to capture the relevant contact details of persons entering the place; and*
>
> *(b) all persons entering the place upload their relevant contact details to the approved contact tracing system on entry or as soon as reasonably practicable after entry.*

The COVID-SAfe Check-In app collects an individual user's name, mobile phone number and date and time of visit to the business/place/activity. The mobile phone number is validated by an SMS code to ensure integrity of the data.

2.3.1.2 Capturing contact details in written or verbal form

Schedule 3(3)(a) and (b) of Direction 24 prescribe requirements if a person's contact details cannot be captured by the approved contact tracing system. For example, when electricity or internet connection prevents its proper use, or the person does not have a smartphone.

These sections also note circumstances in which it might not be possible for the person entering a place to provide their contact details. This includes when they are unable to communicate this information to the venue in written or verbal form. A responsible person (eg the business owner or person in charge of the activity) or a companion of the person entering may record or provide the relevant contact details on behalf of the person entering.

---

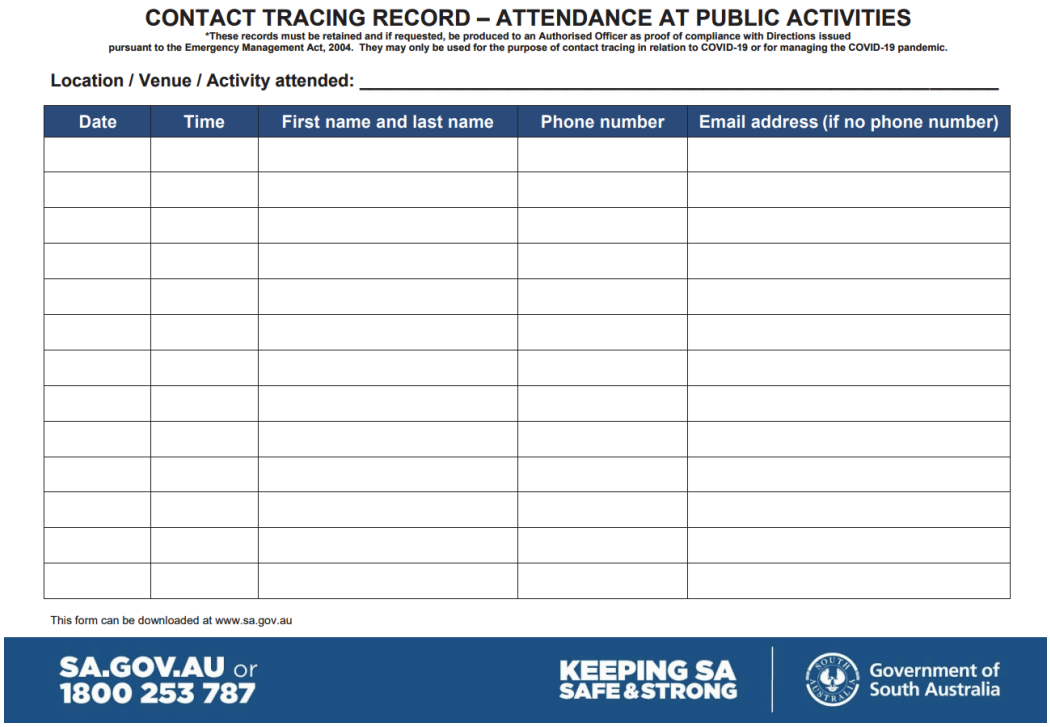
[17] Emergency Management (Public Activities No 13) (COVID-19) Direction 2020.

[18] Direction 27, Schedule 3(10) prescribes that privately sourced or alternative electronic platforms or systems for capturing contact details are not approved contact tracing systems.

[19] We note that section 10(7) of Public Activities Direction 13 also included ScanTek as an approved contact tracing system. DPC advised us that this system was not implemented for contact tracing purposes.

The State's COVID-19 website provides a template to capture the same information as is captured by the COVID-SAfe Check-In app as contact tracing records for people entering a business/place/activity.

Figure 2.7: Contact tracing attendance record template



CONTACT TRACING RECORD – ATTENDANCE AT PUBLIC ACTIVITIES

*These records must be retained and if requested, be produced to an Authorised Officer as proof of compliance with Directions issued pursuant to the Emergency Management Act, 2004. They may only be used for the purpose of contact tracing in relation to COVID-19 or for managing the COVID-19 pandemic.

Location / Venue / Activity attended: _____

Date	Time	First name and last name	Phone number	Email address (if no phone number)

This form can be downloaded at www.sa.gov.au

SA.GOV.AU or 1800 253 787 KEEPING SA SAFE & STRONG Government of South Australia

Regardless of the circumstances, the responsible person must make and retain contact tracing records and the person entering a place must provide their contact details.[20] These hardcopy records must be destroyed within the prescribed period of 28 days.[21]

2.3.1.3 Use for proper purpose

Schedule 3(6) of Direction 27 prescribes that:

> *The relevant contact details captured by the approved contact tracing system under this or any other direction made under the* Emergency Management Act 2004 *may only be used for the purpose of contact tracing in relation to COVID-19 or for managing the COVID-19 pandemic.*

2.3.1.4 Penalties for non-compliance

We sought advice on the legislative enforcement of penalties against a business/place/activity and individuals for not complying with the COVID-SAfe Check-In process.

Section 28(1) of the EM Act provides for prosecuting offenders for not complying with directions under the EM Act. This includes a maximum penalty of $75 000 for a body corporate and $20 000 or imprisonment for two years for a person.

[20] Direction 27, Schedule 3(3)(a) and (b).
[21] Direction 27, Schedule 3(4)(e).

As such, when a business/place/activity or an individual breaches a COVID-SAfe Check-In requirement under Direction 27, the breach is under section 28 of the EM Act.

As an alternative to prosecuting a failure to comply with an EM Act direction, regulation 6 of the Emergency Management Regulations 2009 prescribes that authorised officers may issue expiation notices for an alleged breach:[22]

> *(1) Subject to the* Expiation of Offences Act 1996*, an authorised officer is authorised to give expiation notices for alleged offences against section 28 of the Act* [the Emergency Management Act 2004].
>
> *(2) The expiation fee for an offence against section 28 of the Act is fixed at—*
>
> *(a) in the case of a natural person—$1000*
>
> *(b) in the case of a body corporate—$5000*

2.3.1.5 State Records exemption

The *State Records Act 1997* (SR Act) includes a set of requirements and responsibilities for agencies to manage official records.

To meet these responsibilities agencies must ensure official records in their custody are:

- maintained in good order and condition
- not destroyed without appropriate authority.

State Records of South Australia (State Records) has developed several determinations in response to the COVID-19 pandemic under section 24 of the SR Act.

State Records stated that the QR code data stored in DPC's database is considered an official record for the purposes of the SR Act and is governed by State Records policies. It further stated that the data is only obtained for COVID-19 contact tracing purposes or for managing the COVID-19 pandemic and is expected to only be retained for 28 days. As such, State Records approved a determination authorising the destruction of records obtained through the QR code application when they are no longer required. This includes the hardcopy equivalent.[23]

2.3.1.6 Capturing and destroying people's contact details

When the COVID-SAfe Check-In app was made available on 1 December 2020, the SA Government advised the South Australian public that the check-in data would be held on an encrypted server and deleted every 28 days.[24]

---

[22] In addition, the *COVID-19 Emergency Response Act 2020* has temporarily modified section 28 of the EM Act to expressly refer to the expiation penalties for breaching an EM Act direction.

[23] State Records of South Australia, File Reference: SRSA20 – 00572, RDS2020/16 v1: *QR Track and Tracing*, 17 November 2020.

[24] ABC news article December 2020, 'Data gathering capped as centralised QR check-in system launches in South Australia', https://www.abc.net.au/news/2020-12-01/centralised-qr-check-in-system-launched-in south-australia/12933424, viewed 5 May 2021.

The legislative requirement to destroy people's contact details was prescribed in Public Activities Direction 22[25] on 8 April 2021 but was in operation prior to the legislated change.

Schedule 3(8) of Direction 22 prescribes that:

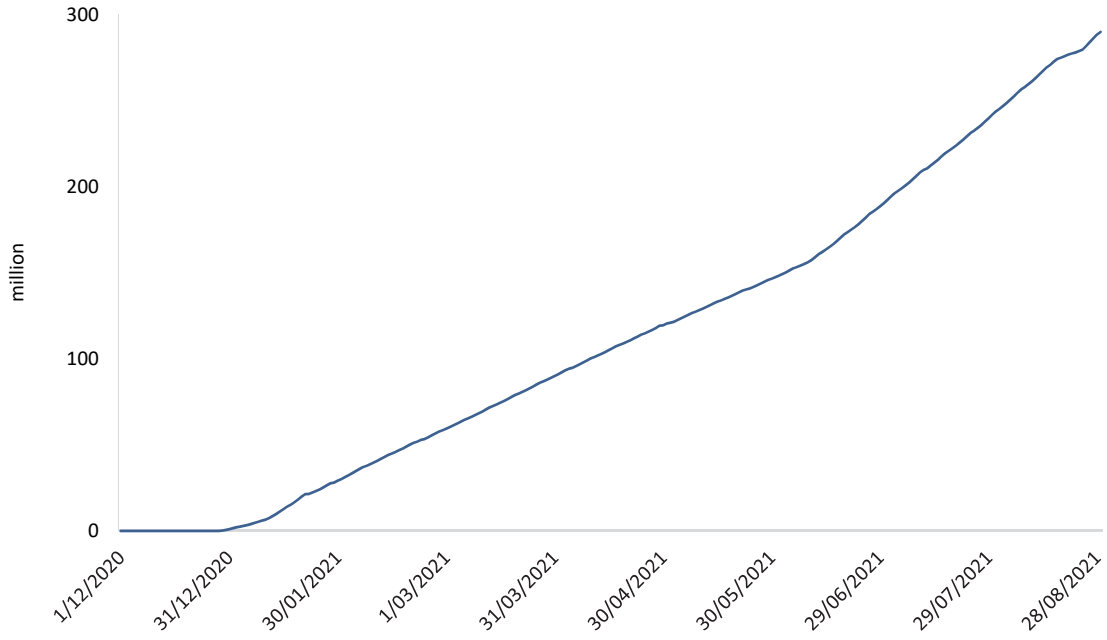
> *All reasonable steps must be taken to destroy the relevant contact details captured by an approved contact tracing system under this or any other direction made under the* Emergency Management Act 2004 *and stored on a prescribed database within the prescribed period.*

Schedule 3(10) of Direction 22 defines the prescribed period as seven days commencing 28 days after the day on which the contact details were received. Therefore, no longer than 35 days.

We sought sufficient evidence of the controls applied to manage and destroy people's contact details in line with SA Government advice and Direction 27 (the most current direction at the time of our review, superseding previous directions). Sections 5.2.1 and 6.2.1 discuss this further.

Figure 2.8 shows the high-level check-in data deletions.[26]

Figure 2.8: COVID-SAfe check-in data deletions since inception



[25] Emergency Management (Public Activities No 22) (COVID-19) Direction 2021.

[26] <https://data.sa.gov.au/data/dataset/covid-safe-checkins/resource/a78b4b4f-834f-4e90-b38a-b3f12750bea5>, viewed 5 May 2021.

3 Review mandate, objective and scope

3.1 Our mandate

The Auditor-General has authority to conduct this review under section 36(1)(a)(iii) of the *Public Finance and Audit Act 1987*.

3.2 Our objective

Our objective was to conclude on the controls applied to manage people's contact details captured through the COVID-SAfe Check-In app for contact tracing purposes. This covered both DPC's and SA Health's data management, protection and disposal arrangements.

3.3 What we reviewed and how

We sought to understand the security controls implemented by DPC to manage the COVID-SAfe Check-In app and by SA Health to manage its COVID management systems. We made recommendations where we identified opportunities to improve controls.

We reviewed the following key control areas across the environments:

- information classification
- risk management
- access management
- capturing and destroying people's contact details
- event logging and monitoring
- change management
- cryptography[27]
- facilities security
- human resources
- system security
- independent assurance and third-party management.

Our control testing was conducted from March 2021 to June 2021.

3.4 What we did not review

We did not review any aspect of the contact details captured in written form, where a person was not able to use the COVID-SAfe Check-In app.

[27] Cryptography involves converting ordinary plain text into unintelligible text and vice-versa. This includes the storage and transmission of data (such as contract tracing data) in a format so that only those for whom it is intended can read and process it.

After we completed our testing, it came to our attention that a small SA Health business unit, separate from the COVID Operations unit, also has access to CMS, which contains contact tracing data. This business unit is called Enterprise Data and Information (EDI) and is responsible for managing positive COVID-19 cases from a hospital operational perspective, compliance monitoring, quarantine checking and emergency management. We were advised that only a subset of contacts details relating to COVID-19 positive cases is fed from CMS into EDI's data warehouse. Confirmation of clinical clearance of COVID-19 cases is then fed back to CMS. SA Health confirmed that EDI supports critical business requirements to manage the COVID-19 pandemic in the State.

We did not perform any testing of the controls applied by EDI.

Key areas of SA Health and SAPOL also receive contact details of COVID-19 positive cases to ensure effective quarantine compliance and infection control. During bushfire season, the South Australian Metropolitan Fire Service is also provided with the details of any COVID-19 positive cases in bushfire communities. We did not perform any testing of the controls applicable to these arrangements.

4 The State's overall COVID-SAfe Check-In governance arrangements

This section applies to the State Coordinator, who we consider is responsible for coordinating the COVID-SAfe Check-In governance arrangements.

4.1 Findings

4.1.1 No clear information asset owner of the COVID-SAfe Check-In app, database and supporting IT environment

Recommendation

We recommend that a clear asset owner be established. They could then, if appropriate, assign responsibility for managing the information to another person or group, known as an information custodian.

Finding

At the time of our review, advice we received when interviewing key stakeholders indicated uncertainty about the owner of the various components of the COVID-SAfe Check-In app.

The COVID-SAfe Check-In app, database and supporting IT environment was implemented by DPC.

While it could be assumed that the implementing agency is the information custodian, there is no formally designated owner of the COVID-SAfe Check-In app database and supporting IT environment.

The COVID-SAfe Check-In project was approved by the State Coordinator in his role under the EM Act. As such, we consider the State Coordinator to be responsible for determining the applicable ownership arrangements for the COVID-SAfe Check-In app, database and supporting IT environment.

Why this is important

The South Australian Cyber Security Framework (SACSF)[28] requires formalisation of ownership arrangements. This includes identifying and recording the information assets according to the South Australian Information Classification System (ICS),[29] and assessing and documenting all related cyber security risks.

[28] The SACSF was developed to standardise and guide the approach for establishing, implementing, maintaining and continually improving the cyber security posture of SA Government agencies.

[29] This ICS is used to help agencies assess the confidentiality, integrity and availability of their information assets and ensure the appropriate protections.

Assigned information owners are responsible and accountable for assets that support critical processes or services. They can assign responsibility for managing the information to another person or group, known as an information custodian.

Without clarity of roles and responsibilities, delays can occur in resolving security incidents and remediating any associated control risks. Therefore, formally identifying and documenting ownership arrangements helps to provide a clear understanding of information assets and their relative value.

State Coordinator response

As identified in the review, the system was developed and implemented quickly in response to the rapidly evolving nature of the pandemic in November 2020 and has operated successfully since.

I'm advised the system is being managed and used in accordance with the South Australian Cyber Security Framework with a classification of Protected and note the recommendations regarding assigning an asset owner, formally documenting the security classification and end-to-end IT processes.

As the State Coordinator I will assign ownership of the system and ensure the recommendations are actioned.

4.1.2 A strong information classification is used but not formally documented for the COVID-SAfe Check-In app, database and supporting IT environment

Recommendation

Once an asset owner is established, we recommend that an information classification level is formally assigned and documented in an asset register.

Finding

As mentioned previously, DPC implemented the COVID-SAfe Check-In app. In doing so, it informally classified the associated database as PROTECTED[30] and advised SA Health of this in a minute sent in January 2021. Given the information the database holds in aggregate, we agree that this classification is appropriate.

We also found that DPC is applying the controls relevant for this classification.

The COVID-SAfe Check-In project was approved by the State Coordinator in his role under the EM Act. As such, we consider the State Coordinator to be responsible for ensuring that the applicable owner formally assigns and documents an information classification level in an asset register. It should be in line with the requirements of the SACSF and ICS.

[30] The SACSF defines PROTECTED as a security classification where compromise of the information concerned could result in damage to State or National interests, organisations or individuals.

Why this is important

The SACSF requires information assets to be classified by the asset owner in line with the ICS. Formally documenting the classification of information assets in a register helps to determine the extent of controls to be applied to protect their confidentiality, integrity and availability.

State Coordinator response

See the response provided in section 4.1.1.

4.1.3 The State's end-to-end COVID-SAfe Check-In IT processes are not clearly and formally documented

Recommendation

Documentation describing the State's end-to-end COVID-SAfe Check-In IT processes should be finalised by the information custodians (DPC and SA Health) and approved by the information asset owners. For key components of the environment, this should include:

- the delegated custodian responsible for the management and operation of each system component and the information it contains
- the risks and associated risk rating of each component
- the controls and risk treatment activities to mitigate the identified risks.

Finding

Due to the speed at which the COVID-19 situation was evolving, in late-2020 the focus was on developing functional IT systems to support contact tracing and case management as quickly as possible. As a result, minimal formal documentation was created prior to the systems going live.

The information custodians are responsible for defining, documenting and managing the risks associated with their delegated system components and associated controls. We identified that architectural design documents describing the end-to-end IT processes were drafted after system implementation for both the COVID-SAfe Check-In app and the COVID management systems. At the time of our review, these documents were still in a draft and not yet formalised.

We acknowledge the original priority to develop and make available improved systems to support contact tracing and case management. As these systems are now in operation, however, there remains a need to formalise the end-to-end systems architecture and information workflows for the State's COVID-19 management processes.

Why this is important

Effective security risk management of information systems includes understanding:

- what you have (the asset) and what could go wrong with it (the risk)

- how you can prevent or mitigate the risk (the controls)
- who is responsible for managing the controls associated with the risk
- how you will obtain assurance over the ongoing effectiveness of the controls.

Documenting the overall system architecture and end-to-end information workflows makes it easier to understand where key control risks exist, and what risk mitigation activities need to be applied. In its absence, controls are applied on a best-effort basis. In our opinion, that is not a satisfactory basis for reasonable assurance.

State Coordinator response

See the response provided in section 4.1.1.

5 Department of the Premier and Cabinet

This section applies to the COVID-SAfe Check-In app, database and supporting IT environment managed by DPC.

5.1 Positive observations

5.1.1 Regular process for destroying COVID-SAfe Check-In data older than 28 days from the production database

Our testing identified that people's contact details obtained from COVID-SAfe Check-Ins is effectively destroyed from the production database, which is the database accessible on a day-to-day basis. This is an automated process that checks for records older than 28 days.

5.1.2 DPC followed good practice to develop and release the COVID-SAfe Check-In app quickly

Due to the speed at which the COVID-19 situation was evolving, in late-2020 the focus was on developing functional contact tracing and case management systems as quickly as possible. DPC was able to deliver a solution and at the time of this report it had received few public complaints or issues about it.

5.1.3 Encryption techniques are used to secure people's contact details

People's contact details are encrypted on receipt in the COVID-SAfe Check-In app. Once encrypted, the data cannot be viewed or read again until it is unencrypted within DPC's PROTECTED environment. Encryption keys to access the encrypted data are generated from within the PROTECTED environment.

5.1.4 User access management processes are industry best practice

We tested the user access management processes DPC applied to the COVID-SAfe Check-In components and identified several positive controls. These include:

- user access management practices are formally documented
- all accounts are unique for traceability of actions to individual users
- appropriate approval is sought before assigning access to systems or information
- access is provided at the minimum privilege level required for what was requested
- accounts with privileged access are restricted to a small number of authorised users for administering the system
- passphrases and multi-factor authentication are used for all users
- access is removed when no longer required
- users access reviews within the COVID-SAfe Check-In database and supporting systems are scheduled and performed regularly.

We did note that user access reviews are only performed on an ad-hoc basis for some components of the overall COVID-SAfe Check-In environment (refer to section 5.2.4).

5.1.5 Physical security of the COVID-SAfe Check-In environment is industry best practice

The COVID-SAfe Check-In database and associated infrastructure are administered and maintained in Information Security Registered Assessors Program (IRAP)[31] accredited physical security zones that are appropriate for the level of data classification applied (PROTECTED).

5.1.6 Security vetting occurs for users with access to the data

Our testing found that DPC's standard process for new starters includes National Police Checks and signed confidentiality agreements. In addition, because it is (informally) classified PROTECTED, Australian Government Security Vetting Agency baseline security clearances are required, at a minimum, to access or view the COVID-SAfe Check-In database.

5.1.7 Endpoint protection and patching levels are operating

Our testing indicated that endpoint security software[32] is installed and operational on all devices/systems used to manage the COVID-SAfe Check-In app. Appropriate infrastructure patching[33] is also applied.

5.1.8 Independent assurance and third-party management were performed

DPC commissioned an independent penetration testing and program code review over the COVID-SAfe Check-In app and supporting IT environment. We noted that no high-risk issues were identified in this review.

At the time of our review, DPC had also initiated an independent third-party to perform a penetration test on the mechanism used to pass data from DPC to SA Health.

The COVID-SAfe Check-In database is administered from within DPC's IT environment, and it is temporarily stored in encrypted format within a third-party environment. Both environments are IRAP accredited, which exceeds the minimum protection and handling requirements for PROTECTED information defined by the South Australian Protective Security Framework (SAPSF).[34]

---

[31] The IRAP is an Australian Signals Directorate initiative. The purpose is to provide high-quality ICT security assessment services to government.

[32] Endpoint security software is software that is directly installed on each device, such as laptops and servers, to help protect them from a range of attacks that can infect them.

[33] Software patches released by vendors often remediate known security vulnerabilities. These vulnerabilities are common targets for attackers seeking to compromise systems and data.

[34] The SAPSF was developed to help the SA Government protect its people, information and assets.

5.1.9 Change management processes are controlled

Our testing found that changes to system components are well controlled, with access to perform changes within the platform restricted to authorised users.

5.2 Findings related to the COVID-SAfe Check-In app

5.2.1 Backups kept of COVID-SAfe Check-In data beyond 28 days of capture

Recommendation

We recommend that DPC update its backup restoration policy and procedures to include the requirement for COVID-SAfe Check-In data older than 28 days to be immediately destroyed once a required restoration is complete.

Finding

A key objective of our review was to determine the adequacy of DPC's and SA Health's disposal arrangements for people's contact details obtained through the COVID-SAfe Check-In app.

Our testing found that people's contact details are effectively destroyed from the production database, which is the database accessible on a day-to-day basis. This is an automated process that checks for records older than 28 days. In addition, DPC's encrypted portal, which is used to allow SA Health to retrieve COVID-SAfe Check-In data for contact tracing purposes, is configured to automatically delete the files after three days.

DPC is keeping backups of the COVID-SAfe Check-In IT environment, which includes the database containing all captured contact details. This is in line with its PROTECTED IRAP accreditation, which requires all backups to be regularly conducted and the data secured and retained indefinitely.

Backup of system information is vital for the recovery of critical systems in the event of a disaster or system failure. For COVID-SAfe Check-In data, Direction 27 indicates that all reasonable steps need to be taken to destroy the contact details captured within the prescribed period (within seven days after 28 days from capture).

DPC advised us that it intends to destroy all backups when contact tracing in the State is no longer required. Until this time, data restorations are possible, although controls exist to protect the data from any unauthorised restorations. These notably include controls for physical and logical access to backups and system monitoring. DPC also indicated that multiple people would need to be physically on site for any data restore to occur.

If COVID-SAfe Check-In data records older than 28 days were restored without appropriate authority, there is a risk of breaching Direction 27 under the EM Act. We note, however, the Direction allows for reasonable steps to be taken to destroy contact details.

Why this is important

There is a risk that if backups are restored, the restored information may contain people's contact details captured through the COVID-SAfe Check-In app that are older than 28 days.

DPC response

> *In line with the Auditor General's recommendation, DPC has updated its backup restoration procedures in line with this recommendation, and included an additional requirement to verify that once restored, no data exists that is over 28 days.*

This activity is targeted for completion by October 2021.

5.2.2 Some components of the COVID-SAfe Check-In IT environment are not included in DPC's overarching Cyber Security Program

Recommendation

To better manage cyber security risks, DPC should expand the scope of its Cyber Security Program to ensure that it includes all components of the COVID-SAfe Check-In app and associated environment.

Finding

To comply with the requirements of the SACSF, agencies need to develop a Cyber Security Program to demonstrate their ongoing commitment and approach to managing cyber security risk.

DPC maintains a Cyber Security Program and the COVID-SAfe Check-In database is included in its coverage. The PROTECTED controls applied to the database have been IRAP assessed and exceed the minimum protection and handling requirements for PROTECTED information defined by the SAPSF.

Despite this, our testing indicated not all the other components of the COVID-SAfe Check-In app and associated environment have been included in the scope of DPC's Cyber Security Program.

Why is this important

Including all key systems in the Cyber Security Program helps to better manage and understand all ongoing cyber security risks.

In doing so, it is important to implement robust cyber security controls that are tracked through key initiatives and ongoing operational tasks. Ensuring that controls are in place to address agencies cyber security risks also helps to comply with applicable legal, regulatory and contractual requirements.

DPC response

> *DPC has engaged an independent, external consultant to undertake a review of current processes and security operating models around the COVID-SAFE Check-In app and other digital government services initiatives, to ensure alignment with the SA Cyber Security Framework and the overarching Cyber Security Program.*

This activity is targeted for completion by December 2021.

5.2.3 A full risk assessment has not been performed to confirm the adequacy of the end-to-end COVID-SAfe Check-In controls

Recommendation

DPC should perform a full risk assessment of the COVID-SAfe Check-In app, database and supporting IT environment. This should align with its risk assessment processes, with outcomes updated in the system design documentation.

As part of this process, DPC should consider the inherent risks (risks before taking into consideration internal controls) we identified in our review.

Risk treatment plans should be developed for all identified risks and should include clearly defined owners, mitigating controls and time frames for remediation activities.

Finding

The SACSF requires agencies to assess and document cyber security risks for all projects undertaken.

The COVID-SAfe Check-In app was developed as part of the State's emergency response to COVID-19. DPC advised that due to time constraints, a formal risk assessment was not performed prior to the system being made available for public use.

We identified some inherent risks associated with the COVID-SAfe Check-In. We rated these risks in line with DPC's risk management procedure and provided them to DPC for its consideration.

Why this is important

Understanding what can go wrong with an asset, the impact it can have on the agency and how likely it is to occur, helps to identify effective mitigating controls. Understanding the types of risks introduced by an asset also helps agency leadership to make informed decisions on the extent of investment required to protect the asset.

DPC response

Recommendation accepted.

DPC will perform a full risk assessment of the COVID-SAfe Check-In app, database and supporting IT environment and develop treatment plans where required.

DPC has already undertaken risk assessments of the components of the solution as part of the project which will form part of the full risk assessment.

This activity is targeted for completion by December 2021.

5.2.4 Minor weaknesses in user access reviews

Recommendation

DPC should formalise its access administration processes and schedule (at least quarterly) and formally document user access reviews of all relevant COVID-SAfe Check-In components, so that access is appropriately provided and validated.

Finding

Our testing identified several positive user access management practices (refer to section 5.1.4).

We noted, however, that there is no schedule to perform formal user access reviews for components of the COVID-SAfe Check-In environment that are managed outside of the IRAP accredited environment. In these instances, only ad hoc reviews are performed.

Why this is important

Not formalising user access administration practices, including regularly and thoroughly reviewing all relevant user access, increases the risk of users retaining inappropriate access to systems and potentially performing unauthorised activities. This could compromise the confidentiality, integrity or availability of sensitive information in the system.

DPC response

Recommendation accepted.

DPC will formalise its access administration processes and undertake quarterly user access reviews.

This activity is targeted for completion by December 2021.

5.2.5 Event logs need monitoring

Recommendation

DPC should ensure that event logs generated by the COVID-SAfe Check-In supporting cloud infrastructure service are forwarded to a centralised security monitoring system. This would enable advanced monitoring of various event triggers to identify potential security incidents.

Finding

Our testing identified that, where applicable, event logs recording user activities, exceptions, faults and other events are adequately captured. This includes all event logs generated by the COVID-SAfe Check-In supporting environment and database.

However, although event logs are captured they are not monitored and analysed to identify potential security incidents.

Why this is important

When event logs are not monitored in real time, there is an increased risk of security incidents going undetected for an extended period. Forwarding the event logs into a dedicated security monitoring system enables advanced monitoring through correlation of various event triggers to identify potential security incidents.

DPC response

> *Recommendation accepted.*
>
> *DPC will ensure that event logs from the COVID-SAfe Check-In and supporting infrastructure are forwarded to the Whole of Government Security Information and Event Management (SIEM) platform.*

This activity is targeted for completion by October 2021.

6 Department for Health and Wellbeing

This section applies to SA Health's COVID management systems.

6.1 Positive observations

6.1.1 Sound change management processes were applied

Our testing found that changes to SA Health's COVID management systems are controlled. This includes conducting testing in a separate environment and maintaining appropriate documentation, including approvals.

6.1.2 Security vetting and training is performed for users with access to the data

Our testing found that SA Health's standard onboarding process for personnel who may access contact tracing data includes National Police Checks and signed confidentiality agreements.

A training platform and knowledge management system has been implemented to ensure all users understand their responsibilities when using CMS. Ad-hoc training in relation to the CMDB is provided to staff as part of the onboarding process.

6.1.3 Appropriate end user device protection and patching levels were operating

Our testing found that all end user device/systems have security software installed and operational to manage the COVID management systems. Infrastructure patching is managed by the vendor for CMS and Digital Health SA for the CMDB.

6.2 Findings related to the COVID management systems

6.2.1 Data retention varies under the *Health Care Act 2008,* the *Emergency Management Act 2004* and the State Records disposal determination

Recommendation

For clarity about retention of the data SA Health receives from DPC for contact tracing purposes, it would be helpful if SA Health's public communications include information about the requirements of the *Health Care Act 2008*, such as on websites and in digital media.

In doing so, SA Health should review the requirements of the *Health Care Act 2008* against the EM Act and State Records' November 2020 disposal determination.

Finding

SA Health retrieves a subset of COVID-SAfe Check-In data from DPC's database when requested for contact tracing purposes. Data it receives is stored in its COVID management systems.

These SA Health systems are not part of DPC's database established by directions issued under the EM Act, where the data is required to be destroyed within a 7-day period commencing 28 days after the contact details are received.

Schedule 3(7) of Direction 27 of prescribes:

> *Relevant contact details extracted from the prescribed database and provided to SA Health for contact tracing purposes is taken to be information obtained in connection with the operation of the* Health Care Act 2008 *and is protected under that Act.*

SA Health advised us that it intends to retain all data received indefinitely under the *Health Care Act 2008*. The Act makes detailed provisions for the protection and confidentiality of information.

State Records has released a disposal determination[35] indicating that records collected through the COVID-SAfe Check-In app should be destroyed as soon as practicable when no longer required for contact tracing purposes, or immediately following the declaration of the end of the pandemic period, whichever is sooner. In its determination, State Records also indicated that this approach to data retention has been supported by changes made to the *Privacy Act 1988* (Cwlth) and through orders issued under that Act with State and Territory health authorities. SA Health's current approach of keeping COVID-SAfe Check-In data indefinitely after it is received from DPC is not consistent with the State Records disposal determination.

Why this is important

There are differences in data retention periods under the respective legislative provisions that apply to the DPC and SA Health systems.

It would be helpful if SA Health's public communications included advice that it retains all requested COVID-SAfe Check-In app data indefinitely under the *Health Care Act 2008*. This includes on websites and in digital media.

SA Health response

> *SA Health will review and document its data retention practices relating to information received for contact tracing purposes; and ensure alignment with all relevant legislation.*

[35] State Records of South Australia, File Reference: SRSA20 – 00572, RDS2020/16 v1: *QR Track and Tracing,* 17 November 2020.

In response to identifying a case and conducting a risk assessment, SA Health COVID Operations Team request specific data to be extracted from the database hosting QR code check-in, managed by [DPC]*. The data is transitioned through* [a secure file transfer mechanism] *to a restricted share file within the Digital Health environment. From this share file, the data is uploaded into an approved contact tracing system* [CMS or the CMDB]*, is considered to be contact tracing information and taken to be information obtained in connection with the operation of the* Health Care Act 2008 *and is protected under that Act.*

SA Health will ensure that all information on websites and in digital media reflects this situation. Please note that the share file that temporarily hosts QR code data transitioning to the approved contact tracing systems has a deletion rule set that deletes the data after 28 days.

This activity is targeted for completion by November 2021.

6.2.2 No formal SA Health owner and information classification assigned to the Contact Management Database

Recommendation

in line with Policy Statement 2.1 of the SACSF, SA Health should ensure that the CMDB is identified, recorded and classified according to the South Australian Information Classification Scheme.

Finding

SA Health's COVID Operations unit implemented its COVID management systems, including CMS and CMDB, to help its COVID-19 case management and contact tracing processes.

We found that CMS was assigned a formal owner and is classified as OFFICIAL: Sensitive. We consider this classification level is appropriate for a system containing a smaller subset of individual records that contain people's contact details, aligning with the guidance provided by the SAPSF.[36]

The COVID management systems were authorised under the *Health Care Act 2008*. While assumed custodianship of this system rests with the implementing agency, there is no formal designated owner of the CMDB within SA Health. In addition, the application, relevant environments and associated data stored in the CMDB have not been formally classified in line with Policy Statement 2.1 of the SAPSF.

[36] SAPSF Classification Assessment Tool, <https://www.dpc.sa.gov.au/__data/assets/pdf_file/0006/125961/Classification-Assessment-Tool.pdf>, viewed 16 June 2021.

There is a significant number of OFFICIAL: Sensitive records retained in the CMDB, including records of every COVID-19 test performed in South Australia. Under the SAPSF, exposure of the CMDB records in aggregate has the potential to cause a major loss of confidence in the SA Government.

There is also a risk that there are no formal responsibilities allocated to respond to a security incident should it occur within the environment.

Why this is important

It is important for agencies to have formal documentation of their information assets and their relative value. This helps determine the extent of controls to be applied to protect them.

Once identified, assets should be classified and assigned ownership to ensure appropriate controls can be identified and applied to protect the confidentiality, integrity and availability of the asset.

Not being clear about roles and responsibilities can also delay the resolution of a security incident.

SA Health response

> *SA Health will assign a formal owner to the* [CMDB] *and ensure the CMDB has been assessed and classified in accordance with the South Australian Information Classification Scheme as per the policy requirements of the South Australian Cyber Security Framework.*

This activity is targeted for completion by December 2021.

6.2.3 A full risk assessment to confirm the adequacy of end-to-end COVID management systems controls has not been performed

Recommendation

SA Health should perform a full risk assessment of the COVID management systems. This should align with its risk assessment processes, with outcomes documented in the system design documentation.

As part of this process, SA Health should consider the inherent risks (risks before taking into consideration internal controls) we identified in our review.

Risk treatment plans should be developed for all identified risks and should include clearly defined owners, mitigating controls and time frames for remediation activities.

Finding

The SACSF requires agencies to assess and document cyber security risks for all projects undertaken.

The COVID management systems were implemented as part of the State's emergency response to COVID-19. SA Health advised us that due to time constraints, a formal risk assessment was not performed before the systems went live.

We identified some inherent risks associated with the COVID management systems. We rated these risks in line with SA Health's risk management procedure and provided them to SA Health for its consideration.

It should be noted that after we started our review, SA Health developed a draft technical design document describing its COVID management systems architecture. This document includes some risk areas with descriptions of implemented controls.

Why this is important

Understanding what can go wrong with an asset, the impact it can have on the agency and how likely it is to occur helps to identify effective mitigating controls. Understanding the types of risks introduced by an asset also helps agency leadership make informed decisions on the extent of investment required to protect the asset.

SA Health response

> *SA Health is undertaking a review of current information management systems across South Australia's COVID response activities. The review has a whole of system perspective and as such has captured the COVID-SAfe Check-in system and the approved contact tracing systems that are subject of this audit. The review seeks to identify where systems, people and processes can be enhanced. As part of this review, SA Health will conduct a full risk assessment of end-to-end COVID management systems, including consideration of inherent risk and control effectiveness.*

This activity is targeted for completion by October 2021.

6.2.4 User access management practices need to improve

Recommendation

SA Health should address the user account exceptions we identified in our review. It should also formalise its access administration processes and schedule (at least quarterly) and formally document user access reviews of all relevant COVID management systems, so that access is appropriately provided and validated.

SA Health should strengthen the CMS and CMDB password configuration settings.

In addition, where remote access is enabled, multi-factor authentication should be configured to significantly minimise the likelihood of unauthorised access due to common issues relating to compromised authentication credentials.

Finally, where possible, SA Health should enhance user role-based access privileges in CMS and the CMDB.

Finding

Our testing identified that SA Health's COVID Operations unit applies the following user access management practices to COVID management systems:

- approval is sought before assigning access to systems or information
- access is provided in line with what was requested and is only what is necessary for users to perform their job role/functions
- authentication is enforced by usernames and passphrases
- access to the CMDB requires an SA Health networked device and a network login account.

However, we also noted the following shortcomings:

- There are no formalised user access administration processes for the COVID management systems. As such, access is not always removed when no longer required and access reviews are not scheduled and performed regularly. We did note that ad-hoc CMS user access reviews have been performed due to maximum license constraints.
- We requested that SA Health review the current users of the COVID management systems and identified the following exceptions:
    - of 319 CMS user accounts, 95 were inappropriate including five administrators
    - of 480 CMDB users, 250 were inappropriate including 23 administrators
    - following SA Health's review, we still noted that 28 CMDB user accounts were created with personal email accounts
    - there were 28 instances of users maintaining multiple user accounts in the CMDB
    - there were a further 12 instances where multiple accounts were assigned to the same user's name
    - as noted in section 3.4, after our review SA Health's COVID Operations unit advised us that access to the COVID management systems had not been limited to COVID Operations. A separate business unit EDI also had a single account with administrative access to CMS, which exceeds its current business requirements.
- The CMS and CMDB password settings and authentication processes could be strengthened.
- While administrator and standard user roles are set up in the systems, advanced user role-based access privileges have not been configured in CMS or the CMDB.

At the time of this report, SA Health advised us they had not had any known breach of information security.

Why this is important

Not formalising user access administration practices, including regularly and thoroughly reviewing all relevant user access, increases the risk of users retaining inappropriate access to systems and potentially performing unauthorised activities. This could compromise the confidentiality, integrity or availability of sensitive information within the system.

A lack of appropriate password controls increases the risk of accounts being compromised and unauthorised access to systems, potentially resulting in data loss and access to sensitive information.

Multi-factor authentication significantly minimises the likelihood of unauthorised access due to common issues relating to compromised authentication credentials.

Role-based user access controls ensure that users are only provided with access to information they require to perform their job role/function.

SA Health response

SA Health will formalise periodic user access reviews to ensure user access aligns to staff movement and changes in roles and responsibilities.

Password configuration settings will also be reviewed and adjusted if necessary. Multi-factor authentication will be considered if remote access is enabled.

This activity is targeted for completion by December 2021.

6.2.5 Physical security could be improved

Recommendation

SA Health should relocate the CMDB application server to an appropriately secured Digital Health managed on-premise server room.

Finding

CMS is hosted in a vendor cloud environment that meets the physical security required of the data classification level (OFFICIAL: Sensitive).

The CMDB database infrastructure is stored on appropriately secured on-premise servers managed by Digital Health. The CMDB application server is located in a secure SA Health building with limited access, but resides on a workstation and not in a secure server room.

Why this is important

The CMDB application server is required to support SA Health COVID-19 management practices. Securely storing the CMDB infrastructure is essential to maintaining data security.

Unauthorised physical access increases the risk of data loss and the system being tampered with or inappropriately accessed. Limiting physical access to authorised personnel reduces the risk of improper use.

SA Health response

> *SA Health has migrated the* [CMDB] *to a network-segregated virtual machine dedicated to* [SA Health's COVID Operations unit]*. Following data classification and risk assessment, further restrictions can be implemented as required.*

This activity is targeted for completion by January 2022.

6.2.6 A security impact assessment has not been performed for the Contact Management Database

Recommendation

SA Health should complete a security impact assessment and penetration test of the CMDB.

Periodic security testing and audits should be conducted over high-risk system. The results of these activities should be documented, tracked and reported to the applicable governance committee.

Finding

We found that a security impact assessment and an independent penetration test of CMS was performed post go-live. No significant vulnerabilities in the environment were identified.

A security impact assessment and penetration test of the CMDB had not been performed.

Why is this important

Security testing and audits help to identify potential security weaknesses that could be exploited by malware or attackers. They can also be used to evaluate the effectiveness of cyber security capabilities against different threat scenarios.

SA Health response

> *SA Health will conduct a security impact assessment for the* [CMDB]*.*

This activity is targeted for completion by December 2021.

6.2.7 Contact Management Database event logging and monitoring could be improved

Recommendation

SA Health should improve its event logging capabilities for the CMDB to ensure that all security events are captured and can be reviewed.

SA Health should also establish an audit logging and review procedure that outlines the approach, requirements and roles and responsibilities to capture and review security events and audit logs. It should apply to all COVID management systems containing people's contact details.

Event logs for both CMS and the CMDB should be actively monitored to identify and examine key high-risk events, such as unauthorised access attempts or privileged user activities. This could be managed through a centralised logging database and alert system.

Finding

CMS maintains a full system audit trail for up to six months. This includes system and process errors and data changes. System errors and any errors from user action are notified to system administrators.

The CMDB captures errors, exceptions and job completion logs. However, full audit trail capabilities are not currently available.

We also noted that these system audit logs are not proactively reviewed to identify any key security events.

Why this is Important

Gaps in collecting audit logs and not performing active monitoring reduces the likelihood of unauthorised or inappropriate access or system changes being promptly identified. It also compromises the ability to conduct forensic investigations or root cause analysis of security incidents, if required.

Directing audit logs into a centralised and managed security system enables advanced levels of monitoring through correlation of various event triggers to identify potential security incidents.

SA Health response

> *SA Health will investigate the feasibility of enhancements to event logging and monitoring for the* [CMDB]*. These enhancements will be implemented if practical to do so. SA Health will also ensure that COVID Management Systems will be in scope of the Department's security and incident management system.*

This activity is targeted for completion by December 2021.

6.2.8 Some encryption techniques could be strengthened

Recommendation

SA Health should consider strengthening some aspects of the encryption techniques it applies to its COVID management systems.

Finding

We reviewed the encryption techniques SA Health applied to its COVID management systems to protect people's contact details. We identified some aspects that could be improved, and we provided these to SA Health for its review.

Why this is important

Implementing good encryption techniques helps prevent unauthorised access to information by making the data unreadable to unauthorised parties.

SA Health response

> *Encryption techniques applied for COVID Management Systems will be reviewed and strengthened if feasible to do so.*

This activity is targeted for completion by December 2021.

7 Additional finding applicable for the DPC and SA Health

7.1 DPC's ICT and Digital Government Division and SA Health's COVID Operations unit are not included in their agency Information Security Management Systems

Recommendation

DPC and SA Health should review their current and future state Cyber Security Programs and security operating models to ensure they cover all primary agency functions.

Finding

The SACSF uses a risk-based approach for managing cyber security. This approach is intended to help deliver services to the community in a reliable and resilient manner. This is done by safeguarding infrastructure, digital assets and citizen information against cyber threat.

We found that both DPC and SA Health maintain an ISMS aligned to the SACSF and ISO 27001.[37]

We were unable to obtain evidence to indicate that the scope of their respective ISMS's included the business units we consulted in our review. These include DPC's ICT and Digital Government Division and SA Health's COVID Operations unit. Therefore, the security risk management activities and security controls defined in DPC's and SA Health's ISMS may not be fully implemented across the systems we reviewed. We do acknowledge that the COVID-SAfe Check-In database is contained in an IRAP accredited environment, which exceeds the minimum protection and handling requirements for PROTECTED information defined by the SAPSF.

Why this is important

The SACSF requires the implementation of a cyber security program that is scoped to include all primary agency functions. We consider that this would include functions of DPC's ICT and Digital Government Division and SA Health's COVID Operations unit.

The root cause of this may be a combination of the current reporting structures, competing priorities and a lack of adequate resourcing to support agency-wide security management.

[37] ISO 27001 is an international specification detailing best practice requirements for establishing, implementing, maintaining and continually improving an ISMS. International Organisation for Standardisation 2021, ISO/IEC 27001 *Information security management*, <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm>, viewed 2 August 2021.

DPC response

See the response provided in section 5.2.2.

SA Health response

> *Digital Health SA's Security Services team provides enterprise-wide information security services and support for all of SA Health. The scope of this service will be reviewed to ensure adequate visibility of the COVID Operations unit.*

This activity is targeted for completion by December 2021.

Appendix – Glossary of abbreviations and terms

Term	Description
CMS	COVID-19 Case Management System (known as Salesforce within SA Health)
CMDB	Contact management database
DPC	Department of the Premier and Cabinet
EDI	Enterprise Data and Information
EM Act	*Emergency Management Act 2004*
Health Act	*Health Care Act 2008*
IRAP	Information Security Registered Assessors Program
ISMS	Information Security Management System
SACSF	South Australian Cyber Security Framework
SA Health	Department for Health and Wellbeing
SAPOL	South Australia Police
SAPSF	South Australian Protective Security Framework
SR Act	*State Records Act 1997*