

**Report 9 of 2019**

Information and communications  
technology reviews





# Report of the Auditor-General

Report 9 of 2019

Information and communications  
technology reviews

---

Tabled in the House of Assembly and ordered to be published, 29 October 2019

---

First Session, Fifty-Fourth Parliament

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

---



## **Auditor-General's Department**

[www.audit.sa.gov.au](http://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



Level 9  
State Administration Centre  
200 Victoria Square  
Adelaide SA 5000  
DX 56208  
Victoria Square  
Tel +618 8226 9640  
Fax +618 8226 9688  
ABN 53 327 061 410  
audgensa@audit.sa.gov.au  
www.audit.sa.gov.au

28 October 2019

The Hon A L McLachlan CSC MLC  
President  
Legislative Council  
Parliament House  
**ADELAIDE SA 5000**

The Hon V A Tarzia MP  
Speaker  
House of Assembly  
Parliament House  
**ADELAIDE SA 5000**

Dear President and Speaker

**Report of the Auditor-General:  
Report 9 of 2019 *Information and communications technology reviews***

As required by the *Public Finance and Audit Act 1987*, I present to each of you Report 9 of 2019 *Information and communications technology reviews*.

**Content of the Report**

Each year we review agency security controls over IT systems and the status of selected IT projects.

This report communicates the results of the following key IT reviews we conducted in 2018 19:

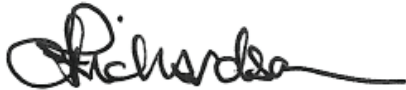
- Information technology general controls
- State taxation systems
- Active Directory within the SA Government
- End User Computing (ICT desktop outsourcing) program
- Education Management System project
- Electronic Medical Record project.

## **Acknowledgements**

The audit team for this report was Andrew Corrigan, Brenton Borgman, Tyson Hancock, Abhinav Tomar and Spoorthy Chitti.

We appreciate the cooperation and assistance given by staff of the agencies involved in these reviews.

Yours sincerely

A handwritten signature in black ink, appearing to read "Richardson", with a long horizontal flourish extending to the right.

Andrew Richardson  
**Auditor-General**

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Information technology general controls</b>	<b>2</b>
2.1	Introduction	3
2.2	What we reviewed	4
2.3	What we found	6
2.4	Details of findings	7
2.4.1	User access management	7
2.4.2	Change management	8
2.4.3	Password management	9
2.4.4	Audit logging	10
2.4.5	Disaster recovery	11
2.4.6	Patch management	12
2.5	What we recommended	12
2.6	Agency responses	13
<b>3</b>	<b>State taxation systems</b>	<b>14</b>
3.1	Introduction	15
3.2	Prior reviews	16
3.3	What we reviewed	16
3.4	Recent control improvements	17
3.5	What we found	17
3.5.1	Excessive access assigned to sensitive RIO functions	18
3.5.2	Periodic review of RIO user access privileges is not being performed	18
3.5.3	Developers have access to the RevenueSA Online production environment	18
3.5.4	Access to create business partners, create new parcels and perform valuations is not adequately segregated within RIO	18
3.5.5	Default RIO user accounts are not being disabled	19
3.5.6	Weak password controls exist in RIO and RevenueSA Online	19
3.5.7	RIO user access termination process is not consistent	19
3.5.8	RIO system and client setting changes are not being performed through the recommended process	19
3.5.9	RIO custom programs, transaction codes and tables are not appropriately restricted	20
3.5.10	Transaction level audit logging is not enabled in RIO	20
3.5.11	Security weaknesses exist in database and application servers	20
3.6	What we recommended	21
3.7	Agency response	21

<b>4</b>	<b>Active Directory within the SA Government</b>	<b>22</b>
4.1	Introduction	23
4.2	What we reviewed	23
4.3	What we found	24
4.3.1	Domain security and password configuration settings	24
4.3.2	User access privileges	24
4.3.3	Legacy operating systems	25
4.3.4	Authentication and communication configurations	25
4.3.5	Managing the outcomes from Active Directory risk assessments	25
4.3.6	Testing of Active Directory environment disaster recovery and documentation of recovery procedures	26
4.3.7	Domain trust relationships	26
4.4	What we recommended	26
4.5	Agency responses	27
<b>5</b>	<b>End User Computing (ICT desktop outsourcing) program</b>	<b>28</b>
5.1	Introduction	29
5.2	What we reviewed	30
5.3	Transformation implementation status	30
5.3.1	Department of the Premier and Cabinet status	30
5.3.2	SA Health status	30
5.4	Program costs	31
5.5	Contract update	33
5.5.1	Ongoing contract variations	33
5.5.2	Annual contract reviews	34
5.6	Benefits realisation	35
5.7	SA Health client satisfaction surveys	35
5.7.1	Internal user satisfaction survey	36
5.7.2	Auditor-General's satisfaction survey	37
5.7.3	Satisfaction survey summary	39
5.8	Current program challenges	40
<b>6</b>	<b>Education Management System project</b>	<b>41</b>
6.1	Introduction	42
6.2	What we reviewed	43
6.3	Project implementation approach and status	43
6.4	Project budget and expenditure	44
6.5	Challenges with legacy systems	45
6.6	Project benefits	45



6.7	Current project challenges	46
6.7.1	Managing several key project interdependencies	46
6.7.2	Challenges in testing outstanding functional and non-functional requirements	48
6.7.3	Feedback on early challenges experienced by the pilot sites	48
6.8	Program assurance	50
6.9	Summary of control findings	50
<b>7</b>	<b>Electronic Medical Record project</b>	<b>51</b>
7.1	Introduction	52
7.2	What we reviewed	53
7.3	Independent review outcomes and recommendations	53
7.4	The SA Government's response	55
7.5	Changes to the implementation approach	56
7.6	Changes to the governance arrangements	57
7.7	System functionality and impacts on hospitals	58
7.8	Update on current project activities	59
7.9	Project budget and expenditure	61
7.10	Project benefits	62
7.11	Impacts on the use of the Country Health system (Chiron)	64
7.12	Current project challenges	64
7.12.1	System configuration and defects	64
7.12.2	Meeting user expectations	65
7.12.3	Implementing priority software configuration and developments at the exemplar sites	66
7.12.4	Clinical ownership of system configuration	67
7.12.5	Integration with My Health Record	68
	<b>Appendix – RIO and RevenueSA Online system functionality</b>	<b>69</b>



# 1 Introduction

Each year we review agency security controls over IT systems and the status of selected IT projects.

This report communicates the results of the following key IT reviews we conducted in 2018-19:

- Information technology general controls
- State taxation systems
- Active Directory within the SA Government
- End User Computing (ICT desktop outsourcing) program
- Education Management System project
- Electronic Medical Record project.

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

## 2 Information technology general controls

Information technology general controls (ITGCs) are policies, procedures and system settings that support the effective functioning of operating system, database and application controls. They also help agencies maintain the confidentiality, integrity and availability of their data.

Each year we conduct selected ITGC testing over key agency financial systems.

This Report summarises the 2018-19 ITGC testing we conducted over 13 agencies and 26 key agency financial systems. Our testing also assessed the remediation of ITGC related issues we raised in prior years.

Although this summary does not include all agency ITGC testing that we conducted in 2018-19, it does provide an indication of the general themes where control weaknesses exist. It also provides agencies with information they can use to make informed decisions to improve the management of their overall control environments.

At the time of this Report, the SA Government was updating its existing Information Security Management Framework and associated agency IT security guidelines. These initiatives are expected to be available for agency use by the end of 2019.

### What we found

Most of the control deficiencies identified in our 2018-19 ITGC reviews related to the management of user access, passwords and audit logging. These deficiencies accounted for 67% of the total findings.

While most findings were medium<sup>1</sup> and low<sup>2</sup> rated, nine that related to user access, change management and patch management were rated as high.<sup>3</sup> Sections 2.3 and 2.4 provide further details of our findings.

It is disappointing that our ITGC reviews regularly highlight these types of control deficiencies. I would again encourage all agencies to be more diligent in addressing these control weaknesses as part of their routine security housekeeping.

---

<sup>1</sup> Medium rated is a control weakness that could have or is having a moderate adverse effect on the ability to achieve process objectives.

<sup>2</sup> Low rated is a minor control weakness with minimal but reportable impact on the ability to achieve process objectives.

<sup>3</sup> High rated is a control weakness that could have or is having a major adverse effect on the ability to achieve process objectives.

## What we recommended

Our recommendations to agencies include strengthening the following controls:

- user access management – promptly removing inappropriate user access, performing regular user access reviews and maintaining evidence of user access changes
- change management – improving policies and procedures, maintaining documented evidence supporting change activities and post-implementation testing, and applying appropriate segregation of duties throughout the change management process
- password management – strengthening password configuration settings, improving policies and procedures and conducting regular reviews of password setting policies
- audit logging – implementing and reviewing audit logging and improving policies and procedures
- disaster recovery – developing and regularly reviewing formal disaster recovery plans and associated procedures and conducting disaster recovery tests
- patch management – developing and improving policies and procedures to ensure patches are appropriately applied.

## 2.1 Introduction

---

The *Public Finance and Audit Act 1987* requires the Auditor-General to form an opinion on agency financial reports. In forming an opinion on whether a financial report is free from material misstatement, the auditor must consider the entity's internal control environment. Internal controls are systems, policies and procedures that help an agency reliably and cost effectively meet its objectives. For the agencies I audit, I consider ITGCs to varying degrees, depending on the nature of the agency's operations and the way it uses IT.

Auditing Standard ASA 315 *Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment* advises that ITGCs commonly include controls over:

- data centre and network operations
- system software acquisition, change and maintenance
- program change
- access security
- application system acquisition, development and maintenance.

Therefore, we seek to understand how agencies respond to risks arising from their IT environment and assess any controls applied. Ultimately, this will inform my opinion as to whether the information in the financial report is free from material misstatement.

## 2.2 What we reviewed

---

In 2018-19 we tested ITGCs for a range of agencies and their IT systems.

**Figure 2.1: Summary of agencies and systems tested**

Agency	System	Description
Adelaide Festival Centre Trust	BASS ticketing system	Revenue system used to record the sales of tickets primarily for artistic performances.
Attorney-General's Department	LOGIC system	Revenue system used to collect gaming, taxation, licence and regulatory fees.
Department for Child Protection	Connected Client and Case Management System (C3MS)	Used to record notifications of child abuse or neglect and track cases of vulnerable children.
Department for Education	Valeo	Payroll processing and other human resource functions.
Department for Environment and Water	Masterpiece	Used for accounts payable, accounts receivable, general ledger and fixed assets.
	Retail Touch	Helps to distribute permits and licences across a broad range of environment and water services.
Department for Health and Wellbeing	Oracle Corporate System	Used for accounts payable, accounts receivable, general ledger and fixed assets.
	Procurement and Contract Management System (PCMS)	Ensures that all required records for procurement processes and all contracts and agreements are accessible, managed and stored in one central repository.
Department of Planning, Transport and Infrastructure	Fee and Resource Management System (FARMS)	Used to manage construction projects.
	Facilities Asset Management Information System (FAMIS)	Used for processing, work orders in breakdown, routine maintenance, minor works and small construction works that support government facilities.
	Masterpiece	Used for accounts payable, accounts receivable, general ledger and fixed assets.
	Adelaide Fare Collection system (MetroCard)	Used for collecting revenue, tracking ticket validation and contract management.
	TRUMPS	Used for collecting revenue, mainly related to driver's licences and motor registration.








Agency	System	Description
Department of Treasury and Finance	Basware, Masterpiece, CommBiz and Chris21	Shared Services SA uses several central systems to process transactions on behalf of agencies. These include: <ul style="list-style-type: none"> <li>• Basware to process accounts payable transactions</li> <li>• Masterpiece for accounts payable, accounts receivable, general ledger and fixed assets</li> <li>• CommBiz banking for disbursing payroll and third-party payments</li> <li>• Chris21 for agency payroll processes.</li> </ul>
	Revenue Information Online (RIO)	Used to process taxation transactions for payroll tax, land tax and the fixed property component of the emergency services levy.
	RevenueSA Online (RSAOL)	Used to process stamp duty and other associated taxes.
Independent Gaming Corporation Limited	Scientific Games Video system	Used to monitor and manage existing gaming machine systems.
South Australia Police	Chris21	Used to process payroll.
South Australian Water Corporation	Chris21	Used to process payroll.
	Customer Service Information System (CSIS)	Revenue system used to bill customers for water usage and sewer charges.
	Ellipse	Expenditure payment system that includes the agency general ledger module.
TAFE SA	Accounts Receivable Point of Sales (ARPOS)	Integrates with accounts receivable components of the student information system and accounts payable management system.
University of South Australia	FinanceOne	Used for accounts payable, accounts receivable, general ledger and fixed assets.

Details of the issues we raised for RIO and RSAOL are included in section 3. For more detail on the issues we raised for the other systems, refer to the commentary on each agency in my Annual Report to Parliament.<sup>4</sup>

In testing these systems, we examined the ITGCs shown in figure 2.2 at the operating system, application and database level.

<sup>4</sup> Report 6 of 2019 Annual report for the year ended 30 June 2019, Part C: Agency audit reports.

**Figure 2.2: Summary of ITGCs tested**

	<b>Password management</b>	Passwords are a common means of verifying a user's identity before access is given to an information system or service according to the user's authorisation.
	<b>User access management</b>	User access management relates to the process of managing access to applications and data, including how access is approved, revoked and periodically reviewed. This helps to ensure that access is aligned with staff roles and responsibilities and prevents unauthorised access to information systems. It includes appropriately restricting and monitoring privileged access permissions, which have a heightened level of access to alter user access profiles and make system changes.
	<b>Audit log management</b>	Audit logging and monitoring of the ICT environment involves the recording and analysing of system and user activities to detect and respond to unusual events within the IT system.
	<b>Change management</b>	Change management is a systematic and standardised approach to ensuring all changes to the IT environment are appropriate, authorised and preserve the integrity of the underlying programs and data.
	<b>Patch management</b>	Patch management is the process of updating (acquiring, testing and installing) a set of changes or upgrades to support software, application and technology enhancements and to fix defects and vulnerabilities to an information system.
	<b>Backup management</b>	Backup management refers to the process of managing the copying of computer data to an archive file. This copy can then be used to restore the original data in the event of data corruption or data loss event.
	<b>Disaster recovery</b>	Disaster recovery is a documented process, or set of procedures, to assist in the recovery of an organisation's ICT infrastructure in the event of a disaster.

## 2.3 What we found

Based on our testing in 2018-19, figure 2.3 shows the key control areas that could be strengthened.

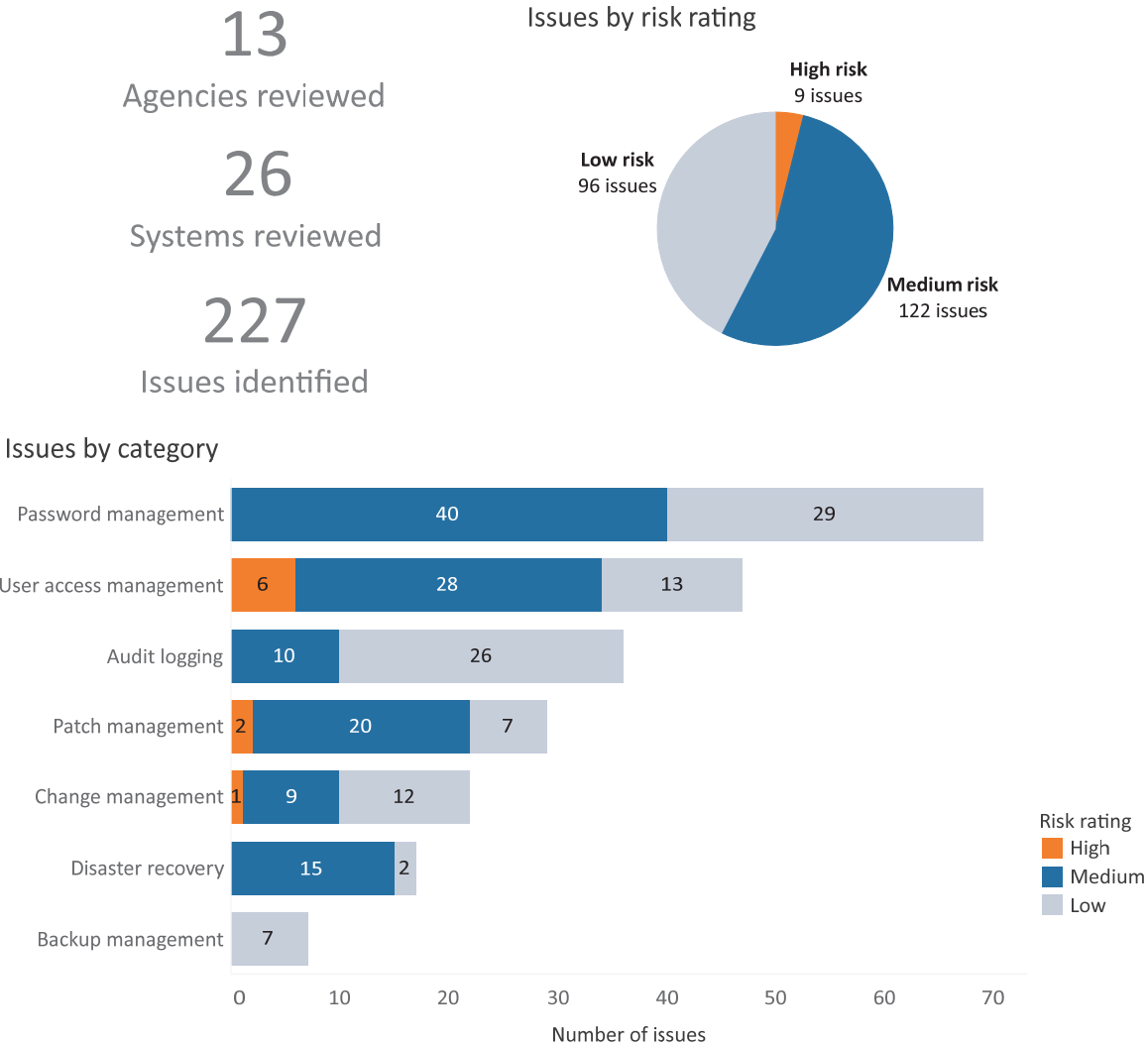
The rating we give the audit issues reflects our assessment of both the likelihood and consequence of each issue in terms of its impact on:

- the effectiveness and efficiency of operations, including probity and compliance with applicable laws
- the reliability, accuracy and timeliness of financial reporting.



The rating also helps agencies to prioritise any remedial action.

**Figure 2.3: Summary of our findings**



## 2.4 Details of findings

Our testing involved performing system walkthroughs with agency representatives and reviewing policies and procedures. The walkthrough helps us to get a better understanding of the agency’s IT environment and to evaluate the design of controls and whether they can be tested for effectiveness. For example, the control exists and evidence can be obtained to test its effectiveness.

### 2.4.1 User access management

#### Why we reviewed it

Weaknesses in user access management controls can result in inappropriate and unauthorised access to business systems. This can impact the completeness and accuracy of

financial information through the destruction of data, improper changes to data or inaccurate recording of transactions.

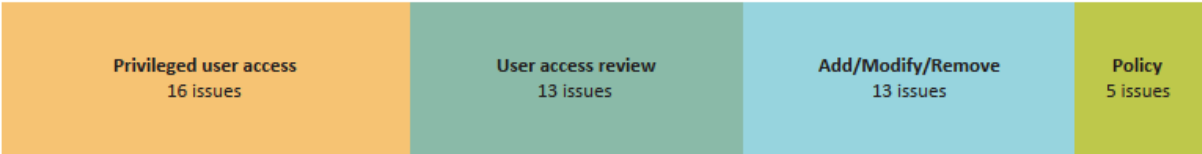
### What we reviewed

We reviewed the user access management policies and procedures that apply to key financial systems. This includes assessing processes applied for user access changes, user roles and responsibilities and profile configurations. For example, assessing whether a new user requires the completion and approval of a user access form before the account is created.

Our testing involved selecting a sample of user accounts and obtaining evidence of the addition, modification and removal of these user accounts and profiles. We also confirmed the appropriateness of privileged user accounts and obtained evidence of recent internal user access reviews and their outcomes.

### What we found

**Figure 2.4: Summary of user access management findings**



The six high rated findings noted in figure 2.3 related to the appropriateness and regular review of privileged user access accounts.

Most findings within these categories related to:

- inappropriate assignment of privileged user access
- internal user access reviews either not performed or not promptly actioned
- insufficient evidence of user access changes (add and modify) and failure to promptly remove user access.

### 2.4.2 Change management

#### Why we reviewed it

Weaknesses in change management controls can result in poorly tested, inappropriate or unauthorised changes to business systems. This can impact the completeness and accuracy of financial data and the correct functioning of the system.

#### What we reviewed

We reviewed the policies and procedures that apply to making system changes to the financial system environments. We did this to understand the process applied to making

system changes, including where change requests originate from, oversight and approval mechanisms, whether changes can be made within the business or require the assistance of an external vendor and the roles and responsibilities of each party in the process.

Our testing also involved selecting a sample of system changes and obtaining evidence to determine whether they were appropriately tested, approved and migrated into the production environment.

### What we found

**Figure 2.5: Summary of change management findings**



The one high rated finding noted in figure 2.3 related to access needing to be segregated and appropriately restricted for developers, change testers and change migration staff in the production environment.

Most findings within these categories related to:

- lack of segregation of duties throughout the change management process
- inadequate change management policy and/or procedure documents
- inadequate evidencing of documentation supporting change activities and post-implementation testing.

### 2.4.3 Password management

#### Why we reviewed it

Weaknesses in password configuration settings may make it easier for a user account to be maliciously compromised, allowing unauthorised access to business systems and data.

Examples of weak password configuration settings include:

- not forcing users to regularly change their password
- not forcing users to change their password to something not previously used
- minimum password length being too short
- not forcing users to add a number, uppercase letter or special character to their password
- not setting a limit on how many times a user can enter an incorrect account password before access is denied.

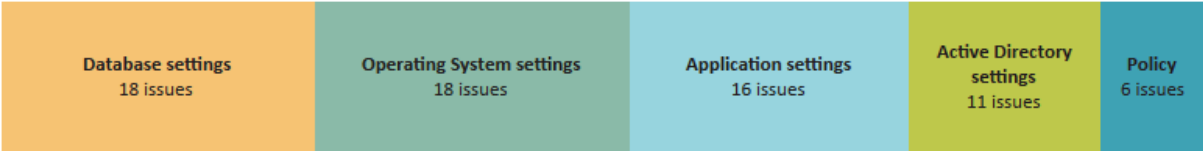
## What we reviewed

Our testing involved reviewing the agency’s password management policies and procedures. We did this to determine whether agencies had specified minimum password standards that their system owners must apply when configuring the password settings for their IT systems.

We compared the password settings of each tested system applied at the application, operating system and database level for in-scope financial systems against the configuration settings suggested in the Commonwealth Government Information Security Manual<sup>5</sup> and the agency’s password standards (if specified).

## What we found

**Figure 2.6: Summary of password management findings**



Most findings within these categories related to:

- weaknesses or inconsistencies in password configuration settings identified across various agency active directory networks, applications, databases and operating systems
- lack of general password policy or insufficient detail within the password policy
- inadequate regular review of the agency’s password policy.

### 2.4.4 Audit logging

#### Why we reviewed it

Weaknesses in system audit logging and monitoring increases the risk of inappropriate and unauthorised activities within the system going undetected. Not having an effective audit trail reduces the likelihood that inappropriate activity can be traced back to an individual.

#### What we reviewed

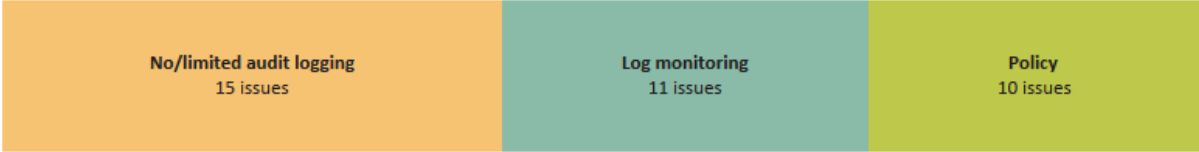
We reviewed the agency’s policies and procedures for audit logging to confirm the approach and extent of audit logging being performed.

Our testing then involved obtaining evidence that audit logs, primarily for privileged user account activities, are maintained, restricted and periodically reviewed.

<sup>5</sup> Although we acknowledge that agencies are not required to comply with this manual, we consider the settings recommended in it represent better practice.

## What we found

Figure 2.7: Summary of audit log findings



Most findings within these categories related to:

- no or limited audit logging conducted across the application, database, operating system and infrastructure
- no regular review of audit logs
- instances where no formal audit logging policy and procedures were maintained.

### 2.4.5 Disaster recovery

#### Why we reviewed it

IT disaster recovery weaknesses may result in agencies not being able to recover key business systems within maximum allowable outage times,<sup>6</sup> in the event of a disaster or system failure. In addition, the completeness and accuracy of financial data is at risk when a financial system experiences an interruption.

#### What we reviewed

Our testing involved establishing whether a disaster recovery plan and associated recovery procedures were in place and adequately tested.

#### What we found

Figure 2.8: Summary of disaster recovery findings



Most findings within these categories related to:

- no formal disaster recovery plan or associated procedures being developed
- insufficient disaster recovery testing conducted across the application and database
- no regular review of the disaster recovery plan.

<sup>6</sup> The maximum allowable outage time is the maximum time that an agency can tolerate the disruption of an important business function before there is a significant impact on its operations.

## 2.4.6 Patch management

### Why we reviewed it

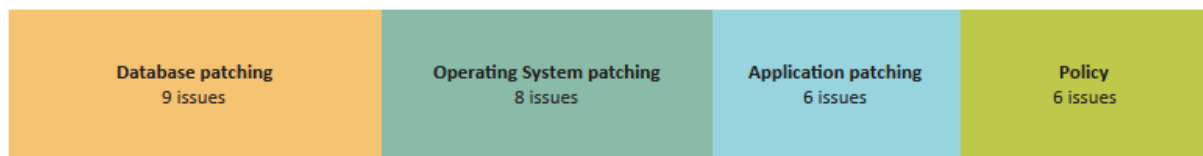
Not patching IT systems at the operating system, database and application level increases the opportunity for attackers to exploit known vulnerabilities. Patching is also used to provide system functionally updates and fix defects.

### What we reviewed

We reviewed the policies and procedures for patch management. Where appropriate, we selected a sample of patches applied to the application, database and operating system. Our testing involved obtaining evidence of a recent patching assessment and reviewing whether patches were subject to a formal risk assessment before being implemented.

### What we found

**Figure 2.9: Summary of patch management findings**



The two high rated findings noted in figure 2.3 related to deficiencies in security updates and patches being evaluated and implemented in a timely way for the agency's application, database and operating systems.

Most findings within these categories related to:

- inadequate patch management processes for specific application, database and operating systems
- instances where no formal patch management policy and procedures were developed.

## 2.5 What we recommended

---

Our recommendations to agencies include strengthening the following controls:

- user access management – prompt removal of inappropriate user access, performing regular user access reviews and maintaining evidence of user access changes
- change management – improving policies and procedures, maintaining documented evidence supporting change activities and post-implementation testing, and applying appropriate segregation of duties throughout the change management process
- password management – strengthening password configuration settings, improving policies and procedures and conducting regular reviews of password setting policies

- audit logging – implementing and reviewing audit logging and improving policies and procedures
- disaster recovery – developing and regularly reviewing formal disaster recovery plans and associated procedures and conducting disaster recovery tests
- patch management – developing and improving policies and procedures to ensure patches are appropriately applied.

## 2.6 Agency responses

---

Agencies generally responded positively to our findings with details of their remediation time frames.

## 3 State taxation systems

The Department of Treasury and Finance (DTF) uses various revenue systems for collecting State taxes.

RevenueSA, a business unit of DTF, is responsible for the key systems that collect State taxes. It has migrated all tax components from its legacy revenue systems to the RevenueSA Information Online (RIO) and RevenueSA Online (RSAOL) systems.

Given the importance of the State's taxation systems, we have conducted several security reviews on them over the last few years.

In 2018-19, we reviewed RIO and RSAOL. Our review considered the actions taken by RevenueSA to address the findings we raised in our previous audits of RIO in 2012-13 and 2015-16.

### What we found

We identified several high and medium risk areas that require remediation. This included the following application related findings:

- excessive access assigned to sensitive RIO functions
- periodic reviews of RIO user access privileges not being performed
- developers having access to the RSAOL production environment
- access to create business partners, new parcels and perform valuations not adequately segregated in RIO
- default RIO user accounts not being disabled
- weak password controls in RIO and RSAOL
- RIO user access termination process not consistently applied
- RIO system and client setting changes not being performed through the recommended process
- RIO custom programs, transaction codes and tables not appropriately restricted
- transaction level audit logging not enabled in RIO.

We also highlighted security weaknesses in both the database and application servers.

Some of these findings were raised in our prior reviews.



## What we recommended

To address the above risks we recommended the following:

- improving user access management, through ongoing periodic reviews, timely removal of inactive user accounts, deactivating default system accounts and tightening/restricting access to sensitive data, transactions, tables and programs
- improving segregation of duties across change management for the RSAOL environment and transaction access in the RIO environment
- strengthening password controls
- making system and client setting changes through the recommended interface
- enabling transaction level audit logging
- improving security settings and functions for operating systems and databases.

RevenueSA responded positively to these findings with details of remediation action and proposed time frames.

## 3.1 Introduction

DTF is the lead agency for the collection of State taxes exceeding \$3.6 billion p.a. Principal revenue taxes include payroll, land, fixed property components of the Emergency Services levy (ESL) and stamp duty.

DTF uses RIO and RSAOL to help collect these taxes.

**Figure 3.1: State revenue tax as at 30 June 2019 (unaudited)**

	RIO \$'million	RSAOL \$'million	Total \$'million
Taxation revenue			
Payroll tax	1 545	-	1 545
Land tax	524	-	524
ESL	146	-	146
Stamp duties (insurances, motor vehicles etc)	-	1 097	1 097
Other	3	43	46
Subtotal	2 218	1 140	3 358
Other generated revenue <sup>1</sup>			317
Total revenues			3 675

<sup>1</sup> Other generated revenue includes stamp duties (relating to real property sales, mortgages etc) transferred from the Department of Planning, Transport and Infrastructure (DPTI).

<sup>2</sup> Total revenue disclosed may vary to financial statements and reflect certain funds, remissions and concessions that were subsequently applied/adjusted.

RIO was previously known as RevenueSA Information System to Enable Compliance (RISTEC). RISTEC was originally intended to be deployed through the RISTEC project by a series of

releases. In 2012, Release 1 implemented the base application and production system and payroll tax. In 2015, land tax and ESL were implemented in Release 2.

The final release at that time was intended to add stamp duty and sundry taxes. Due to system problems, this was dropped from the project and the collection of stamp duties and sundry taxes remained on RevenueSA's existing taxation system.

In 2017, RevenueSA implemented RSAOL which migrated stamp duties and sundry taxes and provided other associated processing functionality.

The functionality of both systems is documented in the Appendix.

## 3.2 Prior reviews

---

Given the importance of the State's taxation systems, we have conducted several IT control reviews on them over the past few years.

Our last review was in 2016-17, when we looked at RIO to assess the level of remediation of matters we raised in our 2015-16 review. We again identified numerous control weaknesses. We also confirmed that several matters raised in our 2012-13 and 2015-16 RIO reviews still required management attention.

For further details of our 2016-17 review refer to our Supplementary Report for the year ended 30 June 2016 *RevenueSA Information Online system: October 2016*.

In 2018, we intended to review both RIO and the then new RSAOL system. We postponed this as RevenueSA was in the process of undertaking a major upgrade of RIO. The upgrade aimed to implement improvements in user access controls and was intended to resolve several matters that we had previously raised.

## 3.3 What we reviewed

---

In 2018-19, we reviewed RIO and RSAOL. The scope of work included:

- testing selected application controls relating to specific business processes including revenue, cash management and general ledger audit cycles. Some of the key areas considered included segregation of duties, logical access controls, billing, receipting, master files/standing data update, interfaces/general ledger updates and transactional adjustments
- testing IT general controls (ITGCs) over RIO and RSAOL that directly support the reliable processing of financial information. This included testing the implementation of key controls operating within and around the two systems, such as change management, user access management, password configuration, selected application controls, backup and disaster recovery, problem and incident management, patch management and operating system and database security

- validating selected system business exception rules including land tax, ESL and payroll tax in the RIO application
- following up previously raised audit issues to assess remediation action undertaken (where applicable).

## 3.4 Recent control improvements

---

Based on the scope of testing performed, we noted that 12 of the 25 issues we raised in our 2016-17 RIO review were fully remediated.

Some of the control improvements implemented by RevenueSA since that previous review were:

- updated central problem and change management processes for RIO to enable effective tracking and prioritisation of standard changes and system issues
- processes to review and remove dormant and terminated application user access accounts in RIO<sup>7</sup>
- password management software used to store administrative account passwords
- establishing a segregation of duties ruleset and a process that defines potential conflicting access permissions within RIO. This assists in decision-making about access changes
- a firefighting<sup>8</sup> mechanism for emergency application access to RIO. These access requests are also initiated through a service desk and the activities performed are logged and monitored.

Despite these control improvements, our 2018-19 review noted that several previously raised findings are yet to be fully remediated. The following section highlights previous and new high and medium risk findings that need to be remediated promptly.

## 3.5 What we found

---

Our review of the RIO and RSAOL applications and associated servers and databases highlighted the following application issues.

Finding 3.5.11 relates to the computer servers used by the databases and applications.

---

<sup>7</sup> We have raised some deficiencies in this new process in sections 3.5.2 and 3.5.7.

<sup>8</sup> Firefighting: a firefighting role has been created in RIO for authorised users to undertake tasks that require elevated privileges. For example, a developer may need this access to investigate an unusual incident. As a mitigating control, access is temporary and activities performed are logged and monitored.

### 3.5.1 Excessive access assigned to sensitive RIO functions

While DTF has actioned some of our previous recommendations on user access, our testing identified that several users still had excessive access to critical and sensitive system functions<sup>9</sup> in RIO. This may compromise data integrity and increase the risk of inappropriate changes to financial data.

Among the users with access to sensitive functions, we noted that 18 vendor technical support users for the RIO environment had similar privileges. These privileges enable the creation, editing, deletion and approval of all business transactions.

### 3.5.2 Periodic review of RIO user access privileges is not being performed

A quarterly review is performed to validate user accounts across RIO and RSAOL. These reviews only validate the currency of users and do not assess the appropriateness and potential privileged user access conflicts assigned within these applications.

We found that several users had higher privileges assigned in RIO that do not align with their current job role. This increases the risk of those users intentionally or inadvertently performing unauthorised transactions.

### 3.5.3 Developers have access to the RSAOL production environment

Our review identified that development activities in RSAOL are performed by the vendor and DTF's internal support team. These teams were assigned privileged administrative access on the RSAOL production environment. They can also migrate system changes into the RSAOL production environment.

This increases the ability of these teams to develop and deploy unauthorised or fraudulent changes directly into the production environment.

### 3.5.4 Access to create business partners, create new parcels and perform valuations is not adequately segregated within RIO

While land parcel and valuation data are received from the Land Services Group<sup>10</sup> daily batch file process, several users were assigned a specific system role allowing them to manually create business partners, create new land parcels and assign land valuations.

This increases the risk of fraudulent land parcel entries being manually created in RIO.

Although management is aware of this risk, there is no detective control in place to formally review the appropriateness of these high-risk manual entries.

---

<sup>9</sup> These functions are a series of subprograms that may allow access to sensitive and confidential data and/or information.

<sup>10</sup> Refer to the Appendix for details of integration with Land Services Group data.

### 3.5.5 Default RIO user accounts are not being disabled

The RIO environment comes with several default user accounts. While DTF has disabled most of these default accounts and changed their respective passwords, we noted that some default accounts remain unlocked and/or not changed in RIO.

This increases the risk of data loss through security compromises where default user credentials have not been changed or remain active.

### 3.5.6 Weak password controls exist in RIO and RSAOL

We noted that RIO and RSAOL's password control configurations are not aligned with DTF's network password policy and industry better practice.

While most RIO users are authenticated using single sign on, which enforces stronger password controls, there are several system and administrator accounts that authenticate directly through RIO's operating system.

There is a risk that RIO or RSAOL system and administrator accounts could be compromised by using inadequate password controls.

### 3.5.7 RIO user access termination process is not consistent

While DTF has implemented a detective process by performing quarterly user audits, several user accounts were not disabled immediately after termination of their employment. Failure to promptly revoke access increases the risk of unauthorised users performing inappropriate, malicious or fraudulent activities.

In addition, we noted that a terminated vendor support team user account was still active in RIO at the time of our audit.

While these terminated users have not logged into their accounts after their termination dates, their user accounts still existed and needed to be removed from the system.

### 3.5.8 RIO system and client setting changes are not being performed through the recommended process

RIO's administrative function provides privileged users with the ability to centrally manage user master records across the entire RIO system.

We have noted instances where changes to user access were performed through a batch job rather than using RIO's recommended administrative function. This increases the risk of excessive, inappropriate or unauthorised user access being granted.

### 3.5.9 RIO custom programs, transaction codes and tables are not appropriately restricted

Our follow up review of security over custom program, transaction codes and tables mapped to authorisation objects or classes across the RIO production environment indicated that further restrictions still need to occur.

This increases the risk of inappropriate access to the custom programs, tables and sensitive data.

### 3.5.10 Transaction level audit logging is not enabled in RIO

User transaction logging to record and monitor transaction changes is currently not enabled within the RIO production environment.

We also confirmed that logs recording the firefighting/emergency access process are only retained for three days.

This limits visibility over the history of transactions processed and/or changes applied to master data when investigating potential incidents or invalid transactions.

### 3.5.11 Security weaknesses exist in database and application servers

Several security weaknesses were identified within the server databases supporting RIO and RSAOL including:

- 'execute' privileges were incorrectly assigned to a database role enabling these users to execute functions or stored procedures
- default account(s) were enabled
- limited security events logging
- certain highly privileged accounts were used on the RSAOL database schema<sup>11</sup>
- inconsistent patching on the databases
- inadequately configured key server database parameters.

Inadequate security controls increase the database's vulnerability to malicious changes, unauthorised access, viruses and denial of service attacks. This could result in unauthorised disclosure, alteration or destruction of data.

Several security weaknesses were also identified in relation to the RIO and RSAOL servers, including:

- administrative user account passwords were not regularly changed
- auditing of key security events was not performed.

This increased the risk of passwords being compromised and limits the ability to trace key security events and inappropriate or unauthorised access by user(s).

---

<sup>11</sup> Database schema is the repository which assists in the logical grouping of database objects.

## 3.6 What we recommended

---

We recommended the following to DTF:

- improving user access management, through ongoing periodic reviews, timely removal of inactive user accounts, deactivating default system accounts and tightening/restricting access to sensitive data, transactions, tables and programs
- improving segregation of duties across change management for the RSAOL environment and transaction access in the RIO environment
- strengthening password controls
- making system and client setting changes through the recommended interface
- enabling transaction level audit logging
- improving security settings and functions for operating systems and databases.

## 3.7 Agency response

---

DTF responded positively to all findings and recommendations and provided details of proposed remediation action and completion time frames.

We note that several of our recommendations have already been partially actioned, with the rest to be completed by September 2020.

## 4 Active Directory within the SA Government

The State Active Directory (AD) provides authentication services (ie login) to around 27 000 users and access to networked resources across many SA Government agencies.

AD provides a way to manage ICT resources and allows access to the following across - government and agency-based services:

- electronic messaging services (such as email)
- file storage and print servers
- web services
- applications.

### What we found

Our review of AD across several SA Government agencies identified areas that could be strengthened, including:

- domain security and password configuration settings
- user access privileges
- legacy operating systems
- authentication and communication configurations
- managing the outcomes from AD risk assessments
- testing of AD environment disaster recovery and documenting recovery procedures
- domain trust relationships.

These observations do not necessarily apply to all AD environments we reviewed.

### What we recommended

We provided each agency we tested with recommendations to further strengthen their AD environment.

This included specific details of domain security and password configuration settings. It also included reducing the number of privileged user and inactive accounts. Some privileged user activities and trust relationships need to be reassessed and any legacy servers and workstations should be removed.

We also recommended that agencies improve the monitoring and management of known vulnerabilities, with increased communication between agencies.

Finally, we recommended that the Department of the Premier and Cabinet (DPC), as the governing agency, establish a disaster recovery test schedule for the State AD and Resource Directory (RD). Detailed recovery procedures and test plans should be developed to support identified test scenarios.



## 4.1 Introduction

---

The SA Government network is known as StateNet and incorporates several, but not all, SA Government agency networks and AD forests.<sup>12</sup> StateNet has grown to become a large, complex environment. Its inter-connected agency relationships, coupled with differing agency environments and continual machinery of government changes, make it a difficult environment to implement cross-departmental AD-integrated security solutions.

A key forest, the State AD, contains several agency AD domains.<sup>13</sup> In addition, the State RD is configured to allow agencies to share resources across StateNet.

The State AD and RD structures are governed by DPC's ICT Services and is operationally managed by an external vendor under a formal services support agreement. DPC maintains the primary relationship with the external vendor and supports other agencies with the procurement of their services, with the aim to reduce agency procurement risks.

While DPC provides this support, ultimately each agency is responsible for managing and securing its own AD environment. This includes domain configurations, including creating and managing trust relationships between agency networks, domain controller security settings, groups/accounts and firewalls.

In 2014-15, we sought an understanding of the controls implemented to manage and secure the State AD forest. This included governance arrangements, relevant aspects of IT security mandated by the SA Government *Information Security Management Framework* (ISMF) and business continuity arrangements.

We made several recommendations for improvement at that time, including finalising key procedure documentation and implementing an Information Security Management System, strengthening the ongoing monitoring of outstanding issues requiring remediation and periodic testing of business continuity arrangements.

## 4.2 What we reviewed

---

In 2018-19 we conducted a further review of the adequacy of selected governance and security controls applied to the current StateNet AD environment. To do this we selected a sample of agencies for testing.

We conducted our review with help from an external specialist and included selected testing of:

- AD structure governance arrangements
- AD risk management approach

---

<sup>12</sup> A forest is a collection of one or more domains that share a common global catalogue, directory schema, logical structure, and directory configuration.

<sup>13</sup> An AD domain is a collection of objects, including computers, users and groups. within a Microsoft AD network.

- AD assurance and reporting
- AD trust relationships
- domain controller patch management
- domain controller password policies
- privileged users
- change management
- firewall configuration<sup>14</sup>
- backup and disaster recovery.

## 4.3 What we found

---

Our 2018-19 review identified several security control areas that could be strengthened. Some findings were rated as high or medium, as we concluded that they increase the risk of malicious users gaining access to agency networks and sensitive information.

Due to the sensitivity of this review, we have not detailed our findings in this Report. Specific details were provided to each agency for their attention and remediation. We provide only a high-level summary of the outcomes in the following sections.

### 4.3.1 Domain security and password configuration settings

Weaknesses were found in some domain security and password configuration settings.

Some of the domain security configuration setting weaknesses increased the risk of attackers gaining access to domain information. Although the exact information that can be disclosed varies according to each agency domain configuration, it may include extracting key system details such as user listings and domain policies.

We also found weaknesses in the password management and configuration settings of some agencies. These password controls are used to manage authentication and prevent unauthorised user access to the AD environment.

### 4.3.2 User access privileges

Our review identified an excessive number of privileged user accounts. Typically, these accounts provide a higher level of access, including the ability to create and modify user accounts and access agency sensitive information.

We also identified some privileged user activities that should be reassessed, including their login techniques and the elevation of privileges.

---

<sup>14</sup> A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

Further, we noted an excessive number of inactive user accounts and instances where user and service accounts contained privileges above the user's current job/role function. This is due to certain configurations, assigned attributes or group memberships.

### 4.3.3 Legacy operating systems

We identified several legacy servers and workstations listed in agency domains that were using outdated operating systems that need to be upgraded or replaced. These systems either no longer receive vendor security patches<sup>15</sup> or only receive vendor support for a defined period.

We acknowledge that some of these legacy workstation and server accounts may no longer be active or in use.

### 4.3.4 Authentication and communication configurations

In addition to the password deficiencies in section 4.3.1, we identified that certain authentication protocols, authority and communication mechanisms require further restriction. This would reduce the risk of attackers taking control of domain user accounts and hosts to conduct further network attacks, gain access to sensitive information and modify agency workflows or information.

The weaknesses we found may enable account passwords to be compromised, remote code execution, unauthorised access to authentication certificates and data intercepted or modified in transit between hosts.

### 4.3.5 Managing the outcomes from Active Directory risk assessments

DPC proactively performs annual risk assessments of the State AD and RD using an external service provider. These risk assessment reports include details of some individual agency vulnerabilities requiring attention, which are provided to the agency.

We acknowledge that ultimately each agency must secure its own AD environment and therefore it is up to them to appropriately remediate any high and medium risks communicated to them. However, under the current arrangement DPC is not advised by other agencies whether their recommendations have been appropriately actioned. Therefore, it was unclear whether issues were sufficiently remediated from a whole-of-government perspective.

In addition, for one agency we tested, the risks identified in the most recent assessment were actioned but were not documented, monitored or reported on within the agency. This included the risks not being recorded in its corporate risk register. In addition, this agency

---

<sup>15</sup> A patch is a piece of software that is designed to fix defects and known vulnerabilities or provide updates to an information system.

had not performed its own AD risk assessments but instead relied on DPC's risk assessments. This could be partially attributed to a lack of clarity about roles and responsibilities between agencies.

#### 4.3.6 Testing of Active Directory environment disaster recovery and documentation of recovery procedures

Planning for disasters is an important part of the risk management process. An AD disaster recovery plan helps to ensure that access and authentication to State AD and RD is available in the event of interruption or helps to restore these services when required.

We noted that the existing Service Continuity Plan does not incorporate recovery procedures, a test plan scenario or recovery time objectives,<sup>16</sup> recovery point objectives<sup>17</sup> and maximum allowable outage<sup>18</sup> times.

In addition, an AD disaster recovery test has not been conducted for the State AD and RD environments. Therefore, there is a risk that recovery would not be made within maximum allowable outage time frames in the event of a disaster or system failure.

#### 4.3.7 Domain trust relationships

The State AD and RD forests include several trust relationships to share resources between agency domains. A trust can be one directional or can operate in both directions and the level of trust can be configured accordingly.

In assessing the current trust relationships, we noted that their appropriateness may need to be reconfirmed to ensure they are still required for current business purposes. For example, for one agency a trust relationship remained active despite the trusted domain being decommissioned.

### 4.4 What we recommended

---

We provided each agency we tested with recommendations to further strengthen their AD environment.

This included specific details of domain security and password configuration settings and reducing the number of privileged user and inactive accounts. Some privileged user activities and trust relationships need to be reassessed and any legacy servers and workstations should be removed.

---

<sup>16</sup> The length of time it will take to restore a key business system after a failure or disaster occurs.

<sup>17</sup> The amount of data that could potentially be lost during a disaster.

<sup>18</sup> The maximum length of time that can elapse before a business process outage is considered unacceptable or intolerable.

We also recommended that agencies improve the monitoring and management of known vulnerabilities, with increased communication between agencies.

Finally, we recommended that DPC establish a disaster recovery test schedule for the State AD and RD. Detailed recovery procedures and test plans should be developed for identified test scenarios.

## 4.5 Agency responses

---

Two agencies had responded to our findings at the time of this Report. Their responses were generally positive, and provided details of proposed remediation actions. The other agencies we reviewed were still preparing their responses.

## 5 End User Computing (ICT desktop outsourcing) program

In February 2017, the End User Computing program (the EUC Program) agreement was signed between the SA Government and DXC Australia Technology Pty Ltd (DXC) for seven years, with extensions available to a maximum term of 10 years. The aim of the EUC Program was to reduce agency ICT operating costs and increase ICT productivity across SA Government agencies through a desktop-as-a-service arrangement with DXC.<sup>19</sup> This involved outsourcing the support and maintenance of ICT desktop devices, initially planned for 17 agencies.

The EUC Program was to be implemented in individual stages called tranches. While the EUC agreement did not specify time frames for each tranche and associated tranche phases, it was originally expected that implementation of the program for all 17 agencies would be completed by February 2019.

In 2017-18, we reviewed the EUC Program and reported our findings in the Auditor-General's Annual Report.<sup>20</sup> At that time, we noted that the EUC Program was experiencing several challenges, including:

- implementation delays
- budget overruns and increased costs
- contractual challenges
- challenges impacting future rollout.

In 2018-19, we did a follow-up review of the EUC Program. This included reviewing the current scope and implementation status, program costs, benefits realisation, outstanding activities and challenges.

### What we found

Since our last review, the SA Government has decided that no further tranches will be delivered beyond the two Tranche 1 agencies: the Department of the Premier and Cabinet (DPC) and SA Health (the Department for Health and Wellbeing and associated local health networks). This is a significant reduction in scope for the EUC Program from the original 17 agencies.

---

<sup>19</sup> Desktop-as-a-service is typically a vendor hosted and managed end-to-end desktop service that accommodates both virtual and traditional desktops (desktop, laptops, tablets and other computing devices) using a variety of support management models. It is usually provided on vendor supplied and managed assets.

<sup>20</sup> Report 5 of 2018 *Annual report for the year ended 30 June 2018, Part A: Executive Summary*, pp 91-96.

The amended total cost relating to just SA Health and DPC is now \$175.4 million (GST inclusive) for seven years and \$245.8 million (GST inclusive) for 10 years. This compares to the expected costs for 17 agencies of \$317.3 million (GST inclusive) for seven years and \$457.2 million (GST inclusive) for 10 years.

For DPC and SA Health the migration process remains problematic and complex, with the EUC Program continuing to fall behind schedule and incurring increased costs. We noted that due to the reduced scope, revised financial modelling and incorrect initial assumptions, the financial savings originally anticipated for the EUC Program will not be achieved.

Tranche 1 has received approval of \$48 million for increased contract costs and removal of an estimated \$37 million of expected savings.

The Department of Treasury and Finance (DTF), on behalf of the SA Government, finalised negotiations for a contractual variation with DXC to resolve the ongoing issues, delays and disputes that have plagued the EUC Program since its inception. DTF advised that the current contract variation will not increase the cost of the contract with DXC.

The EUC Program requires close monitoring and ongoing strategic management to ensure that the implementation for DPC and SA Health is finalised within the revised budget and timelines.

The 15 agencies that are now out of scope will need to develop alternative strategies for managing their desktop environments in the long term.

## 5.1 Introduction

---

The implementation of Tranche 1 of the EUC Program was restricted to DPC and SA Health. On its completion, it was intended that additional tranches for the remaining 15 in-scope agencies would be implemented.

Within each tranche are two subcomponents called phases: transition and transformation. The transition phase covers the transfer of in-scope agency staff and EUC services to DXC. The transformation phase involves DXC providing desktop services and ongoing administration.

Under the EUC Program, devices are purchased by DXC and leased back to the agencies. DXC provides a range of application packaging, deployment and general IT support services once each device has been migrated onto DXC's Windows 10 environment. As part of this process agencies are required to ensure that the applications their staff use are Windows 10 compliant.

Once devices were transformed it was expected that the price paid per device would reduce the overall operating costs of each in-scope agency.

DPC managed the EUC Program's transition phase until that phase was closed in January 2019. The next phase, the transformation phase, was transferred to DPC and SA Health as part of their business as usual operations.

Ongoing contract management of the EUC Program has since transferred to DTF's Strategic Procurement unit.

## 5.2 What we reviewed

---

Similar to last year's review, we performed a follow-up review of the EUC Program's costs, contract updates, ongoing implementation status, benefits realisation and current challenges.

Last year we reported that certain key documentation about the EUC Program was not made available to us because it was linked to Cabinet submissions and regarded as Cabinet in confidence. We were advised that there have not been any further Cabinet submissions for the EUC Program since then.

## 5.3 Transformation implementation status

---

### 5.3.1 DPC status

DPC continues to migrate its devices to Windows 10 as part of the transformation phase. It intended to migrate all of its devices by August 2019.

A Windows 10 upgrade delayed the migration process, and as at 23 July 2019 only 96 of a total 633 devices had been transformed. The Windows 10 upgrade process was recently finalised, and the migration of DPC devices recommenced.

### 5.3.2 SA Health status

To help with its device migration strategy, SA Health initiated the EUC transformation (Windows 10) project. This project was tasked with upgrading SA Health devices to Windows 10 through a phased approach. The phases include planning, piloting and deploying. The planning phase has been completed, with the pilot phase currently underway using a series of small device deployments across SA Health's business areas. Once the initial pilot phases have been completed, larger group deployments across SA Health are intended to occur.

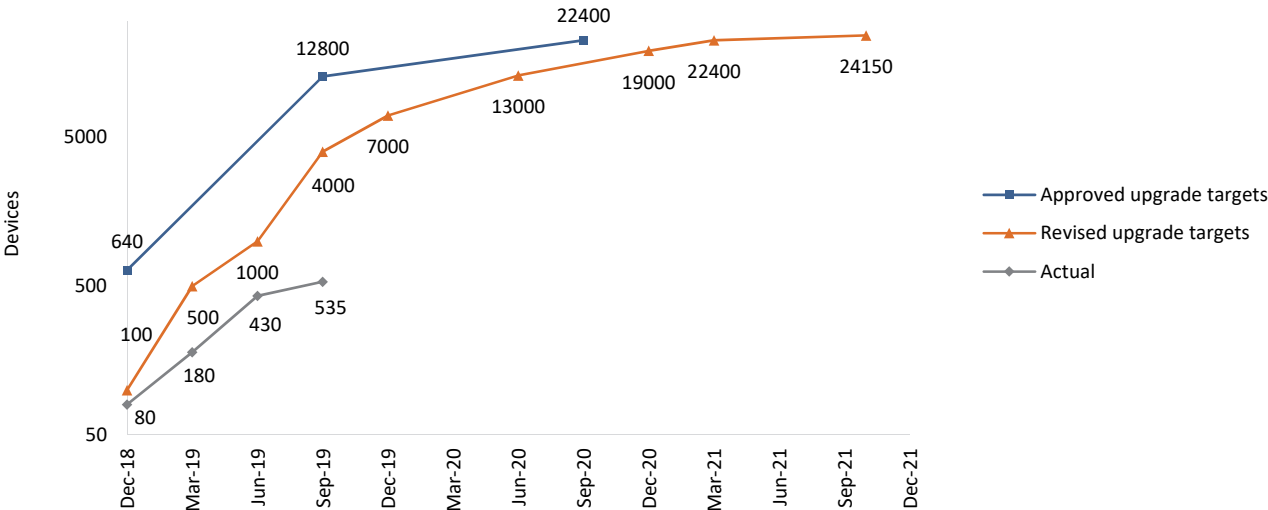
SA Health has a total desktop environment fleet of 34 500 devices. As at early September 2019, the number of upgraded devices was 535 out of the revised target of 24 150 devices that are now expected to be migrated by October 2021.



SA Health continues to face complexities and is still validating key applications to ensure they are Windows 10 compatible and fully supported. We were advised that around 10 000 of the total desktop environment fleet currently fall outside of the initial migration strategy and will be the subject of further application compliance analysis. This ongoing analysis will help to determine the suitability and supportability of these devices in the Windows 10 environment. This is expected to occur after 2021.

Throughout the Windows 10 project the timelines and number of targeted devices for migration has continued to change. Figure 5.1 shows the current implementation status against the approved and revised device migration targets. In particular, it highlights that the actual number of devices that have been migrated to Windows 10 has continued to fall below the original approved and revised upgrade targets.

**Figure 5.1: SA Health Windows 10 upgrade migration targets<sup>21</sup>**



SA Health continues to face challenges that are impacting their overall Windows 10 project time frame. These include delays in the project’s pilot migration schedule, associated Windows 10 dependencies and unexpected increases in the number of potential devices to be migrated.

## 5.4 Program costs

The primary aim of the EUC Program was to reduce agency ICT operating costs and increase ICT productivity across government agencies by outsourcing the support and maintenance of EUC devices.

The cost of the EUC Program, with DXC providing the services over seven years, was originally estimated at \$280.5 million (GST inclusive) and \$394.2 million (GST inclusive) for 10 years. This covered the EUC Program’s transition and transformation phases for 17 in-scope agencies.

<sup>21</sup> SA Health is currently undertaking a project assessment to highlight potential impacts of the recent contract variation and additional devices included with SA Health’s total desktop fleet.

Since the EUC Program started in February 2017, costs per in-scope agency have continued to increase. In August 2017, the EUC Program’s financial model, assumptions and savings opportunities was reviewed. This identified that parts of the original business case were incorrect, resulting in the EUC Program’s total cost increasing to \$317.3 million (GST inclusive) for seven years and \$457 million (GST inclusive) for 10 years.

The SA Government approved additional funding for Tranche 1 (SA Health and DPC). This covered increased contract charges (\$48 million) and the removal of estimated financial savings (\$37 million) from the EUC Program, and other related areas (eg accommodation).

Additional funding of around \$5.5 million was provided to SA Health to help ensure that its current applications are Windows 10 compatible. SA Health has since acknowledged that this additional funding may not be enough to perform this task, with more funding potentially required in future. Any additional funding would further impact the total cost of the EUC Program.

Based on the revised cost of the EUC Program and other challenges, the State decided that the EUC Program would not progress beyond Tranche 1.

The amended total cost relating to just SA Health and DPC is now \$175.4 million (GST inclusive) for seven years and \$245.8 million (GST inclusive) for 10 years.

Figure 5.2 shows the changes in total EUC Program costs and reduction of in-scope agencies.

**Figure 5.2: Changes in total EUC Program costs for in-scope agencies**

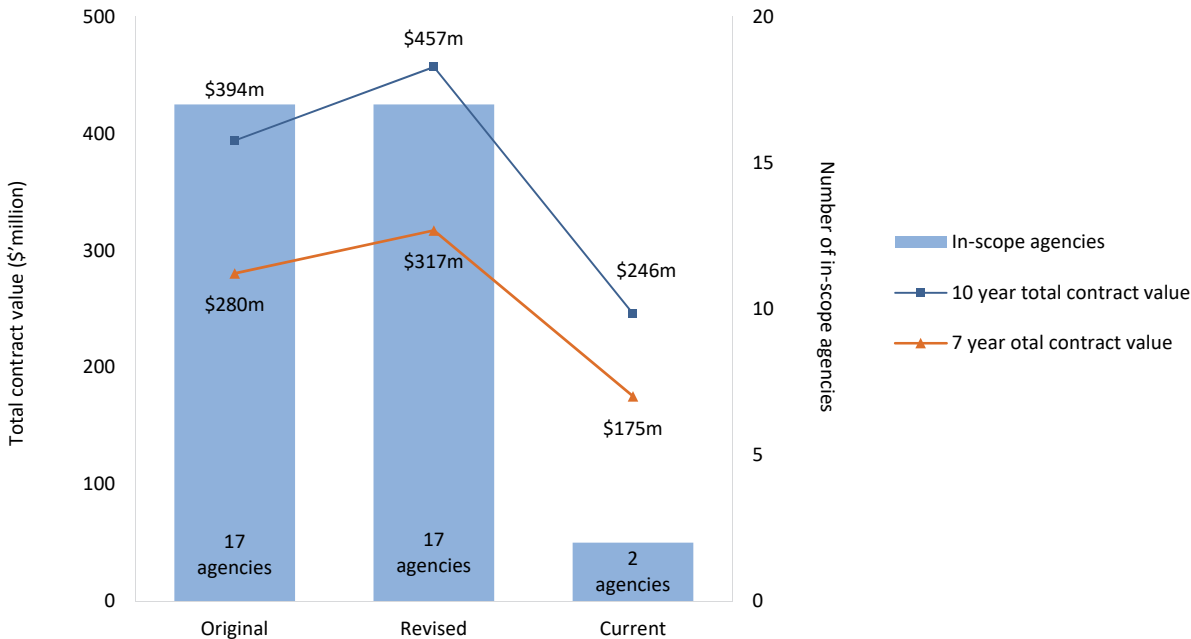


Figure 5.3 shows the total EUC Program costs for Tranche 1 in-scope agencies as at 30 June 2019.

**Figure 5.3: Breakdown of total EUC Program costs for in-scope agencies as at 30 June 2019<sup>22</sup>**

Final program scope	Contract term	Agency	Revised current total costs (including GST) \$'million
Tranche 1: Two in-scope agencies (SA Health and DPC)	<b>10 years</b>	SA Health	226.65
		DPC	19.20
		<b>Total</b>	<b>245.85</b>
	<b>7 years</b>	SA Health	161.63
		DPC	13.73
		<b>Total</b>	<b>175.36</b>

As of 30 June 2019, expenditure under the EUC contract totalled \$21.4 million – \$19.6 million for SA Health and \$1.8 million for DPC.

In addition to the contract expenditure, in 2018-19 around \$700 000 was incurred by DTF in administering the EUC Program, against a budget of \$1.46 million.

The total cost of the EUC Program is likely to continue to change due to contract variations, delays in the transformation phase and current program challenges.

Due to these ongoing amendments to the EUC Program, it is proposed that once the transformation activities for DPC and SA Health are completed, a revised estimated total EUC Program cost will be calculated.<sup>23</sup>

## 5.5 Contract update

The delivery of services under the EUC agreement continues to be challenging.

In September 2018, both parties agreed to participate in a review and renegotiation (reset) of the EUC agreement. The reset negotiation, which was still in progress at the time of our review, focused on contractual issues, operational progress, continuing challenges, risks and clarification of responsibilities by both parties.

### 5.5.1 Ongoing contract variations

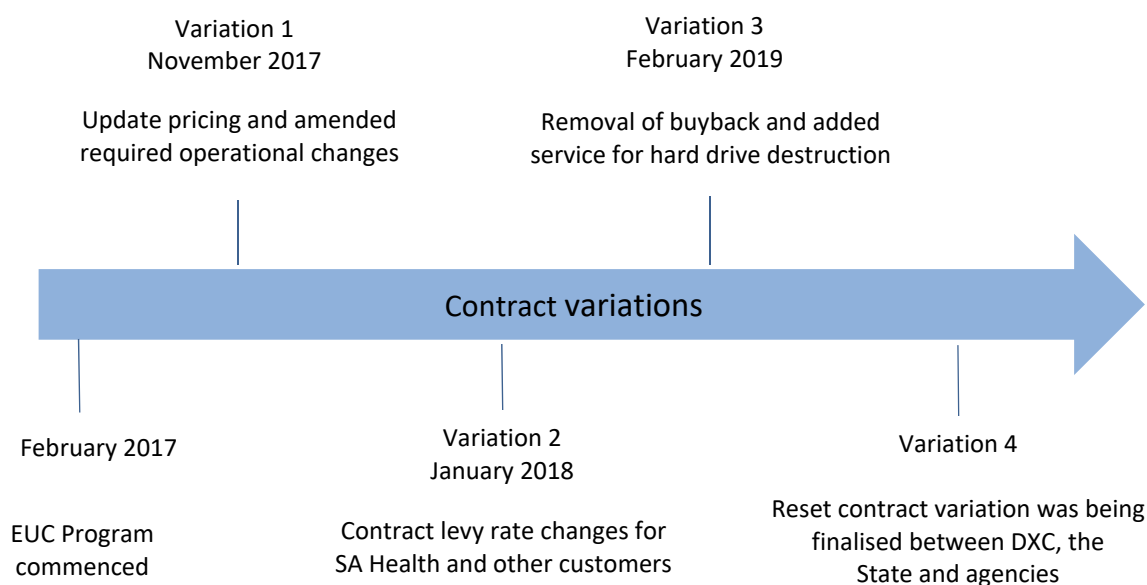
Since the EUC Program was initiated, there have been several contract variations. These changes were continuing at the time of this review, with another contract variation being finalised.

The outcome of the reset negotiation will form the baseline of any future contract variation between the State and DXC.

<sup>22</sup> The budget and expenditure figures to date were provided by DTF and are unaudited.

<sup>23</sup> Strategic Procurement, a business unit within DTF, is responsible for managing the EUC program contract.

**Figure 5.4: Contract variation timeline**



The reset contract variation is likely to include:

- redefining transformation milestones, deliverables and payment schedules
- defining regional and remote area support provisions
- incorporating 24x7 support services for regional areas
- revision of core applications and supported operating systems within the program
- increased application remediation services
- amendments to optional services currently not required by DPC or SA Health
- amendments to the application packaging service fee
- updates to device catalogue and changes to service levels.

## 5.5.2 Annual contract reviews

After the EUC Program was established, it was agreed that an annual contract review would be performed to determine the adequacy of the contract and DXC's performance over the year. The initial review was performed and recommendations for change were approved in mid-2018. In July 2019, a second review was performed, with the resulting recommendations approved.

The July 2019 review acknowledged that the transition phase of the EUC Program was effectively closed on 31 January 2019 as no further agency transitions/tranches were to occur. It also acknowledged that the EUC Program is continuing to work with DPC and SA Health to develop their transformation plans and time frames under the contract.

The review also identified several concerns specific to the contract, including the following:

- The last machinery of government changes and termination of future tranches has precluded the anticipated minimum device targets being achieved. This will result in an increase in the support price by a further 7% per device.

- The transformation phase initially estimated that 80% of all end user devices for DPC and SA Health would be in place by 2018. This target was revised due to difficulties in upgrading devices to the Windows 10 environment.
- The device catalogue developed by DXC has been updated in consultation with the SA Government and agencies. While the updated catalogue increased the services being offered, the price for devices and some services also increased.
- SA Health will pay a higher support price for devices that are yet to be transformed until application remediation is completed.

## 5.6 Benefits realisation

---

The EUC Program advised that several positive program outcomes have occurred. This includes improved security associated with upgrading ageing and legacy devices and provides an opportunity for DPC and SA Health to reduce their ongoing operating costs once all devices are transformed. Migrating legacy devices to the Windows 10 environment may not have occurred at a similar rate without this program.

Despite these benefits, the overall expected benefits from the EUC Program have reduced. In particular, the savings target has fallen by \$35 million, for the total cost of the EUC Program significantly increasing by \$48 million. This has primarily been caused by implementation delays, Windows 10 compatibility challenges and the reduced number of agencies participating in the EUC Program.

In addition, the failure to achieve the contracted minimum volume level of 55 000 units through the termination of future tranches has resulted in an increased support cost of 7% per device. EUC Program delays have also increased the potential for extra costs to be incurred by SA Health if ongoing Microsoft Windows 7 support<sup>24</sup> beyond 2020 is required.

Other challenges, documented in section 5.8, may also result in additional costs and reduced benefits.

We were advised that after all DPC and SA Health devices are migrated to Windows 10 a formal post-implementation and benefit realisation assessment will be performed.

## 5.7 SA Health client satisfaction surveys

---

SA Health, as part of the pilot phase of its Windows 10 project, initiated several small pilot deployment exercises to prepare for larger group deployments of devices across its business areas.

Following these small pilot projects, SA Health surveyed the participating users to understand their migration experience and overall satisfaction and to identify any migration issues that may have occurred.

---

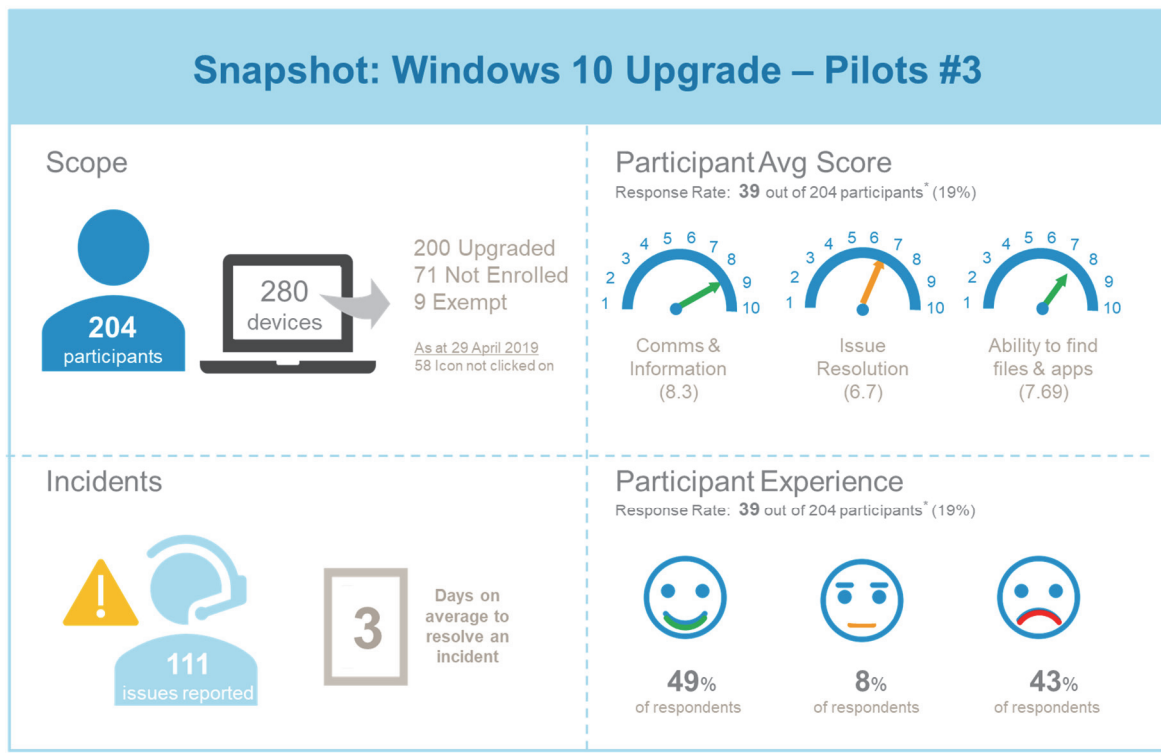
<sup>24</sup> Microsoft will stop supporting Windows 7 devices (laptops and desktops) in January 2020.

### 5.7.1 Internal user satisfaction survey

In May 2019, after the third pilot project was finalised, a user satisfaction survey was conducted. Participants were asked the following questions about their device being migrated to Windows 10 as part of the ongoing upgrade:

- Prior communications via multiple emails were sufficient during my upgrade (including participant fact sheet and reference guide and reminder correspondence).
- I felt confident about how to access support during my upgrade.
- On-screen messages were easy to follow.
- The reference guide was helpful during my upgrade.
- Technical issues with my upgrade were resolved effectively and on time.
- I was able to locate all my files and applications following my upgrade.
- My overall windows 10 upgrade experience was positive.

**Figure 5.5: Summary of Windows 10 Pilot 3 program survey results**



Source: SA Health (May 2019).

A summary of positive and negative general survey user comments confirmed that while a number of users found the device upgrade quick, easy and seamless with no data loss, there were also negative experiences.

General negative feedback suggested that upgrade reference guides and system alerts were not always followed or available. Users also experienced instances where multiple programs were missing from their devices which required them to seek further support. Some users were also required to undertake the installation process more than once and application device settings were not always correctly configured.

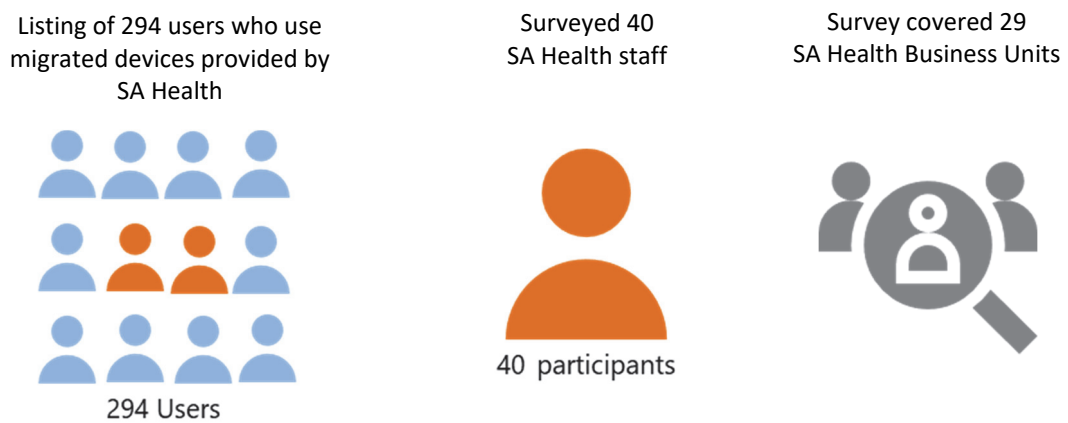
Participants also raised issues regarding the preparation and readiness of the help desk and time taken to complete the device upgrade. It also highlighted that the resolution of certain matters was by email rather than through phone conversations. This sometimes increased delays in installation, especially for remote users, when attempting to upgrade their devices. These issues impacted their general day-to-day work functions and overall connectivity.

Based on the above survey results, SA Health made several adjustments to improve its migration processes.

### 5.7.2 Auditor-General’s satisfaction survey

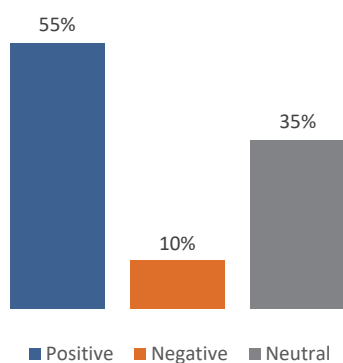
In mid-July 2019 we conducted our own survey. Its purpose was to confirm SA Health’s survey results and to get an up-to-date picture of current challenges.

**Figure 5.6: Summary of survey process**



We asked the following questions to gauge the level of satisfaction that pilot participants experienced following the Windows 10 upgrade.

Question 1: What was your overall Windows 10 upgrade experience?



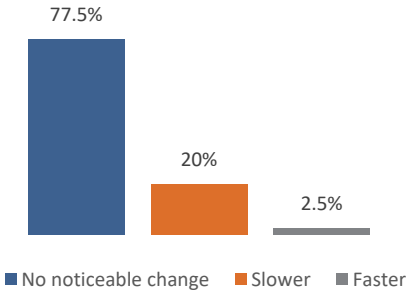
General user comments:

- Good communication during the upgrade.
- Information was easy to understand.
- Interface was easy to follow.
- Trouble navigating through new interface.
- Lack of communication as to when the update was going to take place.

While a large proportion had no concerns relating to the Windows 10 upgrade, several surveyed users experienced some issues that needed to be addressed, including aspects of useability.

Question 2: Has your upgraded device (eg laptop or workstation) been impacted by the following:

Question 2A: Performance/Speed

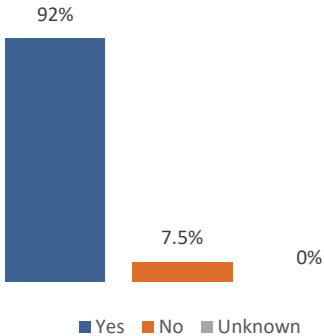


General user comments:

- Performance has slightly improved.
- Device has been slower.

Surveyed staff suggested that in general the new Windows 10 devices either performed at around the same speed or in some instances were slower.

Question 2B: Are you still able to use all software/applications required as part of your job?

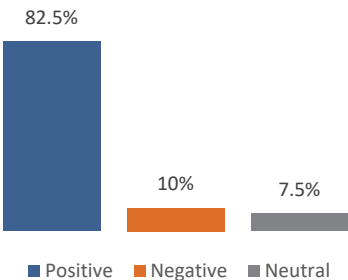


General user comments:

- Outlook is slow, PDF is slow.
- Some applications have disappeared after upgrade.
- Had to repurchase certain licensed software.
- Outlook was not operating properly.

Surveyed staff identified instances where devices associated with the Windows 10 upgrade experienced some degree of difficulty. These difficulties extended to usability of key software and applications, which on some occasions impacted their ability to work effectively.

Question 2C: Reliability of your device



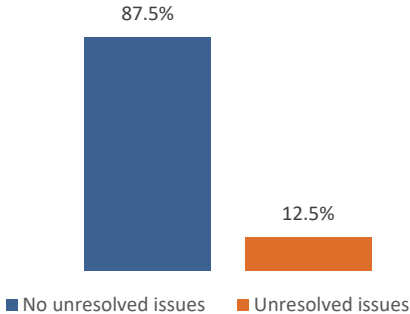
General user comments:

- Device does not turn on straight away.
- Has to use different applications as a main one is not operating.
- Device is not connecting to Wi-Fi.



Generally, most devices were considered to be working reliably, with the exception that some users experienced difficulties implementing key applications and functions on their upgraded device.

Question 3: Do you have any outstanding/unresolved issues with your upgraded device?

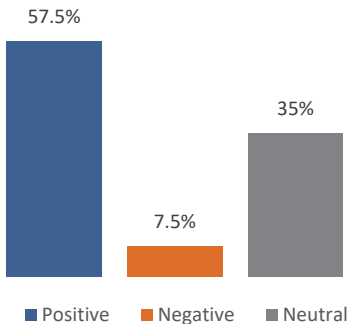


General user comments:

- Some issues have not been resolved.
- Windows licensing keeps popping up.
- Issues with the display settings.
- There are issues every day.

Most users do not have any outstanding issues and for the ones who do, the issues tended to involve perceived slowness of the device and issues with display settings.

Question 4: If you have requested assistance, what is your experience with the level of support available?



General user comments:

- Once the issue was reported the support people dealt with it quickly.
- Support takes too long to resolve.

Over half of the surveyed staff had positive experiences with the available support. The negative experiences were generally due to the amount of time it took to resolve their issues.

### 5.7.3 Satisfaction survey summary

The results of our survey and SA Health’s internal survey highlighted that some users have had problems since the Windows 10 upgrade, but overall user satisfaction was generally positive.

We recommend that SA Health continues to use its Windows 10 pilot program to deploy devices for small user groups, in preparation for larger group deployments that are anticipated in late 2019 and 2020. The ongoing use of client surveys to assess the adequacy of the pilot programs is encouraged and where improvements are identified, they should be promptly implemented.

## 5.8 Current program challenges

---

While the EUC Program is still progressing, it has not reached the point where DPC and SA Health can finalise their transformation phases because both agencies are still migrating devices to Windows 10 and resolving compatibility issues.

The key challenges that are impacting the EUC Program's ability to achieve key milestones, budgets and savings targets include:

- DPC's rollout schedule was recently disrupted by a Windows 10 version upgrade. This postponed its rollout by three months.
- SA Health's application assessment and remediation activities are ongoing and have not been completed within anticipated time frames. At the time of our review SA Health had identified 1100 applications as compliant, 560 applications as non-compliant and 2700 applications still requiring compliance assessment. Key applications used by SA Health that are not compliant impact around 12 000 devices.
- Around 2000 legacy devices in the SA Health fleet cannot be upgraded to Windows 10 due to incompatible applications and hardware issues that continue to impact SA Health's current Windows 10 upgrade program.
- Certain SA Health printer and application server infrastructure are currently not Windows 10 compliant, which could impact over 10 000 devices. In addition, the current number of printers to be supported exceeds the original agreement. DXC and SA Health are currently negotiating ongoing printer support services and associated costs.
- Contract negotiations between the State and DXC are yet to be finalised, such as agreement on the definition of transformation activities, technical solution offerings and roles and responsibilities in the EUC contractual arrangement.

In addition, the 15 out-of-scope agencies associated with the further tranches of the original EUC Program that are not proceeding now need to develop their own alternative Windows 10 upgrade strategy and support arrangements.

## 6 Education Management System project

The Department for Education (DfE) is the SA Government body responsible for delivering education, safety and development outcomes for children and students.

DfE has indicated that its legacy school administration, curriculum and finance systems are no longer meeting the needs of schools and preschools. They have limited functionality, failures have occurred at some sites and several workarounds have been developed, resulting in inefficiencies. Each school also has a separate instance of the Education Department School Administration System (EDSAS), with varying configurations.

To address these issues, DfE intends to replace the legacy systems, EDSAS for schools and the Early Years System (EYS) for preschools. In February 2015, an Education Management System (EMS) business case was developed and in December 2016 a submission to acquire an EMS was approved by the SA Government. This resulted in a 10-year contract with an application vendor (Civica Pty Ltd) in September 2018 to implement an EMS.

The total budget for the EMS implementation is \$130 million. This includes the 10-year contract with Civica for system implementation and support services of \$76 million.

### What we found

Once implemented EMS is intended to replace several legacy systems used in SA Government managed schools and preschools (sites).

Some early project delays were experienced, mostly due to procurement activities and the time taken to submit the business case for initial SA Government approval. EMS was originally expected to be rolled out by mid-2020, but this will not occur.

Despite these delays, the EMS Project has been able recover some time by entering a pilot phase to test 'out of the box' functionalities, prior to any level of customisation of the core EMS modules. Entering the pilot phase was intended to inform the broader rollout strategy.

The EMS Project rolled out the core EMS modules to 10 pilot sites across the metropolitan area and one regional school in Port Lincoln. This included a mix of preschools, primary schools and high schools. The sites operated EMS in parallel with their existing systems throughout the pilot phase, to the end of term 2, 2019. At the end of July 2019, the EMS Project Board endorsed proceeding with the implementation phase of the project.

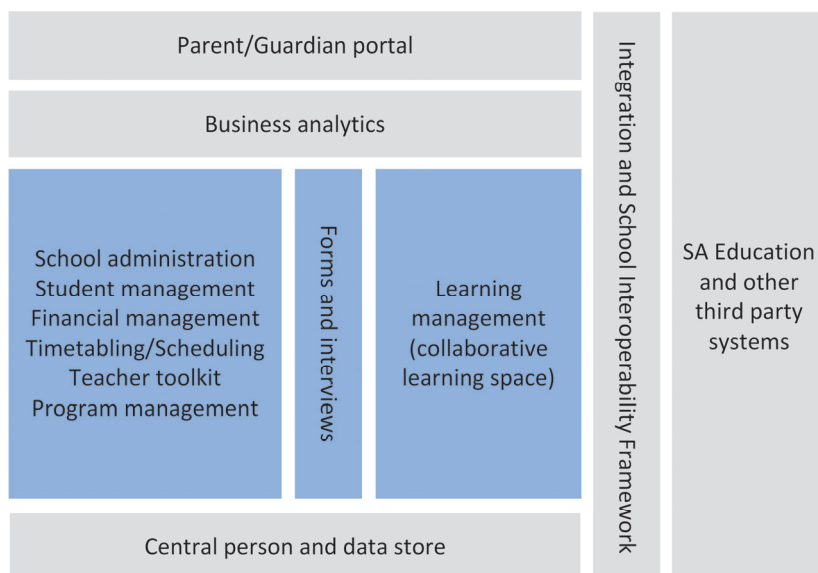
The full rollout is now scheduled to commence in school term 2, 2020 (end of April 2020 to early-July 2020) and is not expected to be completed until the end of 2023. Implementing EMS to over 900 sites in a three-year period (approximately one site per day) is an aggressive rollout schedule. The EMS Project may need to consider the time it has taken to implement EMS at the pilot sites and whether the rollout schedule is achievable.

Our high-level review of the EMS Project has not identified any concerns about the budget expenditure at this point.<sup>25</sup> The EMS Project is well structured, with key controls in place that we would expect to see in a project of this size and nature. While these controls exist and most key project risks appear to be appropriately managed, we did identify some challenges and areas where management attention is required.

## 6.1 Introduction

EMS is an ‘out of the box’ enterprise system solution that is intended to standardise school business processes. It consists of several integrated modules that support curriculum, finance, communication and administration services. It includes learner management functionality, online forms, parent portal and business analytics to help decision-making processes in schools and preschools. It will also provide standard financial information to support consolidated financial reporting.<sup>26</sup>

**Figure 6.1: EMS modules**



It is intended that most current school business processes will be altered to meet the ‘out of the box’ EMS requirements. The use of EMS functionalities will depend on the type of site and its needs.

EMS will be hosted on Civica’s private cloud environment under a software as a service<sup>27</sup> model. DfE advised that EMS will be accessed through a web browser and is proposed to be more flexible, reliable and student focused. It is planned to capture all the relevant information of a student’s journey through the public education system in a single record with tools to communicate and measure educational progress.

<sup>25</sup> The budget and expenditure figures were provided by DfE and are unaudited.

<sup>26</sup> A separate project has been initiated to procure and implement a solution to perform this consolidation of financial reporting.

<sup>27</sup> Software as a service is a software distribution model in which Civica will host the EMS application and make it available to customers (primarily pre-schools, primary schools and high schools) over the Internet.

## 6.2 What we reviewed

---

The purpose of our high-level review was to obtain an update on the EMS Project's current implementation status, budget and expenditure to date, aspects of key control issues and risks impacting the project.

We did not perform detailed controls testing or evaluate system usability.

## 6.3 Project implementation approach and status

---

EMS was originally expected to be fully rolled out to all sites by mid-2020. This involves over 900 sites, including:

- preschools/children's centres
- primary schools
- secondary schools
- area schools (combined primary and secondary)
- special needs schools
- Aboriginal schools.

The EMS Project has developed a governance structure to oversee its delivery. The EMS Project Board consists of several DfE senior executives representing various areas of the business.

Delays were experienced in the early stages of the EMS Project, including the time to submit the business case for initial SA Government approval and finalise the procurement process. As a result, the original implementation time frame will not be achieved. The full rollout is now scheduled to commence in school term 2, 2020 (end of April 2020 to early-July 2020), with completion at the end of 2023.

Despite these delays, the EMS Project has been able to recover some time by conducting a pilot phase to test 'out of the box' functionalities, prior to any level of customisation of the core system modules. This pilot phase has been completed, with EMS rolled out to two preschools, four primary schools and four secondary schools in term 1 and term 2 of 2019. The pilot phase tested 'out of the box' functionalities of the core modules (highlighted in blue in figure 6.1), except for program management<sup>28</sup> which still needs development.

The 10 sites that participated in the pilot phase were:

- Oaklands Estate Preschool – 59 students (14 February 2019)
- Mitchell Park Preschool – 41 students (22 February 2019)
- North Ingle Primary School – 161 students (19 March 2019)
- Ingle Farm Primary School – 434 students (21 March 2019)
- Para Hills High School – 496 students (25 March 2019)

---

<sup>28</sup> Program management would be used for developing specific education programs, such as music.

- Paralowie High School – 1459 students (2 April 2019)
- Seaview High School – 860 students (1 May 2019)
- Port Lincoln High School – 720 students (3 May 2019)
- Para Hills Primary School – 267 students (14 May 2019)
- Gilles Street Primary School – 397 students (16 May 2019).

During the pilot phase, sites continued to use their existing systems in parallel with EMS. Dual data entry was required and the existing systems were considered as the single source of truth.

The pilot provided several key learnings, which the EMS Project has taken into consideration in developing the broader implementation plan for the remainder of the project, including the full rollout strategy.

## 6.4 Project budget and expenditure

---

The total project budget for implementation is \$130 million. This includes the 10-year contract with Civica for system implementation and support services of \$76 million. The remainder of the budget relates to procurement, DfE implementation costs and future enhancements. Under the contract arrangement, DfE is purchasing the right to use the software with a 10-year right of renewal at a further cost of \$82 million. DfE will maintain ownership of the data, while Civica will retain ownership rights for the software licences.

At the time of our review, the EMS Project was on budget. So far, the EMS core modules have been rolled out to all 10 pilot sites and the project has used around 11% of the total budget.

In October 2018 the overall budget for the EMS Project was reduced by approximately \$4.3 million. This included removing some items related to other specific departmental projects that were incorrectly recorded against the EMS budget.

**Figure 6.2: EMS Project budget and expenditure as at the end of August 2019<sup>29</sup>**

	Approved budget Sept 2018 \$'000	Overall project expenditure to date \$'000	Remaining budget \$'000
EMS procurement	7 833	7 833	0
Civica pilot	1 126	1 126	0
Civica licence, hosting and support	67 251	2	67 249
Civica implementation	8 063	832	7 231
Future changes/new products	5 000	0	5 000
DfE implementation	40 860	5 006	35 854
<b>Total</b>	<b>130 133</b>	<b>14 799</b>	<b>115 334</b>

<sup>29</sup> These figures were provided by DfE and are unaudited.

## 6.5 Challenges with legacy systems

---

DfE advised that its legacy<sup>30</sup> systems have limited functionality and rely on outdated technology, making them difficult to upgrade and integrate with other more modern systems. EYS does not have financial capabilities and each site using EDSAS has a separate version of the system with varied customisations. Inefficient manual processes are required to consolidate data to provide State-wide visibility of finance, administration and educational performance.

The current systems' inability to effectively manage student and staff data from a State-wide perspective makes it difficult for DfE to participate in future national initiatives. In addition, DfE advised that these systems cannot automatically consolidate site actual results to conduct financial analysis against budget throughout the financial year and at year end to produce a consolidated set of financial accounts. We note that DfE conducts several manual processes to consolidate its accounts for financial reporting purposes as at 30 June each year.

The current cost to maintain and support EDSAS and EYS is around \$7.6 million annually. As a contingency, DfE has extended the EDSAS vendor contract for three years, to the end of June 2022, with the option to extend for a further two years.

Other system limitations include the inability to integrate with other information sources, including Vocational Education and Training (VET) and The National Assessment Program – Literacy and Numeracy (NAPLAN). This impacts DfE's ability to make informed department-wide decisions.

## 6.6 Project benefits

---

EMS is intended to provide the functionality to efficiently and effectively manage education, administration and finance.

DfE advised that some key benefits include:

- improved efficiencies for student enrolment
- improved reporting on assessment, achievement and attendance
- finance efficiencies from improved processes for financial reporting
- increased integration with other key business systems and other external data sources
- reduced effort and cost in supporting site infrastructure.

These benefits are expected to help inform DfE of financial and educational decisions from a State-wide perspective.

---

<sup>30</sup> An outdated computer system that may not be able to be upgraded and requires replacing. Vendor support may be limited or not exist.

We note that EMS will provide standard financial information to support the consolidation of site financial reporting. The consolidation of this data with DfE's corporate general ledger is not within the EMS Project's scope. A separate project has been initiated to procure and implement a solution to consolidate DfE corporate, school and preschool accounts for financial and management reporting purposes. The procurement process is expected to start in 2019-20.

DfE advised in the EMS business case that it was not possible to be definitive about the benefits that can be delivered, but that it was essential to justify the investment proposed. It estimated tangible benefits to be between \$6.9 million and \$11.3 million p.a. These tangible benefits are savings on hardware support and maintenance and software licensing costs for school administration servers.

## 6.7 Current project challenges

---

The EMS Project advised that as of September 2019 its risk register contained 39 active risks, of which 23 were considered high and 16 moderate.<sup>31</sup> After considering preventative and mitigating controls, the risk profile was reduced, with controlled risk ratings counted as four high and 19 moderate.

Despite progress occurring as part of the pilot phase, the EMS Project still faces several challenges. These challenges include the following.

### 6.7.1 Managing several key project interdependencies

Several interdependent projects are underway that are required to successfully deliver the intended EMS Project benefits. The EMS Project has identified interdependencies as a high risk and they include the following.

#### Integrated data platform

EMS needs to be integrated with other key business systems used by corporate, schools and preschools to perform certain business functions. These systems include the centralised EDSAS data store, the Valeo payroll and human resources system and EYS.<sup>32</sup>

Civica is required to perform additional integration works between EMS and other extended modules, including learning management and forms management products. Once completed, DfE intends to test this integration.

---

<sup>31</sup> This count does not include low rated risks.

<sup>32</sup> The data store and EYS currently feed external systems and data repositories and will be maintained to provide continuity for system-wide integration and reporting. DfE intends to decommission these systems once EMS is rolled out to all sites.



## Central data warehouse

DfE intends to procure a central data warehouse for financial and non-financial consolidation, data analysis and analytical reporting for decision-making purposes. It is intended to be a central repository of integrated data from the DfE's disparate data sources.

A business case for the procurement was approved and includes business requirements and market research. A further project brief is awaiting approval and includes the budget for the implementation approach. A key outcome will be to decommission several legacy reporting systems. DfE noted that data cleansing activities might be required before using the central data warehouse for reporting.

## Identifying, assessing and cleansing financial data

DfE intends to allocate a minimum of 12 weeks to help each site to identify, assess and cleanse its financial data to align with its scheduled implementation date. This notably includes:

- confirmation and reconciliation of the site's cash balances, including identifying any unrepresented deposits and cheques
- assessing and cleansing aged debtor and aged payable balances
- identifying and cleansing depreciation of all non-current assets
- reconciling the site's GST liability
- assessing and reconciling all Governing Council employee entitlements
- identifying, assessing and cleansing all other liabilities and any reserve balances.

DfE considers these activities as high risk, as the opening balances as at the date of implementation are imperative to the completeness and accuracy of schools'/preschools' financial statements.

In addition, as part of the EMS implementation, DfE intends to implement a State-wide single chart of accounts for sites. This was implemented as part of the pilot. Within the 12 weeks mentioned above, DfE, in collaboration with individual sites, will transition each site's current chart of accounts into this new chart of accounts format.

DfE has also commissioned a review into certain finance policies and procedures, which has the potential to increase project dependencies. These include, the treatment of tax and fringe benefits tax, payroll for Governing Council employees, accounts receivable, accounts payable and other financial services.

## Financial management business processes

DfE is working through some other finance activities to support the EMS rollout, to help ensure the EMS financial management module effectively replaces schools' existing finance systems and processes. This includes reviewing and updating the existing business processes to reflect EMS requirements and processes for the single school supplier vendor master list.

We also note that schools are using accrual accounting within EDSAS. Most preschools, however, do not use EDSAS and are using cash accounting. DfE is currently reviewing options to help preschools and small schools transition their accounting processes.

The EMS Project advised it will continue to monitor these interdependencies through ongoing meetings and using implemented tracking tools.

Some pilot site feedback on their early challenges using the EMS finance module are discussed in section 6.7.3.

### 6.7.2 Challenges in testing outstanding functional and non-functional requirements

As part of the procurement process, DfE identified 1474 functional business requirements and 179 non-functional requirements. Civica responded advising that EMS met most requirements, but some were either non-compliant or only partially compliant.

The EMS Project has taken a risk-based approach and identified 820 base functionalities for testing. It intends to test the remaining functionalities prior to the full site rollout, scheduled to commence in school term 2, 2020 (end of April 2020 to early-July 2020).

Despite the testing approach, it has not yet formally risk assessed its complete list of functional and non-functional business requirements.

There is a risk that there may not be enough time to conduct all required testing in conjunction with other planning activities before the full rollout. This risk will require close monitoring.

**Figure 6.3: Status of RFP functional and non-functional requirements**

Requirement status	Functional requirements <sup>33</sup>	Non-functional requirements <sup>34</sup>
Fully compliant	1 367	114
Partially compliant	71	65
Non-compliant	36	-
Totals	1 474	179

### 6.7.3 Feedback on early challenges experienced by the pilot sites

As part of our review we asked a sample of pilot sites how they were progressing with using EMS.

We noted that generally sites were confident that EMS will improve workflows and save time in the long term. Some notable positive feedback from sites included:

<sup>33</sup> Functional requirements describe technical functionalities of the system.

<sup>34</sup> Non-functional requirements define system qualities or attributes, such as security, usability, reliability and performance.

- additional resources and funding were provided by the EMS Project to support pilot sites. This includes assistance from subject matter experts and funding for sites that required additional support hours
- when a major data entry and release to the general ledger is performed in EDSAS, a backup is taken. Users perform this backup approximately 5-10 times a day. This activity will not be required in EMS
- in EDSAS, manual calculation of the GST component is required for every applicable transaction. When generating invoices in EMS the system will automatically calculate the GST component based on the total item value
- generally, issues identified throughout the pilot phase are being appropriately addressed.

However, sites did express some concerns, which included:

- the adjustment to new workflows and system functionalities is bigger and more difficult than expected
- some system functionalities that were advised in training have not worked properly
- despite the additional resources provided by the EMS Project, dual data entry during the pilot phase has increased staff workloads and added a large amount of pressure on finance staff. The main time-consuming aspect is ensuring the data matches in both systems
- the EMS Project has done well in providing the support it has. However, it does not appear to have enough resources available to support all sites
- EMS is not as user friendly as expected. It takes longer to perform administration and finance tasks, mostly related to longer processing of payments. For example, there are extra clicks required to look up account codes and then input them into an invoice form.

Some specific functional concerns raised by sites included:

- It is not very user friendly for making error adjustments. An example is that, if a user submits an incorrect general ledger account entry on an invoice it cannot be adjusted. Entering a negative/cancellation entry is a lengthy process. Some aspects take a long time to get to work as expected
- difficulties were experienced with the single chart of accounts, mostly due to missing school suppliers. Users are required to submit a request to DfE corporate to create a new supplier in EMS
- difficulties were experienced balancing monthly accounts receivable
- not all types of assets appear in EMS. When purchasing a new asset, users cannot add the asset and therefore an expense line is created in EMS. This is not testing the complete and correct workflow.

Pilot users had the following suggestions for the EMS Project going forward:

- The EMS Project needs to ensure there is good consultation with sites as a whole and all potential issues are foreseen and already addressed before sites go live.

- Lead times should be long enough to ensure all school account codes and suppliers are appropriately configured in EMS.
- All staff need to be fully accustomed to EMS before go-live. It will take users some time to get used to it.
- The EMS Project is being conducted in line with DfE policies, however schools may not always comply with them. There are some change management factors involved in ensuring all schools conform to new processes.
- The EMS Project may be underestimating the extent of resources needed to support the number of staff that will need assistance when sites go live.

The EMS Project advised that it is capturing site feedback in its requirements register and analysing it to address any missing functionality or capability gaps. It should be noted that we did not verify the accuracy of the feedback that sites provided.

## 6.8 Program assurance

---

The EMS Project engaged KPMG in early January 2017 to provide independent project assurance. This includes providing advice to the EMS Project Board and tracking the project's progress. KPMG has delivered several reports providing observations and recommendations which the EMS Project has responded to.

A quality management strategy was developed to drive quality practices across the EMS Project. In addition, the EMS Project was subject to an internal audit review in October 2018.

From a security perspective, DfE advised that in early 2019, independent penetration testing was conducted over the EMS product suite. The EMS Project advised that an action plan to remediate identified issues has been agreed with Civica and its partners.

The EMS Project intends to conduct further penetration testing in around February 2020. This will be when the EMS solution is finalised and prior to its rollout to all sites.

## 6.9 Summary of control findings

---

As previously mentioned, our review scope did not involve performing detailed controls testing of EMS or the EMS Project. We did, however, identify some control findings that required management attention. The main findings included:

- no formal benefits realisation plan
- no formal transition out and contract management planning
- potential weaknesses in migration testing of financial data.

DfE responded positively to our findings and recommendations, with most to be actioned by December 2019.

## 7 Electronic Medical Record project

Since early 2012 the Department for Health and Wellbeing (SA Health) has been implementing its Enterprise Patient Administration System (EPAS). It is a key platform for achieving SA Health's single State-wide electronic health record for each patient. It also supported the previous government's Transforming Health initiatives.

Other key drivers for implementing EPAS were:

- ensuring an integrated electronic system was implemented at the Royal Adelaide Hospital (RAH) to manage patients and their care
- supporting State policy and strategic agendas
- addressing inherent risks associated with maintaining legacy patient administration and billing systems.

Due to ongoing challenges and a change in government in March 2018, the implementation of EPAS was paused to conduct an independent expert review<sup>35</sup> to inform decisions moving forward. Activations were halted at the Mount Gambier and Districts Health Service (MGDHS) and the Flinders Medical Centre (FMC).

The independent experts found that continuing with EPAS 'as is' was not acceptable. Despite this, they acknowledged the improved patient outcomes and efficiency benefits to be gained from electronic medical records and made several recommendations for improvement to gain user acceptance. The SA Government accepted, or accepted in principle, all recommendations made in the review.

One outcome of the review was rebranding EPAS. The EPAS Program is now known as the Electronic Medical Record (EMR) Project. In principle, SA Health intends to continue using the same base system and attempt to reconfigure its functionality to better meet user expectations.

Since the review, the EMR Project has been progressing activations at two exemplar sites (the RAH and MGDHS). Implementation at MGDHS was completed in October 2019, while the first two of four stages of the activation have been implemented at the RAH. In approximately March 2020, SA Health intends to recommend to the SA Government whether to continue implementing the system at other in-scope sites or consider other options. This includes returning to market to select a new system for the State.

### What we found

The EMR Project has made some significant changes to its implementation approach and governance in response to the outcomes of the independent review, which have been applied to the exemplar sites. There is now a strong focus on gaining user acceptance at the exemplar sites before rolling out EMR to other in-scope sites.

---

<sup>35</sup> EPAS Independent Review: Final Report, December 2018, [www.sahealth.sa.gov.au](http://www.sahealth.sa.gov.au), viewed 15 October 2019.

The approved project budget remains at \$421 million as established in the 2011-12 mid-year budget review. The EMR Project intends to address as many of the independent review priority recommendations as can be achieved within the remaining budget of \$45 million (as at August 2019). It also intends to implement the remaining clinical functionalities at the RAH. It is anticipated that not all priority independent review recommendations can be implemented at the exemplar sites within the allocated time frame and budget.

The key challenge for SA Health is to make an informed decision on whether the revised solution has been a success. This will depend on the extent of improvements made in the revised solution. It is also important to provide users (including clinical staff) with enough time to use and accept the system in their hospital environment.

SA Health plans to develop a new business case and seek SA Government approval before continuing with any further rollout of EMR beyond the exemplar sites. This will include a revised approach, estimated costs and benefits that the EMR Project will be monitored against. Another business case is being developed for a solution for regional sites.

## 7.1 Introduction

---

We last reported on the status of the EPAS implementation in June 2016.<sup>36</sup> In November 2016 we conducted operational testing of EPAS covering several system usability aspects at selected local health network (LHN) sites. This also included following up previously raised identity access management issues.<sup>37</sup>

At the time of this Report, EPAS (now EMR and referred to in this Report as 'the system') was implemented at the following sites:

- Noarlunga Hospital and Noarlunga GP Plus Super Clinic (August 2013)
- Aldinga, Morphett Vale and Seaford GP Plus Health Care Centres (November 2013)
- SA Ambulance Service Inc metropolitan headquarters (November 2013)
- Daw House at the Repatriation General Hospital (December 2013)
- Port Augusta Hospital (December 2013)
- Repatriation General Hospital (April 2014)
- The Queen Elizabeth Hospital (June 2016)
- Marion GP Plus (April 2017)
- RAH (September 2017)
- SALHN Service Moves and Flinders Medical Centre new building (October 2017)
- Hampstead Rehabilitation Centre (March 2018)
- MGDHS (exemplar site – stage 1 in September 2019 and stage 2 in October 2019).

---

<sup>36</sup> Supplementary Report of the Auditor-General for the year ended 30 June 2015 *Enterprise Patient Administration System: June 2016*.

<sup>37</sup> Supplementary Report of the Auditor-General for the year ended 30 June 2016 *Health information technology systems: November 2016*.

The September 2017 implementation at the RAH was with reduced functionality and was limited to patient administration and minimal clinical functionality in the emergency department. Stages 1 and 2 of the exemplar site activities were implemented in June and July 2019 respectively, leaving two stages still to be completed.

When the then EPAS Program was paused to conduct an independent review, activations were halted at MGDHS and FMC. No plans were made for implementations at the Lyell McEwin Hospital, Modbury Hospital, Women's and Children's Hospital, Glenside, Modbury and Elizabeth GP Plus.

Although not in the project scope, system implementation delays made it difficult for SA Health to consider appropriate solutions to replace the Chiron country hospital patient administration system beyond the Port Augusta and Mount Gambier hospitals.

An independent expert panel (the Review Panel) was appointed to conduct the review to determine if the system is adequately meeting user expectations. The SA Government accepted, or accepted in principle, all the review recommendations. We sought confirmation from SA Health of their activities to progress the project and address the concerns raised in this review.

## 7.2 What we reviewed

---

The purpose of our high-level review was to get an update on the EMR Project's current implementation status, including the outcomes of the independent review, the SA Government's response and SA Health's current activities. We also sought an update on the project's budget and expenditure to date, expected benefits and key challenges. We did not perform detailed control testing or evaluate system usability.

## 7.3 Independent review outcomes and recommendations

---

In December 2018, the new SA Government completed its independent review of the system. The review noted that 78% of original funds had been spent, with 28% of the original project scope<sup>38</sup> implemented. It estimated the total cost to complete the implementation would be \$695 million, which is \$273 million over the approved budget of \$421 million.

The purpose of the independent review was to determine whether issues raised by clinicians about the system could be adequately addressed to meet user expectations.

The review raised several issues related to the software solution, its configuration and the implementation and governance of the then EPAS Program. The Review Panel concluded that these elements have contributed to the system not meeting user expectations.

---

<sup>38</sup> The original scope refers to the extent of public hospital occupied bed days where the system has been implemented.

The review provided some statistics on incidents directly linked to the system after go-live:

- RAH: 29 incidents
- The Queen Elizabeth Hospital: 58 incidents
- Repatriation General Hospital: 36 incidents
- Noarlunga Hospital: 15 incidents
- Port Augusta Hospital: 11 incidents.

It also noted that most system related incidents did not result in harm to patients and can be described as 'near misses'. The incidents related to incomplete information entered by users, workflows not being followed and technology limitations. As such, they cannot be solely attributed to the system.

While the review noted that continuing with the system 'as is' is not acceptable, it did acknowledge the improved patient outcomes and efficiency benefits to be gained from using an electronic medical record system. Sites advised the Review Panel that they did not want to return to paper records, explaining the advantages of legible patient clinical notes being stored in a single location that can be accessed simultaneously.

The review also noted the following:

- The assumption that the system would meet 60% of the State's needs, made in the business case, was incorrect. In addition, the implementation timing was ambitious given it was not configured for the Australian healthcare environment. Configuration was centrally driven, and clinical engagement was not sustained after the early stages of the design and build process. The current software version is out of date and workflows need to be standardised across sites.
- The implementation was conducted by SA Health without help from the vendor or any other external party with expertise and experience in workflow design and the complexities associated with implementing and adopting an electronic medical record system.
- Weaknesses were noted in the governance model, particularly that accountability for outcomes was poorly understood and managed. LHNs do not have any accountability for implementing at their hospitals and clinicians have not been empowered as key decision-makers and therefore lack ownership.
- Although improvements have been made to the site implementation model, including the training approach, not having the sustained presence of system expertise post go-live has resulted in limited investment and incentive for LHNs to identify efficiency, clinical and quality benefits.

Based on the substantial human and financial investment, the Review Panel recommended that the solution be optimised, with major changes made to its operations including:

- developing a digital strategy for SA Health that includes a single integrated State-wide electronic medical record system, with standardised workflows and interoperability with other key systems



- implementing significant governance reforms, in particular passing responsibility for implementing and configuring the system to LHNs and clinicians
- improving the solution and the implementation approach, including post go-live support
- applying the proposed changes to two exemplar sites, with future decisions contingent on user acceptance at these sites
- replacing the billing module as a priority, as it is currently not suited to Australian billing conditions.

It also recommended that a Review Implementation Taskforce be established for an initial 12-month period to ensure each recommendation was progressed.

We note that many of the concerns raised in this review were raised in our previous Reports to Parliament. This includes the following implementation and control risks and audit concerns:<sup>39</sup>

- instances of deficiencies in governance communication and decision-making
- the rollout approach and budget estimates to complete the remaining in-scope sites are unclear
- continual system and billing issues and defects
- potential delays in some patient administration and care related tasks
- interface challenges with other SA Health systems impacting hospital workflows
- the project experiencing issues in supporting business as usual at existing sites
- problems with periphery devices accessing the system.

## 7.4 The SA Government's response

---

The SA Government accepted, or accepted in principle, all recommendations made in the independent review.

It advised that rebranding the system and deploying it to two exemplar sites would be the immediate focus. The exemplar sites will receive the most updated version of the software (version 17.3). Other key actions advised were:

- establishing a new governance structure with a revised implementation approach
- re-engaging the vendor in the implementation, including involving the vendor in optimising the system and the governance process

---

<sup>39</sup> Supplementary Report of the Auditor-General for the year ended 30 June 2014 *Health ICT systems and the Camden Park distribution centre: June 2015*, Supplementary Report of the Auditor-General for the year ended 30 June 2015 *Enterprise Patient Administration System: June 2016* and Supplementary Report of the Auditor-General for the year ended 30 June 2016 *Health information technology systems: November 2016*.

- local clinical leadership of the implementation and business change during the reconfiguration and deployment
- assessing several priority enhancements proposed in the independent review. SA Health will need to consider its ability to address these matters simultaneously with existing health system priorities and associated reform programs.

The SA Government plans to complete system implementations at the exemplar sites within the existing project budget. A new business case will be developed for future activities and will be subject to SA Government approval. It will include a revised approach, estimated costs and benefits that the project will be monitored against.

## 7.5 Changes to the implementation approach

---

While system activations were paused, the rebranded EMR Project focused on upgrading the IT support environment, enhancing system functionalities, reporting and business as usual support.

The independent review was completed in December 2018. The EMR Project then focused on changing the implementation approach for the two exemplar sites, RAH and MGDHS. The change in approach includes:

- a phased activation
- increased onsite engagement and support from the EMR Project team and the vendor, Allscripts
- recruiting and upskilling onsite support staff
- updating the training approach, targeting specific functionality and staff groups
- establishing ongoing staff education processes and access to training facilities
- implementing fit-for-purpose devices, defined by clinical users
- standardising workflows across SA Health
- establishing new clinical advisory groups
- increasing LHN accountability by leading and controlling site activations, and defining clinical and administrative governance and leadership arrangements with support provided by the EMR Project
- improving EMR Project governance (discussed further in section 7.6).

The RAH was chosen due to the ongoing clinical and corporate risks associated with continuing with a hybrid model of paper and electronic patient records.

Overseen by the LHNs, clinicians are responsible for the system configuration at the two exemplar sites. The EMR Project team has transferred into these sites to work with them. Super users have been allocated onsite and dedicated EMR skills centres have been established.

EMR activation at MGDHS was completed in October 2019 and the final stage of the RAH is expected to be completed in the first quarter of 2020.

This revised approach will determine whether the system can be configured and implemented to meet user expectations. A decision on whether to continue to implement the revised solution at the remaining in-scope sites is expected to be made in approximately March 2020. It will be based on user acceptance at the exemplar sites and a supporting business case. SA Health agreed to the Review Panel's recommendation that, if reasonable user expectations are not met, it should return to market to select a new system for the State.

## 7.6 Changes to the governance arrangements

---

The independent review highlighted major concerns with the then EPAS Program's governance model, citing a lack of accountability, authority, transparency and focus on outcomes. LHNs have had little accountability for clinical and non-clinical benefits associated with the system.

To address this, project governance arrangements were changed in March 2019. The EMR Project Board is now independently chaired. LHN Chief Executives have returned to the Board and have been joined by other senior medical representatives. The EMR Project advised that it has increased its engagement with Allscripts to leverage its configuration and implementation experience. This has involved including the vendor in the governance process.

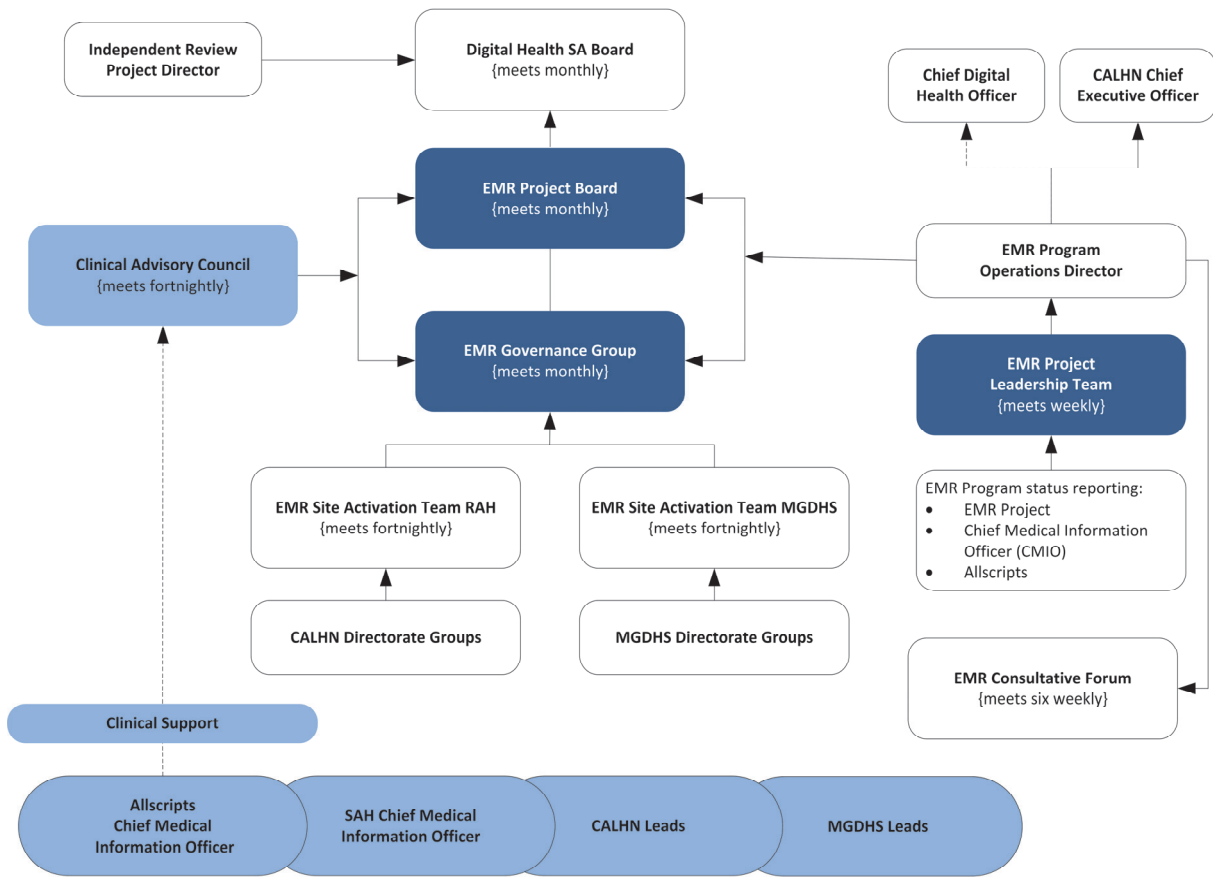
A newly created EMR Governance Group now reports to the EMR Project Board to provide advice and recommendations on significant matters. It also provides direction and leadership to the EMR Project and is accountable for all work streams and ensuring they are aligned with approved project scope and functions.

Newly implemented clinical specialty groups now focus on standardising workflows and the system configuration in their clinical area. These groups include medical, surgical, obstetrics and gynaecology, paediatrics, mental health, outpatients, pharmacy, radiology, pathology, nursing, allied health, patient administration and restorative and extended care. They report to the reconstructed Clinical Advisory Council, which first convened in June 2019 and includes the chairs of each clinical specialty group.

In addition, eHealth Systems is now known as Digital Health SA, with the EMR Project now reporting to a Digital Health Board chaired by the Chief Executive of SA Health through the Central Adelaide Local Health Network Incorporated (CALHN).

SA Health has also established the role of an EMR Independent Review Project Director to oversee the progression recommendations made as part of the review. Progress is reported monthly to the EMR Project Board.

**Figure 7.1: EMR Project governance model**



Source: EMR Project, October 2019.

The EMR Project Board continues to monitor the progress of the recommendations made in the independent review.

## 7.7 System functionality and impacts on hospitals

The independent review noted some efficiency gains using an electronic medical record system. They include reducing the time it takes to find and retrieve patient records, timely outpatient letters and discharge summaries and improved visibility of patient workflows. However, these efficiencies appeared to be offset by other slower system workflows. The independent review assessed whether the functionality of each system module was fit for purpose.

We note that while the independent review was being conducted, the then EPAS Program continued to work on several system shortcomings that were raised in the review. The EMR Project advised that several improvements were made, notably implementing a software upgrade and enhancing several aspects of system functionality (both clinical and patient administration), integration and reporting. This included updating a patient record report in response to the Coroner and Freedom of Information requests and addressing some integration shortcomings with other SA Health systems.

The last software version upgrade (to version 14.3) occurred in the first half of 2015.<sup>40</sup> The system was upgraded (to version 17.3) in February 2019, which planned to resolve several software defects and provide new functionalities and enhancements, including:

- a workflow management tool
- a more intuitive graphical user interface when patient notes are open
- the ability to drag and drop problems and linked interventions
- a patient timeline which provides a visual of patient visit history
- a tool to analyse patient conditions such as results, vital signs, problems and observations and provide suggested tasks, workflows and actions
- additional tools for care providers to manage patient concerns
- a tool to record and update patient implant information
- mobile device access to perform clinical tasks
- wounds assessment, treatment and care planning for inpatients and outpatients
- one continuous record of patient surgical care.

It took many months for Allscripts, with support from the EMR Project, to resolve a significant number of product defects that impacted the release of version 17.3. Functional improvements will be progressively enabled, and more regular upgrades are planned in the future.

Not all of the above functionalities have been rolled out to system users yet, and some are outside the scope of the EMR Project. For example, patient surgical care replacing the existing information management system used by operating rooms and mobile device functionality, which is currently not fit-for-purpose for SA Health.

## 7.8 Update on current project activities

---

At the time of this Report, the EMR Project was progressing activation and support activities for the exemplar sites (MGDHS and the RAH). The EMR Project advised that Allscripts has been involved in developing activation timelines for sites.

MGDHS was activated in October 2019. The EMR Project is currently providing activation support, including continued clinical engagement, staff training, site communications and report reconfiguration. It is also configuring and testing integration with other systems and biomedical engineering devices.

The RAH has been operating the system with full patient administration and partial clinical functionality since it opened in September 2017. Exemplar site activation activities are continuing and have been grouped into four stages:

---

<sup>40</sup> This version was to become unsupported in December 2018. This date was extended to February 2019 when the system was upgraded to version 17.3.

- Stage 1: documents and flowsheets for the Cancer Day Centre (including radiology and oncology) and emergency department (implemented June 2019).
- Stage 2: documents and flowsheets for outpatients, discharge medication ordering for stage 1 and 2 locations (implemented late-July 2019).
- Stage 3: documents and flowsheets for inpatients (planned for late-November 2019).
- Stage 4: All remaining clinical functionalities, including medication management and ordering, clinical orders and worklist manager for inpatient, outpatient and emergency department and discharge summaries (planned for March 2020).

The EMR Project intends to implement concurrently the remaining clinical functionalities and action as many independent review recommendations as possible. The timing and approach adopted for these changes is being defined by the RAH clinicians and executives involved.

Activation works continue for Stage 3 and the scope and timelines for Stage 4 are being established. Stage 3 activation includes analysis of workflow requirements, site configuration and staff training. Super users have been allocated and onsite training rooms and a skills centre established.

The EMR Project also continues to conduct enhancement and optimisation planning. This includes:

- engaging with SA Pharmacy to start to develop the Closed Loop Medication Management business case
- Sunrise Records Management used for document scanning being replaced by an Allscripts product called BOSSnet. Sunrise Records Management is considered end of life, is incompatible with Windows 10 and experiences issues indexing scanned documents
- implementing a purpose-built reporting and analytics module focused on clinical decision support. The EMR Project is currently assessing suitable solutions
- establishing a new process to assess workflows and deliver system enhancements.

Refer to figure 7.5 for a summary of independent review priority configurations for development and whether SA Health plans to implement them at the exemplar sites.

SA Health is also working through several other functional challenges. These include:

- replacing the billing module with one that is more suited to the Australian billing environment. Approval has been provided to develop a business case, however at the time of this Report there was no indicative time frame for implementation. While this occurs, the EMR Project is continuing to address outstanding system billing issues
- submitting a tender to procure a single State-wide Enterprise Chemotherapy Prescribing System, because the system's chemotherapy functionality is not currently being used
- integration with the Anaesthesia Information Management System at the RAH. However, funding for this work has not yet been allocated

- liaising with Allscripts on tasklist functionality, which has not been delivered to The Queen Elizabeth Hospital. It was originally planned to be implemented two weeks after go-live, in late-June 2016. The functionality is now available in the latest system version (version 17.3), but it needs to be tested for site deployment.

SA Health intends to develop a new business case before completing implementation at the exemplar sites, which will be subject to SA Government approval. It will include a revised approach, estimated costs and benefits that the project will be monitored against.

## 7.9 Project budget and expenditure

The SA Government originally approved \$408 million to fund the then EPAS Program in December 2011. The budget was increased to \$421 million in the 2011-12 mid-year budget review. SA Health attributed the increase to an accounting error in which inflationary indexation was omitted from the original budget.

In September 2017, the then EPAS Program advised that it would cost \$471.1 million to complete the project and by September 2018, \$329.5 million had been spent, equating to 78% of the approved budget with 28% of the original scope implemented.

The Review Panel estimated that the total cost to complete the project was now \$695 million, \$273 million more than the approved budget. It advised that most costs relate to the project team and other central SA Health expenses, including system implementation delays and extra costs not included in the original business case.

The approved project budget remains at \$421 million. At the time of this Report, no additional funds had been requested to complete the project.

**Figure 7.2: Project budget and expenditure as at August 2019<sup>41</sup>**

	Original approved budget (December 2011) \$'000	Revised approved budget (2011-12 mid-year budget review) \$'000	Expenditure to date (August 2019) \$'000	Total planned expenditure \$'000	Remaining budget \$'000
Capital and operating expenditure	363 100	372 292	376 900 <sup>42</sup>	44 554	0
Contingency	44 800	49 162	-	-	-
Total budget	407 900	421 454	376 900	44 554	-

While system activations were paused pending the outcomes of the independent review, the then EPAS Program focused on the environment upgrade and enhancements to system

<sup>41</sup> These figures were provided by SA Health and are unaudited.

<sup>42</sup> All remaining funding held by the Department of Treasury and Finance (including contingency) was provided to progress recommendations from the independent review, including implementation at the exemplar sites.

functionality, reporting and business as usual support. These activities were funded from the existing project budget.

SA Health advised us that the long-term impact of accepting all independent review recommendations will not be known until it has completed implementation at the exemplar sites and conducted detailed planning. The current vendor contract with Allscripts for maintenance, licencing and support, which was entered into after the SA Government approved the business case in December 2011, is due to expire in March 2020.

While the focus has shifted to improving the system to meet user expectations, the EMR Project Board noted that not all exemplar site independent review recommendations can be funded and delivered in 2019.

SA Health advised that the funding allocation for future business as usual support costs beyond the exemplar sites will be defined in the new business case. It will need to track these support costs, as they form part of the total cost of the project. The EMR Project business as usual support team comprises 110 resources at a cost of approximately \$2 million per month.

## 7.10 Project benefits

Anticipated cost benefits have significantly deteriorated from what was originally expected. Figure 7.3 describes the original expected system benefits and reduced costs (over the 10 years from January 2012 to January 2021) compared to revised figures estimated at the end of June 2017.

**Figure 7.3: Project anticipated benefits and cost offsets (10-year period) estimated at the end of June 2017**

Type of benefits and cost offsets	Description	Original expected benefits \$'000	Achieved to date (June 2017) \$'000	Remaining (June 2017) \$'000
Capital	Reflects the reallocation of capital funding already set aside in existing Health budgets	191 254	149 073	42 181
OACIS	Reflects the reduction in staffing resources required to support OACIS	14 611	8 980	5 631
eHealth Systems	Reflects the reduced resourcing required in eHealth Systems and establishing a team to support the system	72 562	20 560	36 922



Type of benefits and cost offsets	Description	Original expected benefits \$'000	Achieved to date (June 2017) \$'000	Remaining (June 2017) \$'000
LHNs	Reflects the reduced resourcing required in LHNs and establishing a team to support the system	60 650	0	33 498
Decommissioning credits	Reflects the decommissioning of existing legacy system no longer required	96 554	4 563	56 306
Benefit/Cost offset total		435 631	183 176	174 539

SA Health has not updated the expected benefits since June 2017, because there were no site activations while the then EPAS Program was paused for the independent review.

In June 2017, SA Health estimated that \$279.2 million in expected benefits and cost offsets would be achieved by January 2021. These benefits rely heavily on the timing of site activations and therefore, due to the continued delays, this amount would now be less.

In developing a new business case, SA Health intends to revisit the expected project benefits. From a user and clinical benefit perspective, a base set of benefits will be established which the EMR Project and LHNs will hold dual responsibility for. Digital Health SA will be responsible for monitoring and reporting on system performance. Benefits realisation will be reported on a quarterly basis.

To address the recommendations of the independent review, LHNs will now be accountable for identifying, realising and measuring the clinical benefits. SA Health has engaged an external specialist to help define key system benefit measures and to develop a dashboard for ongoing reporting.

Another specialist has been engaged to conduct a user satisfaction survey and perform an in-depth analysis of the results. This includes assessing user experience and whether the intended benefits are achieved (eg less medication errors, increased efficiency, reduced length of stay). Digital Health SA will monitor and report on the user experience and system performance.

SA Health intends to compare the same measures with sites that do not have EMR.

## 7.11 Impacts on the use of the Country Health system (Chiron)

---

The independent review noted that SA Health's focus on the system implementation has resulted in limited digital investment elsewhere, including the legacy patient administration system in Country Health, Chiron.

Following a court-ordered mediation session in August 2016, SA Health agreed to pay \$5 million for five years for a perpetual licence to use Chiron at all hospitals it is currently used in from 1 April 2015 to 31 March 2020. From 1 April 2020, SA Health will pay a renewal fee of \$600 000 p.a. in advance for the ongoing use of Chiron. This new agreement does not include vendor support.

While still in operation, Chiron presents several ongoing risks. These include not patching the system to protect against new defects or vulnerabilities. Due to a lack of vendor support since April 2015, system changes have not been implemented, preventing it from being configured to interface with other systems, such as My Health Record, and accommodate desired business workflows.

At the time of this Report, SA Health advised that it had started to develop a business case for a replacement patient administration system in Country Health. SA Health advised it will be developed at the same time as the new EMR business case. Despite this, we consider it will be difficult to make any informed recommendations until outcomes are known from the EMR implementations at the exemplar sites and SA Health has determined whether it will continue to implement EMR at the remaining in-scope sites or consider other options, including returning to market to select a new enterprise system for the State.

## 7.12 Current project challenges

---

### 7.12.1 System configuration and defects

While the EMR Project is focused on implementation at the exemplar sites, with an amended approach, it continues to work through a steady amount of change requests. The independent review highlighted that changes sought are outpacing the rate of resolution. These requests may arise from changes in clinical practices, user requests for improvement or identified system defects.

An update on the current status of system defects is summarised below. As at August 2019, there were 296 outstanding production defects. This includes seven priority one<sup>43</sup> and 148 priority two defects.

---

<sup>43</sup> Priority one defects are defined as having a severe impact on the business and, by definition, result in an immediate and sustained effort by all available EMR Project resources until resolved.

**Figure 7.4: A monthly summary of all system defects from September 2018 to August 2019**

Month – Year	New defects	Resolved defects	End of month total defects
September 2018	38	26	261
October 2018	54	32	280
November 2018	36	37	279
December 2018	33	25	287
January 2019	26	32	281
February 2019	63	29	315
March 2019	43	53	305
April 2019	26	23	308
May 2019	32	29	311
June 2019	21	22	310
July 2019	18	24	304
August 2019	21	29	296

At the end of August 2019, the EMR Project was actively working on the outstanding production defects. It has updated its change process (refer to section 7.12.4), which is now led by the clinical specialty groups, and defects will continue to be progressed leading into the implementation at the exemplar sites.

### 7.12.2 Meeting user expectations

Although most users expressed strong views that they did not want to return to paper records, a significant challenge remains for the electronic system to satisfy user expectations. The extent of workflows that may require varied degrees of redesign makes this an extensive, ongoing task. The fact that the system is highly configurable provides some reassurance that improvements can be made, however standardising configuration and work practices across users and hospitals is also a challenge.

User expectations of the system improvements anticipated at the exemplar sites are likely to be high. If the EMR Project is not intending to implement all independent review recommendations, these user expectations will need to be managed.

At the time of the independent review, users reported physical performance issues, including the extent of time to log in and navigate between screens and modules. Device slowness and session freezing has also been noted, which the independent review attributed to older devices with limited memory and devices running multiple user system sessions. Subsequent performance testing conducted by the EMR Project at activated sites concluded that the system was not responsible for these performance issues.

These ongoing device issues and their associated impacts on the use of the system need to be considered by SA Health when migrating these devices as part of the End User Computing Project (refer to section 5).

The independent review further advised that most workstations on wheels and bedside monitors at hospitals are not fit for purpose. This has been, and continues to be, a challenge as the original business case did not include the extra costs of hardware devices. To address this, SA Health has subsequently procured new devices for the exemplar sites that were defined by clinicians.

We raised some performance related issues previously in the Auditor-General’s Supplementary Report for the year ended 30 June 2016 *Health information technology systems: November 2016*.

### 7.12.3 Implementing priority software configuration and developments at the exemplar sites

The independent review raised several priority configurations for development, which the SA Government accepted in principle but advised that the time frames for delivery needed to be assessed. SA Health advised that priority configuration will be determined by the Clinical Advisory Council. In addition, its preference is to complete the deployment of the remaining clinical functionalities at the RAH in 2019.

SA Health advised that it intends to implement as many exemplar site recommendations as possible. However, not all of them can be funded and delivered in 2019, for example pharmacy integration and replacing the billing module. Implementing all recommendations at the exemplar sites would likely delay the implementation until at least the end of 2020 and require significant budget allocation.

Figure 7.5 summarises the priority configurations and SA Health’s advice on whether they are expected to be implemented as part of the exemplar sites.

**Figure 7.5: Summary of independent review priority configurations expected for implementation at exemplar sites**

Configuration for development	SA Health intends to fully implement at the exemplar sites (by March 2020)
Upgrade the system to version 17.3	Yes
User interface optimisation, including the presentation of information, standardising workflows, simplifying order sets and personalising specialty templates	Partially (aspects of improvement in these areas to be implemented)
Pharmacy integration	No (business case stage)
Meeting the patient record requirements of the SA Coroner, SA Crown Solicitor, SA Police, courts, Freedom of Information requests, and other statutory bodies	Yes

Configuration for development	SA Health intends to fully implement at the exemplar sites (by March 2020)
Implementing the mobile device functionality	No (a pilot project is planned for the final quarter of 2019 with implementation to be determined post exemplar sites)
Clinical reporting and analytics capability	Undetermined (solutions are being assessed)
Replacement of the record scanning solution	Yes (depending on implementation planning study)
Replacement of the billing module	No (approved to develop business case)
Configuring important functionalities, such as paediatrics and obstetrics	Yes (for services required at MGDHS, not required at the RAH)
Integration with Community Based Information Systems (CBIS) for mental health.	Undetermined (vendor analysis underway to determine feasibility)

The intention of the exemplar site implementations is to trial a revised solution and gain user acceptance of a model that contains improved configuration and functionalities. A decision is planned in approximately March 2020 whether to continue implementing to the remaining in-scope sites.

In consultation with the EMR Project, the LHNs have developed success criteria for the exemplar sites. Despite this, if all system related recommendations are not addressed and users are not provided with enough time to use and accept the system in their hospital environment, we believe it will be difficult to make an informed decision on whether the revised solution is a success.

While implementing at the exemplar sites, SA Health also plans to conduct detailed planning for the rollout to the remaining in-scope sites and review the outstanding independent review recommendations.

#### 7.12.4 Clinical ownership of system configuration

Clinician consensus of system configuration changes and their priority has not typically been sought in the past. Under the revised implementation approach, clinicians will take ownership of these aspects. Clinical specialty groups will identify business problems and develop functional specifications, and the EMR Project resources and the system vendor, Allscripts, will be responsible for assessing the viability of system configuration changes.

While we consider this approach to be positive, the practicalities of the new process still present some challenges. The independent review noted that the current change process is unclear and excessively slow. Clinicians will have limited understanding of the underlying

software and the ability to alter the system to meet their desired specifications. Significant consultation will be required with the EMR Project and Allscripts.

This has the potential to impact the timing of the implementation of required clinical changes at the exemplar sites and the overall EMR Project budget.

### 7.12.5 Integration with My Health Record

The Federal Government contributed \$90 million towards the then EPAS Program and in return the system needed to be integrated with My Health Record by the end of 2018. System integration would allow clinicians to access My Health Record and search for a patient's medical history. Enabling this is in Digital Health SA's top 15 priorities, however it is currently focusing on other higher clinical risks, including other system enhancements.

SA Health held discussions with clinicians in December 2018. Concerns were raised about the proposed integration solution and significant enhancements were required. The EMR Project advised that this was a complex piece of work and a thorough assessment has been put on hold until February 2020. A detailed business case with work requirements, costs and time frames is required. In the interim, a hyperlink to My Health Record has been added to the system.

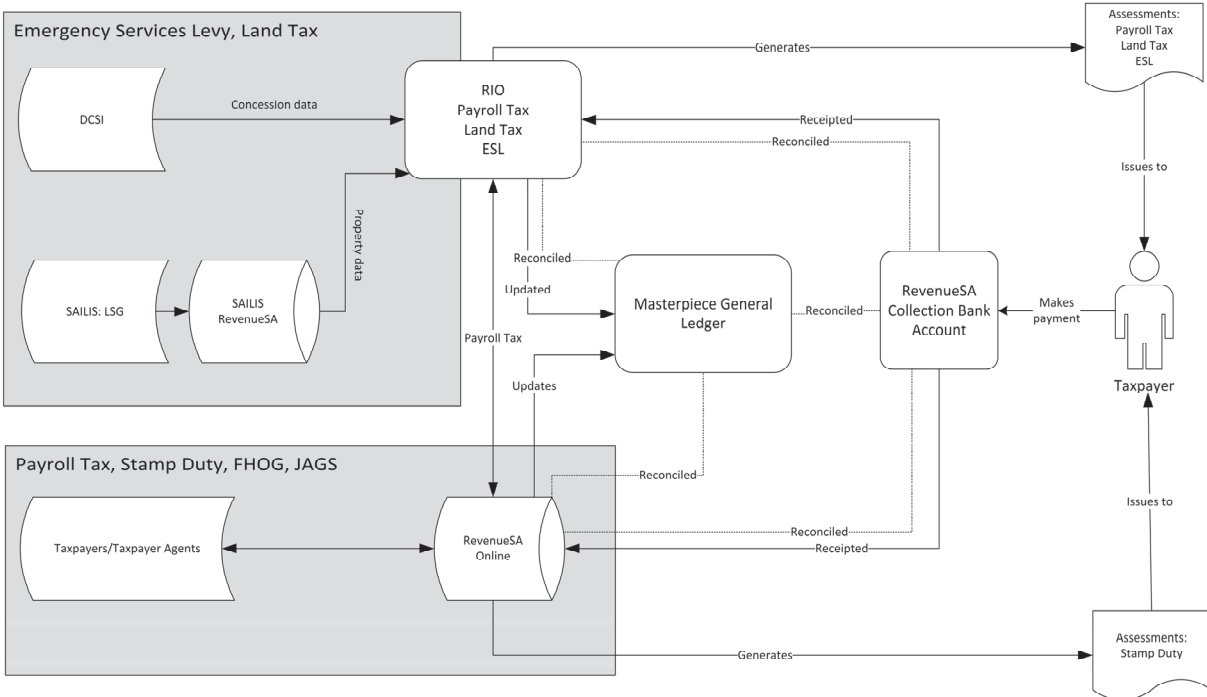
# Appendix – RIO and RSAOL system functionality

RIO processes taxation transactions for payroll and land tax and the fixed property component of the ESL.

RSAOL is a front-end web portal (for external users) for entry and query access to information in processing stamp duty.

Access to the RIO application is through the RSAOL front-end web portal (for external users) or through a RIO application operating system portal for internal office and support staff.

**Figure A.1: Process and generation of revenues for RIO and RSAOL**



Data input process for each tax and levy is as follows:

- **ESL and land tax** – data is provided from the South Australian Integrated Land Information System, managed by Land Services SA. This data confirms the land valuations associated with parcels of land. In addition, concession information is provided by systems within the Department of Human Services.
- **Stamp duty** – generated through two areas covering insurance and property conveyancing. Insurers provide their premium details monthly or annually through the RSAOL web portal to the RSAOL database. Conveyancing is submitted by self-assessment or documentation submitted through the RSAOL web portal for assessment by a RevenueSA tax officer.
- **Grants** – these apply to first homeowner and job accelerator initiatives. Applicants provide details through a Commonwealth system and/or RevenueSA’s web portal for inclusion into RSAOL for review and approval by tax officers.
- **Payroll tax** – employers provide their details of wages progressively during the year into the RSAOL web portal. The portal transfers this payroll information into RIO.

The calculation process attributed to each tax and levy is as follows:

- **ESL** – is a levy on all land to help fund emergency services across South Australia. The ESL is calculated in line with the ownership and value of land on 1 July for the next 12 months.
- **Land tax** – is based on land ownership, site value (not capital value) and land use. It is calculated by applying a progressive rate structure to the total taxable site value of all land owned (by an owner or a group of owners). The tax is calculated as at 30 June of each year to determine the land tax for the forthcoming financial year.

By applying the respective tax rate against the parcel of land valuation, the Department of Treasury and Finance (DTF) generates invoices for both the ESL and land tax which are sent to each property owner. Each invoice makes provisions for conditions where specific tax exemptions, remissions or concessions occur.

- **Stamp duty** – is calculated on the value of an insurance policy premium submitted monthly or annually or conveyancing that is calculated based on legislative duty. This is generally submitted by a taxpayer agent as part of transaction self-assessment by the agent.
- **Payroll tax** – is calculated on wages paid or payable when an employer's (or group of employers') total Australian wages exceeds the South Australian threshold (currently \$1.5 million annual salary and wages expense). It is collected and administered in line with the *Payroll Tax Act 2009*. Employers provide their details of wages progressively during the year and submit their payroll tax where applicable. An annual reconciliation is undertaken by every taxpayer at year end confirming the level of business wages that are subject to payroll tax that have exceeded the State's defined salary threshold.

Each tax and levy is raised through either paper based or electronic transactions. Once received the payments are reconciled to RevenueSA's bank account and then further reconciled between RIO and DTF's Masterpiece general ledger.





