[P.P.4H

Government
of South Australia

Report

of the

Auditor-General

Supplementary Report

for the

year ended 30 June 2015

Tabled in the House of Assembly and ordered to be published, 27 October 2015

Second Session, Fifty-Third Parliament

Information and communications technology report: October 2015

By authority: P. McMahon, Government Printer, South Australia

2015

General enquiries regarding this report should be directed to:

Auditor-General
Auditor-General's Department
Level 9
State Administration Centre
200 Victoria Square
Adelaide SA 5000

Copies may be obtained from:
Service SA
Government Legislation Outlet
Ground Floor
108 North Terrace
Adelaide SA 5000

Website: www.audit.sa.gov.au

ISSN 0815-9157

Government of South Australia
Auditor-General's Department

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

26 October 2015

The Hon R P Wortley MLC
President
Legislative Council
Parliament House
ADELAIDE SA 5000

The Hon M J Atkinson MP
Speaker
House of Assembly
Parliament House
ADELAIDE SA 5000

Dear President and Speaker

Report of the Auditor-General: Supplementary Report for the year ended 30 June 2015: Information and communications technology report: October 2015

Pursuant to the provisions of the *Public Finance and Audit Act 1987*, I present to each of you a copy of my Supplementary Report for the year ended 30 June 2015 'Information and communications technology report: October 2015'.

Content of the Report

Part A of the Auditor-General's Annual Report for the year ended 30 June 2015 referred to audit work on various public sector information and communications technology systems that would be subject to supplementary reporting to Parliament. This report provides detailed commentary and audit observations on the outcome of that work.

Acknowledgements

The audit team for this Report was Andrew Corrigan, Brenton Borgman, Tyson Hancock, Jamie Thompson and James Baker.

I also express my appreciation for the cooperation and assistance provided by agency representatives during the course of the audit.

Yours sincerely

Andrew Richardson
Auditor-General

Table of contents

Information and communications technology report

Table of contents

Table of contents

Table of contents

Information and communications technology report

1 Introduction

ICT plays an important role not only in the provision of government services but also in providing information to the public.

The SA Government's 2013-14 ICT investment report indicated that total ICT expenditure within government increased from $575.5 million in 2011-12 to $626.6 million in 2013-14. In addition, some key ICT projects have large individual budgets and are critical to agency operations. A notable example is SA Health's patient administration system, EPAS, which has a program funding budget of $422 million over a 10 year period.[1]

Given the importance of ICT, each year we review the integrity of general ICT controls across government and the status of selected key ICT projects, and monitor key ICT developments impacting the State.

The purpose of this Report is to outline some of our 2014-15 ICT audit review activity. Details of our 2014-15 ICT reviews have also been separately communicated in Part B of the Auditor-General's Annual Report for the year ended 30 June 2015 (the 2014-15 Annual Report) and the Supplementary Reports for the year ended 30 June 2014 'Health ICT systems and the Camden Park distribution centre: June 2015' and 'Matters of specific audit comment: December 2014'.

2 Audit program

This Report provides commentary on the following ICT audit reviews of systems, projects and key developments we conducted in 2014-15:

- **Information and communications technology general control issues**: provides a summary of key control issues raised during our reviews of agency financial systems.
- **Cyber security: Information Security Management System (ISMS) – assessment and transition update**: mandatory whole of government standards require agencies to transition to an overarching ISMS. In this review we provide an updated understanding of the ISMS transition arrangements within agencies.
- **Cloud computing**: this review provides an update of the developments in cloud computing adoption within agencies and the Government's strategic direction and guidance in relation to cloud computing.
- **Information systems patch management**: regular patching of information systems is a critical component of securing agency information systems and data. This review examined the patch management processes for two agencies.
- **Whole-of-government Distributed Computing Support Services contract**: the DCSS contract relates to the provision of server management and support services on agencies' distributed server infrastructure. This review provides a high-level update of DCSS transition arrangements to the new contract arrangements.

[1] EPAS budget of $422 million as recorded in the SA Health 2011-12 mid-year budget review. Refer to Supplementary Report 'Health ICT systems and the Camden Park distribution centre: June 2015'.

- **StateNet Active Directory**: AD is a centralised information system used to manage network user authentication, data security and distributed resources, and enables integration with other directories. This review sought an understanding of the overall management and security control processes in place for the State AD network.

- **Website management and security follow-up review**: in the Auditor-General's Annual Report for the year ended 30 June 2014 (the 2013-14 Annual Report) we reported on security control deficiencies of selected government website applications. This review provides a recap of those findings and outlines the current remediation status.

- **SA Health hospital activity – data integrity review**: Activity Based Funding is a system used to determine federal funding for public hospital services based on the number of services provided to patients and the price for delivering those services. This review assessed the integrity of activity data provided to the Commonwealth for ABF under the National Health Reform Agreement.

- **Enterprise Pathology Laboratory Information System**: EPLIS is planned to provide SA Health with a consolidated laboratory information system that provides functionality across all pathology disciplines. This review provides an understanding of the current program implementation status, budget and expenditure to date, key risks and the system's impact and readiness for the new RAH.

- **Pharmacy systems implementation at the new Royal Adelaide Hospital**: the new RAH Program includes a number of sub-projects to deliver current and new ICT services to the facility. One such sub-project was the new RAH ICT Pharmacy project. This review obtained an understanding of the project implementation status for pharmacy systems at the new RAH, including expected benefits and costs, key risks and the system's impact and readiness.

3 Information and communications technology general control issues

3.1 Introduction

ICT systems play a crucial role in storing, processing, transmitting and manipulating agency financial data. For example, ICT financial systems are used to perform payroll, accounts payable and accounts receivable functions within government.

Given the importance of these ICT financial systems, we perform selected controls testing across government on an ongoing basis. This ICT controls testing helps us to validate the accuracy and completeness of agency financial data.

3.2 Audit objective and approach

In examining general ICT controls we use the SA Government's ISMF as a baseline. The ISMF represents the Government's mandated information security standards, guidelines and control mechanisms. We also take into consideration recommended best practices. For

example, the Australian Signals Directorate[2] recommends a number of strategies to mitigate against targeted cyber intrusions.

3.3 Key findings

Some of the key ICT control issues for financial systems that we raised in 2014-15 to selected agencies include instances of:

- gaps in procedural and system documentation
- excessive system privilege access being granted and weaknesses in password controls
- lack of timely notifications of employee terminations and instances of obsolete user access
- insufficient documentation and controls of segregation of duties, with potential segregation of duties conflicts identified
- lack of regular internal user access reviews being performed
- lack of independent review of key changes to applications and sensitive data
- insufficient device maintenance and patch management
- inadequate operating system and application logging
- insufficient recording of changes and actions undertaken to resolve system errors
- deficiencies in the timely resolution of known defects and risk management
- the absence of current business continuity and disaster recovery plans and/or testing of plans
- deficiencies in compliance and contractual reporting and monitoring against vendor contractual requirements.

3.4 Concluding comment

If ICT control issues are not appropriately remediated by agencies, there is the increased potential for the confidentiality, integrity and availability of their financial data to be compromised. This can also lead to increased opportunities for fraud and system downtime, and can have significant financial consequences. It is particularly concerning that we raise certain control deficiencies, such as instances of excessive system privilege access and obsolete user access, on an ongoing basis.

We note that these issues must be addressed in a timely manner, taking into consideration a number of other ICT challenges being experienced within government. In particular, the need to reduce budget expenditure, replace legacy systems and consider the implications of ICT developments, such as cloud computing and the growing use of mobile devices.

---

[2] The Australian Signals Directorate is a part of the Australian Government's Department of Defence. It has a whole-of-government role in supporting Australia's national security.

Despite these challenges, all agencies must ensure appropriate attention is applied to address general ICT control deficiencies and comply with mandated government standards.

4 Cyber security: Information Security Management System – assessment and transition update

4.1 Introduction

It is critically important that government agencies have appropriate cyber security controls for protecting sensitive information and providing government services. Cyber incidents are likely to be occurring without being detected. ICT is pervasive throughout government activities and agencies are entrusted with increasing amounts of digital information.

The ISMF describes policies and standards supporting contemporary industry practices for the security of information stored, processed, transmitted or otherwise manipulated using ICT. The ISMF requires agencies to establish and maintain an ISMS.

Last year we reported that the Government's Cyber Taskforce had engaged an external contractor to independently assess whole-of-government security, including the level of maturity of agencies' capabilities to manage and respond to cyber security threats. The Cyber Taskforce review identified several factors that may adversely impact the Government's cyber resilience and preparedness for changing threats, and its ability to withstand and recover rapidly from disruptions. A submission intended to inform Cabinet of the findings of the Cyber Taskforce review was being finalised by the ODG, a division of DPC. We also noted that shortcomings reinforce the requirement for agencies to implement an effective ISMS.

Cabinet received the findings of the 2013-14 Cyber Taskforce review in September 2015.

4.2 Audit objective and approach

In 2014-15, we sought to determine the status of ISMS transition arrangements within agencies. We also sought an update of the activities of the ODG, which has assisted agencies with this transition.

This primarily involved liaising with the ODG, and referring to documentation from the ICT Board and the recent Cabinet submission outlining recommendations from the Cyber Taskforce review.

4.3 Key findings

In September 2015, the findings and recommendations of the Cyber Taskforce review were submitted to Cabinet.

Cabinet approved a series of actions responding to the report findings that, when implemented, will establish:

- the necessary authority and framework to address across-government cyber security incident response and containment

- comprehensive and relevant guidance on the Government's top 10 cyber security resilience and preparedness objectives
- periodic management and annual Cabinet reporting on the top 10 objectives
- annual review of the top 10 objectives to maintain relevance.

Implementing an ISMS is an agency responsibility, with chief executives accountable for ISMF compliance. The ODG has assisted agencies in implementing an ISMS by coordinating workshops and making relevant standards available to agencies at no cost.

4.4 Details of findings

The ISMF records the Government's mandated information security standards, guidelines and control mechanisms for government. Agencies must comply with the ISMF. It applies to government agencies and suppliers to Government whose contractual obligations require compliance with this framework. The purpose is to encourage agencies to adhere to contemporary industry practices for securing their information that is stored, processed, transmitted or otherwise manipulated using ICT.

The latest version of the ISMF (version 3) emphasises the importance of developing appropriate risk management principles and cyber security controls. In particular it requires agencies to transition to an overarching ISMS that is continually monitored and improved as needed. An ISMS consists of a set of policies, standards, implementation guidelines and procedures for information security management.

In February 2012, the former Office of the Chief Information Officer, now the ODG, developed an ISMF transition guideline. The aim of the guideline was to assist agencies and relevant suppliers to progress from their current state to an operating environment that adheres to the requirements introduced in the latest version of the ISMF.

This ISMF transition guideline indicates that agencies should implement an ISMS through a three-phased approach over a period of six years as follows:

- Phase 1 (expired 30 June 2013) – establish an ISMS for information assets or undertakings that are critical or highly sensitive to the business
- Phase 2 (expired 30 June 2015) – improve what is in place, expand and logically progress the coverage of the ISMS to at least 50% of the agency operating environment
- Phase 3 (expires 30 June 2017) – optimisation of the ISMS.

4.4.1 Information Security Management System transition update

In 2015 we requested an update on the status of the ISMS transition by agencies.

The ODG responded that the ISMF mandates that agencies implement an ISMS that encompasses the ISMF baseline requirements (ie State Government critical ICT infrastructure) as a minimum. The implementation time frames in the ISMF transition guideline, however, are not mandatory.

The ODG also indicated that the implementation of an ISMS is an agency responsibility, with chief executives accountable for ISMF compliance (including ISMS implementation) through DPC Circular PC030 'Protective Security Policy Framework'. To assist agencies in implementing an ISMS, the OGD has coordinated several ISMS implementation workshops, facilitated by an accredited trainer. Further, in May 2015, a workshop on ISMF version 3.2 (released in late 2014) and ISO 27001:2013 'Information Security Management' (on which the latest ISMF is based) was made available to agencies at no cost.

4.4.2 Multi-agency cyber security assessment

In 2013-14, on behalf of the Cyber Taskforce, the Office of the Chief Information Officer engaged an external consultant to perform a multi-agency cyber security assessment of a large proportion of government agencies. The Cyber Taskforce review sought to assess each agency's level of security governance maturity. This focused specifically on ICT privacy, security assurance, compliance, and ICT service continuity, relevant to the implementation of their respective ISMF/ISMS.

The review identified significant gaps and further actions to prevent or minimise the impact of cyber incidents or inappropriate use of government ICT systems. In particular it identified that 34% of agencies reviewed had either not yet documented or had only partially documented key ISMS requirements.

Other key findings from the Cyber Taskforce review requiring agency management attention included:

- recognising that technical security controls could be improved
- increasing the level of proactive security monitoring, including privilege access
- incorporating cyber preparedness control
- addressing inconsistencies in process relating to detection, management, reporting and escalation of security incidents across government
- addressing ineffective data classification and security risk management covering critical business services
- improving security governance over third party IT service arrangements.

The review also identified a number of strengths. This included pockets of information security excellence across agencies, and most agencies had a basic level of technical security controls in place in accordance with the ISMF baseline requirements.

4.4.3 2014-15 Information Security Management System developments

This year, our high level review confirmed that while the findings from the Cyber Taskforce review were reported to the Minister for the Public Sector and the Cyber Taskforce, a Cabinet submission reporting on those results was only finalised in September 2015.

The purpose of the September 2015 Cabinet submission was to outline the results of the Cyber Taskforce review and make certain recommendations as to future assessments.

Cabinet approved 10 cyber security resilience and preparedness objectives (the Top 10) to address governance, management and technical matters. This strategy intends to leverage from the issues identified in the original cyber security review outcomes report produced in late 2013.

The new proposed Top 10 objectives include:

- agency security governance
- ISMF implementation and information classification
- incident management
- technical controls, amongst other security considerations.

The ODG advised that it intends to review the Top 10 annually, in order to ensure that it accurately reflects the State's strategic and risk position.

Additionally, agencies are required to lodge an implementation plan within three months of the Top 10 being released, and report progress within their agency to the ODG quarterly thereafter. The ODG will then collate the results for an annual report to Cabinet. This is a fundamental change in role for the ODG, as no formal central monitoring or reporting to Cabinet previously existed. Under this proposed arrangement the responsibility to self-report to the ODG and Cabinet rests with the agency.

We note that a further independent cyber security assurance review, coordinated by the ODG, is proposed for 2016-17. This review is intended to assess agency processes in improving cyber resilience and preparedness. It will assess agencies against existing policy, the Top 10 and the recommendations of the 2013-14 Cyber Taskforce review. The findings from the proposed 2016-17 review are expected to be reported to Cabinet.

4.5 Concluding comments

It is encouraging to note that, when implemented, the recommendations that Cabinet has approved will improve cyber security. Central monitoring and whole-of-government visibility of agencies' compliance maturity with the ISMF and ISMS implementation will be an important element in progressing this improvement.

While the ODG proposes to undertake a further independent cyber security assurance review in 2016-17 to assess the progress of ISMS implementation, the ODG needs to be mindful of the competing time frames of the 30 June 2017 target date for finalising ISMS phase 3. In particular, the results of the 2016-17 review will need to be provided to Cabinet as soon as practicable, so that the State and agencies can act on these findings in order to minimise any risks identified.

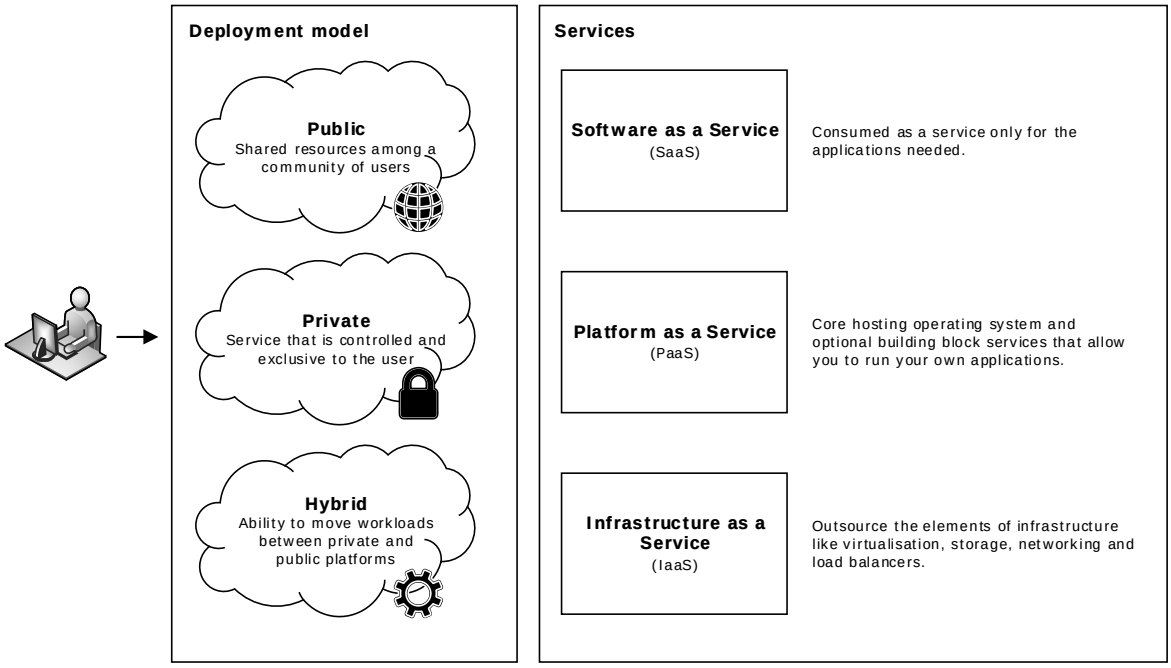
5 Cloud computing

5.1 Introduction

Cloud computing essentially and simply means storing and accessing data and programs over the internet rather than on a local computer's hard drive. Technically, cloud computing is an ICT sourcing and delivery model for enabling convenient, on-demand network access to a shared pool of configurable computing resources, including servers, networks, storage,

applications and services.[3] Cloud computing service providers establish large-scale computing resources and capacity so that they can rapidly respond to changing demands by users with minimal user effort.

The following diagram provides an overview of the multiple model options available within cloud computing.



While there are various cloud computing model options, depending on respective needs and requirements, agencies are generally focusing at this stage on software and infrastructure as a service through a private cloud deployment model.

Part A 'Audit overview' of the Auditor-General's Annual Report for the year ended 30 June 2013 provided commentary on the Government's position at that time regarding cloud computing developments and its recommended direction to government agencies.

At that time, we acknowledged that cloud computing potentially represented an opportunity for government agencies to contain ICT costs and to leverage more adaptive technology. Providing sufficient controls are implemented, cloud computing could offer appropriate security arrangements or improvements, whilst also improving system resilience.

We also acknowledged that whilst cloud computing offered potential benefits, there were also risk considerations that needed to be assessed by agencies.

These risks included:

- the need to realign business processes to ensure that any risk traditionally managed by internal IT departments are not overlooked when moving ICT services to the cloud

[3] 'The NIST Definition of Cloud Computing' Special Publication 800-145, National Institute of Standards and Technology, US Department of Commerce, September 2011. For more details refer to http://csrc.nist.gov/

- legislative and jurisdictional considerations surrounding data held by third parties, potentially offshore.

Part B of the 2014-15 Annual Report includes commentary on cloud computing matters and systems under 'Department for Communities and Social Inclusion', 'South Australian Government Financing Authority', 'South Australian Housing Trust' and 'South Australian Water Corporation'.

5.2 Audit objective and approach

During 2014-15 we monitored developments with cloud adoption within agencies and the Government's strategic direction and guidance in relation to cloud computing.

This primarily involved liaising with the ODG, and referring to whole-of-government frameworks, policies and standards that impact cloud computing.

5.3 Key findings

The review of the SA Government's management of cloud computing has identified:

- the ongoing development of the cloud service policy framework
- the provision of cloud service supporting standards, guidance documentation, tools and case studies
- that agencies continue to purchase, implement and manage cloud services based on traditional government, policy and contractual frameworks that were intended for the previous ICT sourcing model.

5.4 Details of findings

Originally the SA Government did not have a central policy position regarding agency use of cloud services. Rather, it was aligned to the Australian Government position.

This changed in July 2013 when the Australian Government released a new policy that signalled a shift in its approach to cloud computing, which then differed to the SA Government's position.

5.4.1 Government ICT strategy

In October 2013, Cabinet approved 'South Australia Connected: Ready for the Future – A strategic direction for Information and Communications Technology in the Government of South Australia' (SA Connected). This document sets the strategic direction for the use and alignment of ICT in government, and within all agencies.

As part of this strategic direction, there is now an expectation that agencies invest in services, including cloud and cloud-like services, rather than buying hardware and software.

The direction outlined in SA Connected reflects a shift in government ICT expenditure in recent years, with an increase in the use of externally provided ICT services as shown in the following table.

ICT expenditure category[4]	Percentage of total ICT spend 2009-10	2013-14
Traditional hardware and software products	40%	31%
Externally provided ICT services	24%	33%

5.4.2 *Privacy Act 1988* (Cwlth) amendment

In March 2014, the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cwlth) introduced significant changes to the *Privacy Act 1988* (Cwlth). These amendments seek to provide assurance that where an Australian entity discloses personal information to an overseas recipient, it must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach privacy considerations in relation to the information.

Within the ISMF, there is also reference to privacy considerations associated with the implementation of cloud computing and software as a service.

The ISMF requires agencies to gain an understanding/appreciation of:

- legislative and government expectations
- the nature and provision of privacy legislation jurisdiction obligations
- the underlying terms and conditions when implementing these types of services
- user and identity management
- access and connectivity
- change control.

By complying with the above requirements, there is an expectation that an appropriate assessment and classification of agency data and assessment of the cloud service provider will occur that should satisfy privacy compliance considerations. This assessment should occur prior to entering into a formal agreement with a cloud service provider.

This amendment to the *Privacy Act 1988* (Cwlth), and recent changes in storage opportunities within Australia through the use of cloud services, further escalated the need for clearer direction and guidance.

5.4.3 SA Government cloud services policy

Since changes to the Australian Government cloud policy position in 2013 the former Office of the Chief Information Officer, in consultation with agencies, undertook to determine and develop initial guidelines where gaps with the Australian Government policy existed with the SA Government's approach. This incorporated an executive overview and practitioner's guide for off-site storage of government data. This was seen as a key risk and possible barrier for agencies when considering the adoption of cloud computing.

Despite these initial guidelines, agencies were seeking further direction about the legislative and jurisdictional considerations regarding data held by third parties, sovereignty, access and audit, and protection of data. The importance of strengthening this direction was highlighted when a comparison in 2014 of other Australian jurisdictions identified that the majority of entities assessed were contemplating cloud services as part of their procurement options.

[4] Figures taken from 'Government of South Australia 2013-14 ICT Investment Report', Office for Digital Government, April 2015. These figures have not been audited.

To help address agency concerns, in August 2014 the former Office of the Chief Information Officer began to develop a cloud policy position for the SA Government. This included drafting a cloud services framework along with supporting policy, standards and guidance. These were intended to assist SA Government agencies in the procurement, implementation and management of cloud services.

During this period, the SA Government also started developing a government digital strategy. The strategy acknowledged that governments across Australia and the world were increasingly transforming their service delivery to make the most of advances in digital technology.

In early 2015, the ICT Board approved ICT Policy Statement 3 'Cloud Services'. This policy statement requires public sector agencies to evaluate one or more cloud services in every new or reformed ICT sourcing, procurement or market approach. Agencies are also required to consider their business needs, resilience and risk as part of their evaluation.

Additionally, the policy stated that following an equitable evaluation, a cloud service should be chosen unless:

- it will not deliver the best value-for-money outcome for government – that is, another sourcing option is demonstrably better value for money in terms of innovation and productivity outcomes
- the cloud services assessed will not adequately meet the Government's obligations under relevant legislation, instructions, policies, standards, and rulings.

The policy statement also reiterates that agencies remain ultimately accountable for the security of their data in any environment.

5.4.4 Additional policy guidance

Currently, for those agencies that have or are progressing with cloud service initiatives, the decision to invest in cloud services to meet their current operational requirements rests with the agency decision-makers. As such, agencies generally continue to purchase, implement and manage cloud services based on traditional governance, policy and contractual frameworks which were not intended for the sourcing of cloud services.

To further support the cloud services policy statement, the ODG proposed to work with agencies to develop additional areas of guidance.

The ODG has created a cloud services policy framework. This framework is intended to be used as a visual tool in seeking feedback on how the cloud policy and supporting guidance could work together. The framework's primary function is to be used as an internal planning tool to inform agencies of the ODG's approach to the publication of cloud standards, guidance, tools and case studies.

The ODG has confirmed that a number of additional cloud computing guidance materials for agencies have been developed including:

- ISMF Ruling 2 'Storage and processing of Australian Government information in outsourced or offshore ICT arrangements'

- ISMF Guideline 5 ‘Cloud Computing’
- ISMF Standard 139 ‘Security in an Outsourced Environment’
- Privacy and Cloud Computing Guideline
- Offsite Storage of SA Government Data – executive governance
- Data Breach Guidelines – Managing the notification of those affected when data is compromised.

5.4.5 Summary of Office for Digital Government response

The ODG advised that it considers cloud computing an extension of the Government’s existing approaches to outsourced services. As such, it is covered by a number of existing laws, instructions, policies, standards and rulings in use by agencies.

The ODG also acknowledged that it could be viewed that some current governance, policy and contractual frameworks were intended for previous sourcing models. However, the ODG stated that the SA Government has been sourcing, managing and governing technology services and data from outsourced providers for many years, which is analogous to the procurement of cloud services.

The ODG advised that it will continue to develop planning, procurement and evaluation, implementation, and user cloud services guidance. Key areas of priority expected to be addressed in 2015-16 include:

- considering budgeting requirements for cloud services
- clearer guidance on security and risk
- clearer guidance on records management
- consideration of internet traffic and possible capacity/latency issues that may be caused by the uptake of cloud services.

The ODG is also aware that there has been strong support from other Australian jurisdictions for developing consistent cloud standards and guidance. Accordingly, the ODG advised that it is working to identify opportunities for harmonising cloud-related policies and standards.

5.5 Concluding comment

The development of further cloud computing guidance is important in supporting agencies as they attempt to leverage on technical advancements. While traditional governance principles may exist around procurement, security and risk, there remains a need to develop and enhance guidance that reflects the current process, design, governance and contract management requirements for cloud services.

6 Information systems patch management

6.1 Introduction

A software patch is a piece of software that is designed to fix defects or vulnerabilities, or provide updates to an information system. Applying software patches is required for both operating systems and applications.

Regular patching of information systems is a critical component of securing agency information systems and data.

The Australian Signals Directorate has developed a list of strategies to mitigate targeted cyber intrusion. Patching operating system vulnerabilities is listed as one of the four most effective strategies to mitigate this risk.

Additionally, the ISMF outlines the expected patching requirement for agencies. This includes documented and planned procedures for examining hardware and software to ensure that security patches and fixes have been implemented. A maximum time frame for implementing security patches should also be specified in documentation.

6.2 Audit objective and approach

Given the importance of patch management, in 2014-15 we reviewed the patch management processes for DPC and the Department of Planning, Transport and Infrastructure. The review included:

- understanding agency arrangements for managing server and desktop operating system environments (including the use of outsourced providers)
- reviewing the processes for identifying, testing, approving, deploying and monitoring operating system patches
- selecting a sample of servers at each agency for review
- testing the operating effectiveness of server operating system patch management controls for these servers by confirming whether all available and required patches were installed.

6.3 Key findings

The review noted certain positive controls in place in the two sample agencies tested. This included a consistent process for identifying patches, patch testing on development servers or 'early adopter' user workstations, and the approval and deployment of patches via a formal change management process.

Our testing of both agencies also noted the following control weaknesses.

DPC control weaknesses:

- insufficient formal policy and procedure coverage of the patch management process

- insufficient documentation of deployed workstation patches or patching exemptions
- minor discrepancies identified between agency server listings and invoices from outsourced providers with supported servers listed
- delays in upgrading operating systems on a large number of servers to a supported operating system ahead of an end-of-support deadline in July 2015
- servers identified with missing security update patches.

Department of Planning, Transport and Infrastructure control weaknesses:

- patch management procedures not reviewed on a regular basis
- weaknesses in patch management assurance practices, including notification of deployed server patches and server patch compliance monitoring
- servers identified with missing security update patches.

Risk exposure

Where policies and procedures are not developed or reviewed on a regular basis, there is a risk that a consistent process is not applied to patch management, increasing the potential exposure to security vulnerabilities.

Servers running Windows Server 2003 will not receive any operating system security updates following Microsoft's July 2015 support cut-off date. This increases the risk of potential security vulnerabilities, including unauthorised access to sensitive information stored on servers with unpatched operating systems.

Where critical patches are not applied, there is an increased risk of unauthorised access through an unpatched security vulnerability.

Recommendations

Based on the review findings, we provided both agencies with a number of recommendations to remediate control weaknesses.

In order to address weaknesses in policies and procedures, we recommended that server operating system patching follow a formal change management process. This includes documenting approved, implemented or exempted patches. Exemptions should be reviewed on a regular basis to ensure their validity.

We also recommended that agencies ensure that regular patch compliance scans of servers and workstations are performed. Results of compliance scans should be reviewed to gain sufficient assurance that all appropriate patches are applied.

Finally, we recommended that agencies progress the migration of servers to a supported operating system with some urgency. The time unsupported server operating systems remain in the production environment should be minimised following the July 2015 support cut-off date for Windows Server 2003.

Agency responses

Both agencies responded that the identified deficiencies would be remediated. This included updating policies and procedures, as well as ensuring regular reviews of operating system patching compliance.

6.4 Concluding comments

In summary, while we noted positive controls during testing, we found a number of control deficiencies that potentially expose the Government to a number of risks. This includes the unauthorised disclosure and modification of data via unpatched server operating systems.

Patching is a critical component in mitigating the risk of targeted cyber intrusion. All agencies within the SA Government should be diligent in ensuring that their approach to patch management is comprehensive and that critical operating system patches are applied in a timely manner.

7 Whole-of-government Distributed Computing Support Services contract

7.1 Introduction

The whole-of-government DCSS contract covers the provision of server management and support services for agencies' distributed server infrastructure.

The contracted suppliers provide IT support services to government agencies across metropolitan and regional South Australia. The IT support services are responsible for the provision of both physical and virtual server management and support services on agencies' distributed server infrastructure. The availability of continuous and reliable support services is essential given the crucial role ICT systems undertake within government.

In 2007, the SA Government entered into initial DCSS arrangements with HP (then EDS Australia) and NEC (then CSG Pty Ltd). This contract was for a period of three years with an option for a further three years. A further extension to 30 June 2014 was later approved pending the implementation of a new DCSS contract.

Between 2012 and 2013, an acquisition plan, request for tender, request for improved pricing and final evaluation of shortlisted respondents occurred.

In February 2014, Cabinet approved the establishment of the new DCSS contract, with a total estimated cost of $267.5 million (GST inclusive) over a six year term. This includes a three year initial term, with an option to extend the contract for another three years at the SA Government's discretion.

7.2 Audit objective and approach

In 2014-15, we gained an updated understanding of DCSS transition arrangements within the ODG.

This primarily involved liaising with ODG representatives and referring to documentation, such as the DCSS contract, a recent Cabinet submission, estimated savings calculations and ICT Board minutes. We also attended a DCSS transition briefing session provided to affected agencies.

7.3 Key findings

The new DCSS contractual arrangements are with suppliers NEC and CSC.

Despite some clean-up activities, all agencies previously receiving DCSS services from HP migrated to the new arrangements by 30 June 2015.

For agencies previously receiving DCSS services from NEC, DPC advised that these services continued under the new contract. Where these agencies selected CSC as their preferred service provider, temporary customer agreements were initiated by NEC until CSC could take over the services.

DPC estimates a potential reduction in expenditure of $40.2 million over the term of the contract, although it will take at least six months to fully understand agency service requirements and associated costs to provide a more accurate estimate of savings. In the interim the Department of Treasury and Finance has commenced collecting savings as part of its internal budgeting process.

7.4 Detailed findings

7.4.1 Distributed Computing Support Services contract developments

The new DCSS contract commenced on 1 July 2014, with an expected potential reduction in total agency expenditure of $40.2 million between 2014-15 and 2018-19.

The successful respondents to the new DCSS contract were NEC and CSC.

Agencies that had customer agreements with HP, a supplier under the previous DCSS contract, were originally required to transition to either NEC or CSC by 31 December 2014. This transition was subsequently extended to 30 June 2015 in recognition of the original timelines not being achievable.

Agencies with customer agreements with NEC under the previous DCSS contract were permitted, in accordance with the established secondary procurement process, to remain with NEC. This permission was subject to the agency completing a request for quote with both approved suppliers by 30 June 2015.

7.4.2 Secondary procurement process

As at June 2015, a number of existing NEC customers had not finalised a request for quote in accordance with new DCSS arrangement.

Where agencies selected CSC as their preferred service provider, temporary customer agreements were initiated by NEC, as CSC experienced temporary resourcing constraints brought about by the late transitioning of certain agencies onto the new DCSS contract. These temporary customer agreements with NEC on CSC's behalf were for a restricted period, not exceeding three months (30 September 2015).

7.4.3 Distributed Computing Support Services server transition

In August 2015, DPC advised that all agencies that were previously supplied with services provided by HP were successfully migrated to the new arrangements by 30 June 2015. The only activity after this date was an HP audit of the server environment at SA Health to ensure all monitoring tools were removed. HP was also required to disable and remove all core DCSS support infrastructure.

For agencies already receiving services from NEC, DPC advised that these services continued under the new contract. Where agencies had yet to conclude the secondary procurement process and elect to migrate to CSC, DPC regularly monitored the progress of transition activities and sought to ensure migration was completed by 30 September 2015.

7.4.4 Estimated savings

Whilst DPC estimates a potential reduction in expenditure of $40.2 million, it anticipates that a minimum six month time frame from 1 July 2015 is required to fully understand agency service requirements and associated costs.

However, DPC acknowledged that the estimated reduction in expenditure calculated over six years is to be returned to the State's budget. We have also been advised that the Department of Treasury and Finance has already commenced collecting these savings as part of its internal budgeting process.

7.4.5 Summary of Department of the Premier and Cabinet response

We wrote to DPC in June 2015 seeking to confirm our understanding of the DCSS transition arrangements and, having regard to the contract expiry date of 30 June 2015, the status of and actions associated with finalising the transition to the new DCSS contract.

DPC responded that it was satisfied the transition to the new arrangements was well managed and that, despite delays by some agencies in finalising their secondary procurement processes, all services were transitioned within required time frames.

DPC also advised that the new contracts are now fully operational and that it believes the procurement process has delivered significant savings to the State.

7.5 Concluding comments

The whole-of-government DCSS contract underpins the continuous and reliable provision of server management and support services on agencies' distributed server infrastructure. The availability of support services is essential given the crucial role ICT systems within government.

Transition to the new DCSS contractual arrangements was well progressed at the time of this Report. Where agencies had not concluded secondary procurement processes DPC was seeking to ensure migration was completed by 30 September 2015.

The expected savings from the new DCSS contract play a role in the achievement of overall ICT savings targets of agencies and the State.

DPC anticipated that a minimum six month time frame from 1 July 2015 was required to fully understand agency service requirements and associated costs.

8 StateNet Active Directory

8.1 Introduction

AD is a centralised information system within the Microsoft Windows server environment. It is used to manage network user authentication, data security and distributed resources, and enables inter-operation with other directories. It is also generally used by system administrators to assign security policies, deploy software and apply critical software updates to computer servers and end-user workstations.

Within the SA Government some agencies operate their own AD domains. These are generally connected to an overall State AD facility (the State AD Forest). Where an individual agency does not have its own AD domain its users can authenticate to a centrally managed shared domain within the State AD Forest.

The SNS Active Directory Manager is responsible for the State AD Forest. Agencies are directly responsible for their own domains, and vendors provide services to SNS and individual agencies through various SA Government ICT contracts.

The State's AD domains are important as they allow government users to authenticate and access agency networks and use computer based resources, such as file networks and system applications. The AD domain structure also allows for the use of the government's electronic messaging system (SAGEMS) across the South Australian public service.

Because of this importance an overall management group, the Active Directory Services Governance Committee, meets on a regular basis to discuss issues associated with the State AD Forest. The role of this Committee is to provide overall governance in the planning, design and implementation of the technology, endorsing guidelines and standards and approving any new connections to the State AD Forest. Its members include representatives from those agencies that use the State AD Forest.

8.2 Audit objective and scope

Given the importance of AD, during 2014-15 we sought an understanding of the overall management and security control processes in place for the State AD Forest.

This involved reviewing the following related areas:

- governance arrangements including policy and procedures
- aspects of IT security as mandated by the ISMF
- business continuity arrangements.

8.3 Key findings

Our 2014-15 review raised a number of issues to improve management of the State AD Forest. This included:

- a key procedure document needed to be finalised
- implementation of an ISMS needed to be finalised
- ongoing monitoring of issue remediation needed strengthening
- business continuity arrangements needed periodic testing applied.

8.4 Details of findings

8.4.1 A key procedure document needed to be finalised

SNS has developed a number of documents relating to the management of the State AD Forest. Among the documents we were provided in our review were the:

- State Forest Management Plan (dated 25 March 2014)
- IT Service Continuity Plan for Active Directory (dated 7 December 2012)
- StateNet Conditions of Authentication (draft).

At the time of review an important document for the management of the State AD Forest, the StateNet Conditions of Authentication, was still in draft. This extensive document represents a statement of the minimum requirements agencies need to meet before they are able to use the central State AD authentication service.

For example, among the requirements that agencies would have to comply with, or consider, before using the State AD authentication service were:

- the requirement for every organisation using AD to regularly provide the results of a review of AD by suitably qualified and competent resources
- the requirement for trusts to be regularly reviewed to ensure compliance with ISMF Standard 76 'Management of privileges'. This particular standard relates to the need to document business requirements concerning access
- inter-connectivity between AD domains.

We noted that none of these requirements were being enforced by SNS on agencies linked to the State AD Forest as the StateNet Conditions of Authentication document had not been finalised.

We were informed that this document (in draft form) was issued to agencies for comment before it was to be finalised. We were informed that a major reason for this document not being finalised was the extra logistical effort needed to consult with all agencies using the facility. At the time of review a completion date had not been set.

Risk exposure

Without finalisation of all key procedure documents, and enforcement of the document's specified requirements, an agency may not comply with the minimum requirements needed to be able to use the central State AD authentication service.

Recommendation

SNS should establish a time frame for fully implementing the StateNet Conditions of Authentication document, including the implementation of associated compliance requirements within this document for State AD user agencies.

Agency response

DPC advised that the State AD Forest governance document was expected to be finalised by the last quarter of 2015.

8.4.2 Implementation of an Information Security Management System needed to be finalised

During the review, we were informed by SNS that some work was progressing towards implementing an ISMS for the State AD Forest. An ISMS is a requirement of the ISMF.

It was envisaged that the ISMS for the State AD Forest would include a risk register and risk treatment plan, and a Statement of Applicability.

At the time of review SNS had not yet set a time frame for completion.

Risk exposure

Without ongoing confirmation of technical compliance with established policies and procedures, an important facility like the State AD Forest is likely to be exposed to weaknesses which could, in certain circumstances, increase the possibility of security breakdown or loss of service.

Recommendation

SNS should establish a time frame for rolling out an ISMS for the State AD Forest.

Agency response

DPC is currently implementing an ISMS for the State AD Forest. This is almost complete, with refinement and update for the latest version of the ISMF (version 3) being applied. The estimated completion date is February 2016.

8.4.3 Ongoing monitoring of issue remediation needed strengthening

SNS engages an external service provider to conduct a Risk Assessment Program for Active Directory (ADRAP). The ADRAP is undertaken every two years and covers the whole State AD Forest, including internal domains that are connected to it. The findings and guidance provided by this assessment are then passed to agencies that use the State AD Forest and to any service providers.

The findings from the most recent ADRAP review were detailed in a report completed in September 2013. The issues highlighted included:

- no documented standards and policies for the design and implementation of AD related services
- no formalised release management process
- no test AD facility
- issues with security settings on a number of AD accounts
- no testing of the business continuity arrangements for the facility.

In all, the report highlighted 120 separate issues covering both the State AD Forest and the internal domains connected to it.

The report identified that the facility had a number of high risk ratings concerning a number of technical related issues. A critical rating concerning domain controller health related to the absence of a number of operating system patches applied to the AD servers. The SNS Active Directory Manager stated this was due to the length of time between the last ADRAP review being undertaken and the last server patch updates being applied. In the course of the review we were provided with a completed change record approval for the AD vendor that showed the latest patches had been applied.

The SNS Active Directory Manager indicated that many of the findings from the ADRAP were not directly applicable to the State AD Forest, as the findings did not take account of the particular context of its management and operation within the SA Government environment.

We reviewed documentation that detailed those issues that had been raised from the ADRAP review and those where some amount of remediation was either intended or had taken place. We found this documentation did not provide a sufficient level of detail about actions taken to remediate the identified deficiencies in the ADRAP review, in particular expected remediation dates. There was also no trail of actions, including references to related documents, such as emails, that documented action taken by the service provider to rectify any identified issues.

For such an important facility, there is an expectation that more detailed information would be available to enable any new staff to manage the facility if the current SNS Active Directory Manager was unavailable. There was an over-reliance placed on the current SNS Active Directory Manager given the amount of documentation available for this particular aspect of the system's management.

Risk exposure

If review issues are not appropriately tracked and monitored, there is a risk that over time high risk issues will not be sufficiently acquitted, leaving agencies potentially exposed.

Recommendations

SNS should implement a more robust remediation tracking process for ADRAP reports on the State AD Forest. This would ensure issues and resultant management actions/resolutions can be traced to the actual event that caused the problem. The improvements to the tracking of actions should also provide evidence of actual actions taken to resolve any identified issues.

Additionally, emphasis needs to be placed on ensuring issues are remediated in a fulsome and timely manner and that a person(s) is nominated to be accountable to ensure all open issues are dealt with.

Agency response

DPC advised that an improved issue tracking mechanism would be implemented by mid-2016. DPC is currently engaging a service provider to undertake a new ADRAP review.

DPC will then engage the identified AD suppliers and agencies responsible for each risk to address in detail the risks and issues identified. Particular attention will be given to ensuring the issues are clearly documented, tracked and remediated, making sure that accountability and the resulting actions are documented and completed in a timely manner.

8.4.4 Business continuity arrangements needed periodic testing applied

During the review we were supplied with the IT Service Continuity Plan for the State AD Forest. This plan detailed how the ODG would respond to a major disruption to the facility.

The IT Service Continuity Plan details two risk scenarios that could affect the delivery of State AD services. The first relates to the risk to authentication services covering users logging onto the network and/or accessing network resources. The second risk relates to the compromise of system security.

The plan stated that the main responsibilities for continuity management services reside within SNS. AD service providers, however, must comply with all formal service arrangements, contracts and working arrangements regarding disaster recovery and service continuity. The plan further states that the SNS Active Directory Manager is responsible for developing the detailed recovery procedures needed to support the system.

AD has, within its design, a certain level of redundancy built in. That is, if computers offering the service fail, a backup computer would take over the authentication service. It would require a failure of both primary computers and back-up computer systems running the AD system for the service to not be available.

Despite this level of redundancy we found the backup and recovery arrangements were not subject to periodic testing.

Risk exposure

Without testing of backup and recovery arrangements there is increased risk that an outage could affect service provision.

Recommendation

SNS should establish routine ongoing testing of the recovery of the AD servers to ensure recovery can be effected in the event of a total failure of the service.

Agency response

DPC advised that a routine for ongoing testing of the recovery of State AD servers would be implemented with a new supporting AD vendor, appointed in June 2015. Progress on this issue is being reviewed on a monthly basis.

8.5 Concluding comment

The importance of appropriate AD controls and management by both SNS and individual agencies cannot be underestimated.

Although our review found some positive controls in place, improvements were required in documentation, implementing an ISMS, monitoring issue remediation, and testing business continuity arrangements.

9 Website management and security follow-up review

9.1 Introduction

The 2013-14 Annual Report included commentary on our review of government website applications. The review was undertaken because of the importance of agency websites in providing information and services to the public and internal agency stakeholders.

As mentioned in that Annual Report, the then Office of the Chief Information Officer, now the ODG, issued new whole-of-government standards in 2012 specifically relating to web server security and web application security. This was against a background of many agencies not having either established processes to undertake risk assessments of their websites or plans to address issues found in risk assessments.

This section recaps our 2013-14 findings and outlines the status of remediation.

9.2 Audit objective and approach

The objective of this review was to obtain an update on the remediation status of website management and security findings we raised in 2013-14.

This involved formally liaising with the agencies involved to obtain a status update on each finding.

9.3 Key 2013-14 findings

In 2013-14 we gathered certain high-level information regarding agency websites, including internal policies and procedures, results of assessments undertaken against the mandatory website standards, results of penetration testing and known security incidents.

From the high-level information provided by agencies it was apparent that there were:

- gaps in compliance with the whole-of-government web application and security standards
- certain policies and procedures relating to website security and management that either had not been finalised or needed updating
- known vulnerabilities, which had been highlighted by some internal agency automated scans.

This information was then used to select certain agency websites for review, with the assistance of an external security firm. We used the Application Security Verification Standard 2013[5] and Common Vulnerability Scoring System[6] in testing and risk ranking the resultant findings.

[5] The Application Security Verification Standard aims to help organisations to develop and maintain secure applications. For more details refer to http://www.owasp.org

[6] The Common Vulnerability Scoring System provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. For more details refer to http://nvd.nist.gov

From our sample testing of websites we found a number of security and control concerns, including:

- the sending of unencrypted user credentials for some sites
- password weaknesses including no password lockout for failed login attempts, no password expiry and not requiring users to select strong passwords
- inadequate validation of user input in one website, which allowed cross-site scripting attacks and variables in web forms which could be overwritten
- weaknesses in website session key management
- lack of encryption for data transfers
- security weaknesses that allowed the enumeration of valid accounts and their selected security questions, cross-site scripting through lack of input validation, extraction of personal information from databases, and extraction of documents uploaded by other users
- security weaknesses that resulted in the exposure of technical information that could be used as a vector for attack, including the application version in one site and server path for another website.

In summary, we recommended the selected agencies remediate the issues raised and emphasised the need for all agencies to assess their compliance status against the website standards.

9.4 Key 2014-15 findings

In 2014-15 we sought a progress update from selected agencies on their remediation efforts.

In response, the agencies indicated that certain strategies and measures had been taken or were in progress to address the identified website weaknesses, taking into account their particular circumstances.

Some website applications were identified as candidates for replacement and either had been decommissioned since our previous review or were due to be decommissioned. In other instances, applications were being temporarily updated to resolve issues but were ultimately expected to be replaced by other applications that were deemed security compliant.

Some issues identified as low risk were considered by agencies not to warrant remediation. Where direct remediation was determined as appropriate, agencies were at various stages of completion. One agency, for example, had remediated all identified issues with its website while others were still awaiting quotes from their service providers. In the latter scenario, the service provider was to either remediate the current website software version or had scheduled remediation into future software releases.

9.5 Concluding comments

Our 2013-14 review highlighted aspects of non-compliance with the Government's website standards. It also noted in the testing performed on selected sample websites that although some positive controls existed there were a number of security and control deficiencies. These deficiencies had the potential to compromise website data and increase the risk of the modification of website content being presented to the users.

Our 2014-15 follow-up review indicated that certain action had been taken or was in progress regarding the compliance of selected government websites to the website standards. Some issues may not be fully remediated until certain non-compliant applications have been replaced. In the interim, the potential risks of these weaknesses need to be monitored and minimised where possible.

Overall, the outcome provides evidence that the security of websites should be a continued area of focus for all government agencies.

10 SA Health hospital activity – data integrity review

10.1 Introduction

ABF is a system used to determine the funding for public hospital services based on the number of services provided to patients and the price for delivering those services. ABF uses national classifications, cost weights and prices to determine the amount of Commonwealth funding for each activity or service.

As part of the funding process, SA Health is required to regularly submit a number of patient activity data extracts (Commonwealth submissions) to the IHPA and the NHFB . This data is obtained from hospital source systems and loaded to SA Health's CDW via data collections. Data collected includes inpatient (admitted), outpatient (non-admitted) and emergency department patient activity data.

10.2 Audit objective and approach

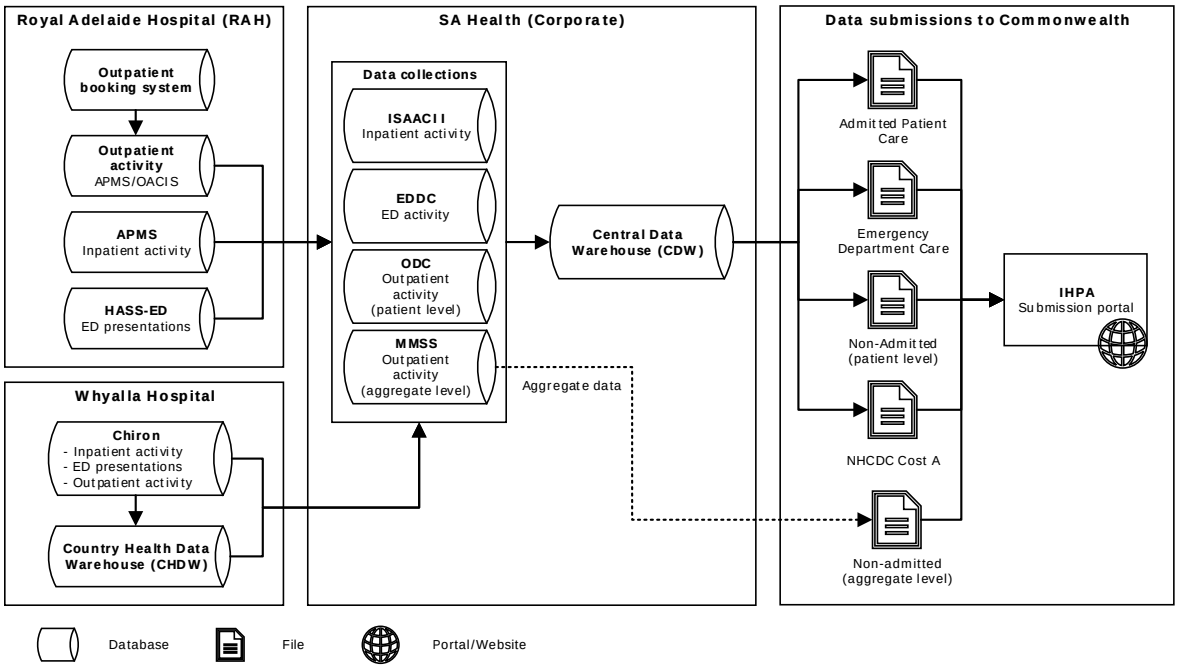
The objective of our 2014-15 review was to assess data integrity for activity data provided to the Commonwealth for ABF under the National Health Reform Agreement.

The scope of this review included assessing, over a defined period, data integrity controls relating to the transfer of activity data from patient administration systems at the RAH and Whyalla Hospital to SA Health data collections.

The completeness and consistency of ABF data was reviewed by matching records between hospital source systems, SA Health data collections, the CDW and the most recent Commonwealth submission files.

A high-level overview of the process of extracting, transforming and loading this data through the various systems is shown in the following diagram.[7]

[7] A more detailed diagram of ABF systems and data flows in contained in section 10.8.1.



For further details of the testing approach and data validated, refer to section 10.4.

10.3 Key findings

Based on the work performed from data obtained for the sample period, we concluded that ABF data integrity controls are operating effectively for admitted and emergency department patient activity data.

This includes the integrity of data as it is extracted, transformed and loaded between the relevant hospital source system, data collection, the CDW and the Commonwealth submission. Exceptions identified from data matching were minimal when compared with the total test populations for Whyalla Hospital and RAH data.

Testing of data integrity controls associated with non-admitted data was restricted to the completeness and consistency of the Commonwealth submission file. We concluded that the controls for this component were operating effectively.

We identified certain shortcomings in need of management attention. The key findings requiring remedial action were:

- insufficient documentation of end-to-end ABF data flows
- no formal review of ABF data prior to submission
- PPM costing manual in draft status
- insufficient documentation of outpatient data collection requirements and the extracting, transforming and loading process

- clinical coding audit not performed since 2011
- emergency department data load process not capturing record corrections
- emergency department data matching exceptions identified for Whyalla Hospital and the RAH
- mismatch of medical record numbers for RAH admitted data.

SA Health responded positively to our recommendations. SA Health explained its risk assessment of the audit findings, noting where areas for improvement did not create risks to funding under existing Commonwealth arrangements. All agreed remedial action is to be completed by March 2016.

For further details of the data validation results refer to section 10.5. Further details of the issues identified, along with improvement recommendations and responses from SA Health, are provided in sections 10.6 and 10.7.

10.4 Detailed testing approach

As mentioned, the scope of this review included assessing data integrity controls relating to the transfer of data between patient administration systems at selected hospital sites and SA Health data collections. The selected sample sites were the RAH and Whyalla Hospital.

We performed high-level validation of data integrity controls across a number of systems and patient activity datasets as data was loaded from hospital source systems and databases through to Commonwealth submissions.

The following types of data were reviewed:

- admitted activity
- emergency department activity
- non-admitted activity (limited to assessing the completeness and consistency of Commonwealth submissions).

Validation performed across this data included verifying the completeness and consistency of data from:

- hospital source systems to SA Health data collections
- SA Health data collections to the CDW
- the CDW to Commonwealth submission files.

We verified the completeness and consistency of records between these systems by matching records using a combination of medical record number, separation date/time and hospital code. Discrepancies between systems were investigated with SA Health or the relevant LHN.

This review also included an assessment of controls over the management of ABF data quality throughout this process and the validation activities undertaken prior to submitting ABF data to the Commonwealth.

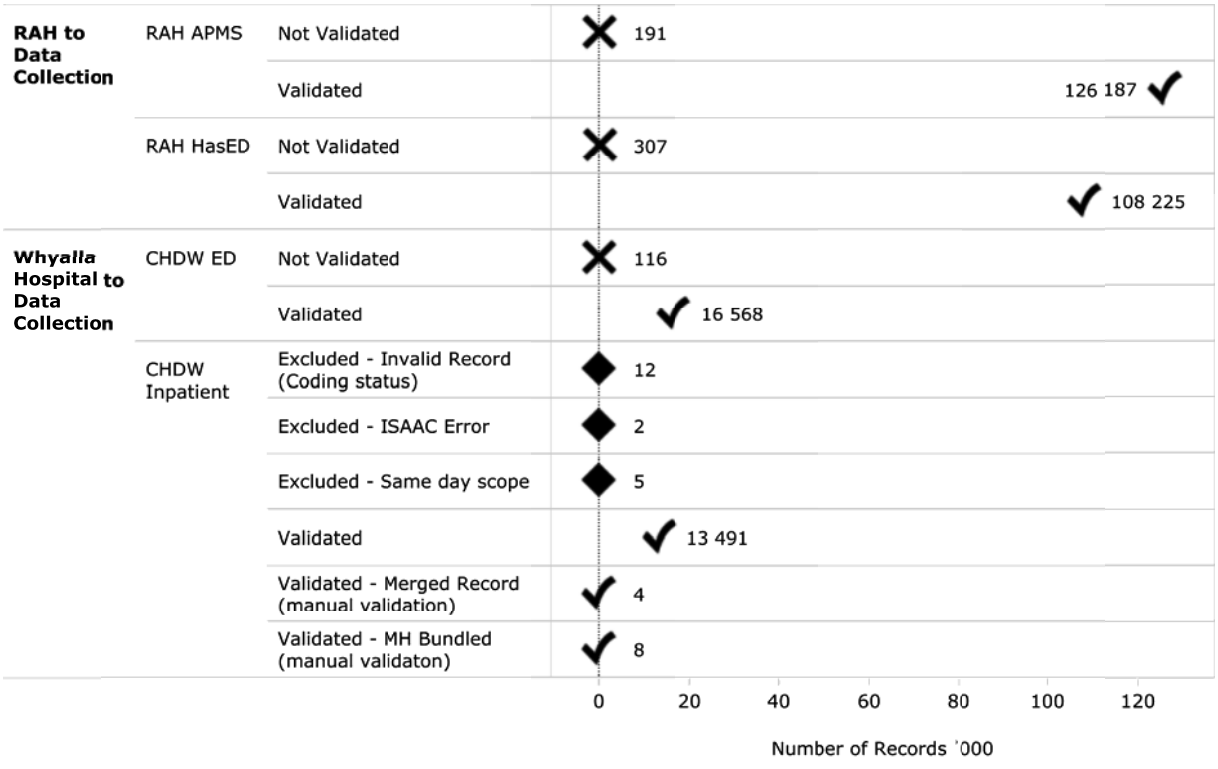
Refer to section 10.8.1 for a diagram of all data flows from the sample hospitals selected to the Commonwealth submissions, and section 10.8.2 for a listing of data obtained from the relevant systems.

The scope of this review did not include:

- validating the accuracy of clinical coding within each record
- assessing the appropriateness of data validation checks applied to SA Health data collections
- validating the accuracy of patient costing allocation data in the National Hospital Cost Data Collection (NHCDC) cost data submission.

10.5 Data validation results

10.5.1 Hospital source systems at the Royal Adelaide Hospital and Whyalla Hospital to data collections (July 2013 to December 2014)



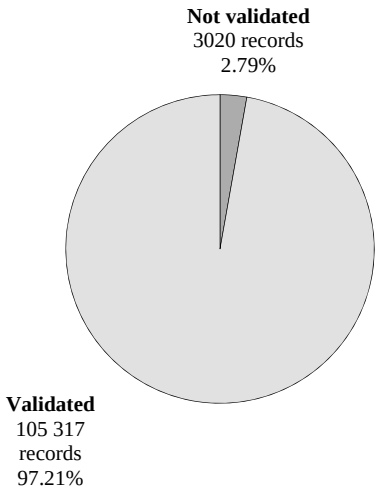
Accuracy of data

As shown above, our validation identified a number of data matching discrepancies:

- 191 records (0.15% of total) in the RAH's patient management system, APMS, could not be matched to records in data collections

- 307 records (0.28% of total) in the RAH's emergency department system could not be matched to records in data collections.

We also identified 3020 records (2.79% of total) in data collections for the sample period that did not match the RAH's emergency department system. These discrepancies were due to subsequent changes to hospital source system data that were not loaded into data collections. Although these mismatches affect the accuracy of data in data collections, we determined that they did not affect the completeness of the Commonwealth submission.



Completeness of data

We identified 116 emergency department records (0.17% of total) from Whyalla Hospital in the CHDW that could not be matched to data collections.

These records were not included in the original data submission for loading to data collections due to the records failing emergency department validation checks. The records have since been adjusted in the hospital source system but have not been loaded into data collections. Accordingly, the records were not included in the Commonwealth submission.

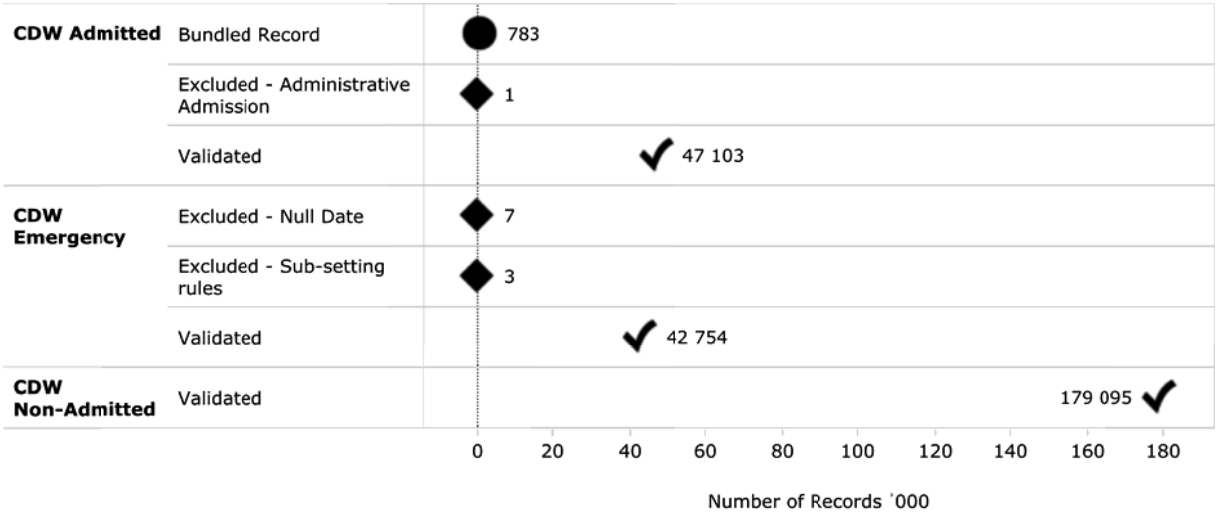
Further comment on these discrepancies in the completeness and accuracy of data is provided in section 10.7.1.

10.5.2 Data collections to corporate data warehouse (July 2013 to December 2014)

All records for the sample period were matched between SA Health data collections and the CDW, with no missing records identified.

10.5.3 Corporate data warehouse to Commonwealth submissions (July to December 2014)

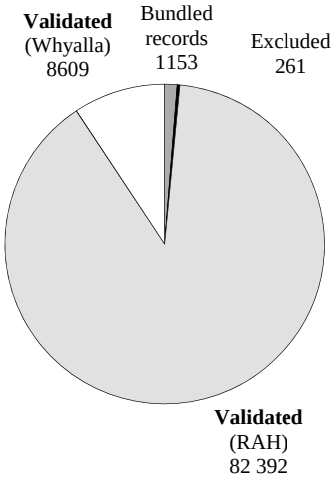
All records for the sample period were matched between the CDW and the Commonwealth submissions, following the application of business rules associated with bundled records, administrative admissions and sub-setting rules.



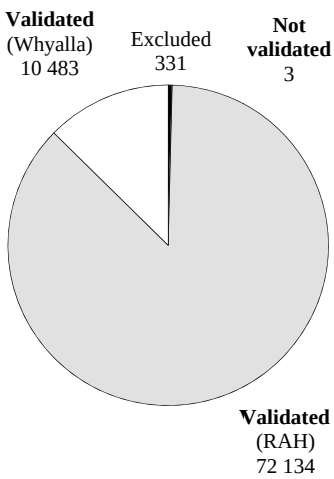
10.5.4 National Hospital Cost Data Collection Cost A submission (July 2013 to June 2014)

We validated data between the CDW and the NHCDC data submission for July 2013 to June 2014. This process identified a number of records that were excluded from the NHCDC submission due to the application of edit checks and business rules. Additionally, three records (0.0036% of total) in CDW emergency data were not loaded to the NHCDC submission due to the timing of the data extract.

CDW (Admitted) to NHCDC Cost A



CDW (Emergency) to NHCDC C



10.6 Detailed findings – review of activity based funding processes

10.6.1 Insufficient documentation of end-to-end activity based funding data flows

SA Health's Data Quality Management Guideline outlines a series of standards and continuous improvement objectives for data quality management across SA Health.

For each SA Health data collection, the Guideline recommends that the responsible teams develop a standardised compliance checking process. Part of this process includes mapping the end-to-end data flows from the initial point of entry at hospital source systems to final targets.

We identified that SA Health has established processes and documentation for the following components of the ABF process:

- hospital admitted data to data collections
- hospital emergency department data to data collections
- admitted and emergency department data collections to the CDW.

Our review also confirmed that data for Commonwealth submissions under the National Health Reform Agreement is generated from sources including data directly extracted from the CDW via database views, as well as data manually prepared in an Access database with data elements combined from a number of sources.

We noted that SA Health does not maintain end-to-end documentation of the data flows from hospital source systems to Commonwealth data submissions. There is no formal documentation detailing the direct inputs to the Commonwealth submission files, data transformation and file outputs.

Risk exposure

Mapping of the end-to-end data flows confirms and documents the data inputs, processing performed, outputs produced, stakeholders involved and technologies used throughout the process. Where data flows are not clearly documented, there is a risk that processes and associated responsibilities will not be clearly understood or followed by SA Health staff.

Recommendation

SA Health should review the ABF process and ensure it meets the requirements of the Data Quality Management Guideline. Specifically, SA Health should develop end-to-end documentation of all relevant data flows and transformations, including data submissions to the Commonwealth.

This documentation should include the sources for all Commonwealth data submissions, transformation or rules applied to data, and the assigned responsibilities of each stage of the ABF process.

Agency response

SA Health responded that, notwithstanding there were no material shortcomings identified in the process itself, end-to-end data flow documentation to capture current practice will be created for this dataset from the receipt of the data by SA Health to the submission to IHPA and NHFB.

The target completion date is March 2016.

10.6.2 No formal review of activity based funding data prior to submission

Patient activity and costing data is submitted to the Commonwealth for ABF via an online submission portal on IHPA's website. Patient activity data is submitted every six months and costing data every 12 months according to a set schedule.

This submission portal contains a series of validation checks to review for known data quality issues. Following the identification of any anomalies, SA Health will adjust data in the source systems or data collections as required and resubmit the data within 14 days.

We noted that there is no formal review or sign-off of ABF data prior to final submission through the online IHPA portal.

Risk exposure

Where data is not formally reviewed and approved prior to final submission, there is a risk that submitted data will be incomplete or inaccurate.

This increases the risk of Commonwealth funding being provided on the basis of incorrect data.

Recommendation

Given the importance of the accuracy of ABF data for the correct allocation of Commonwealth funding, SA Health should implement a formal compliance checking process for submitting ABF data to the Commonwealth.

This includes documenting approval for the data submission and verification of the completeness, consistency and validity of the data to be submitted.

Agency response

SA Health responded that the data submitted to IHPA for its pricing and costing requirements is the same data that is accessed and used by NHFB for State funding and reporting purposes. Data is submitted to IHPA and accessed by NHFB every six months and by the time of submission, has been subjected to numerous validation processes within SA Health and the LHNs. Any exceptions as a result of the validation process are reviewed and, where necessary, rectified so that the data submitted to IHPA is 'fit for purpose'.

SA Health believes that all the appropriate steps and endorsement processes exist but are not formally documented. To this end, a formal document will be developed to ensure that the current review and final sign-off arrangements are evidenced.

The target completion date is March 2016.

10.6.3 Power Performance Manager costing manual in draft status

Hospital patient costing is the process of identifying the inputs used in a hospital and applying the costs of those inputs to the delivery of patient care by various categories. Costed patient activity data is submitted annually to the Commonwealth as part of determining the national efficient price and national efficient cost.

SA Health has implemented the PPM information system to perform patient costing. Hospitals provide data to SA Health on a monthly basis, which is then loaded into PPM along with patient activity data from data collections and cost data from the general ledger. Direct and overhead costs are then allocated to each episode of care.

We reviewed the PPM costing manual, developed by the Funding Models Team. This manual, dated August 2014, is in a draft and has not been formally endorsed by management.

Additionally, SA Health advised that it is currently developing a data requirements plan for costing data submissions. This plan will formally document the data elements that hospitals are required to provide for costing purposes.

Risk exposure

A lack of formally documented and communicated procedures and data requirements increases the risk of an inconsistent approach being applied to patient costing.

Recommendations

SA Health should finalise and approve the PPM costing manual.

Additionally, SA Health should continue to develop the data requirements plan.

Agency response

SA Health responded that the draft costing manual was developed in August 2014, after implementation of the PPM system and in consultation with LHNs. The draft status of the costing manual does not impact the quality of the costing data produced by SA Health.

The costing process has evolved since the draft manual was developed and accordingly a final version of the PPM costing manual will be produced and formally endorsed by management.

SA Health is in the process of developing a patient costing data requirement plan to formalise current arrangements.

The target completion date is March 2016.

10.6.4 Insufficient documentation of outpatient data collection data requirements and the extracting, transforming and loading process

The outpatient data collection records patient-level data on outpatient (non-admitted) attendances for metropolitan hospitals. This data is provided to the Commonwealth for administrative reporting and research purposes but is not presently used for ABF due to known data quality issues.

We reviewed the outpatient data collection technical design specification and the outpatient workflow business rules specification. These documents are in draft and have not been formally endorsed by management.

Inpatient and emergency department collections have detailed manuals describing the required data fields, validation checks and data submission process. SA Health has not yet developed comprehensive documentation of the business-as-usual process for outpatient data collection.

SA Health advised that it is currently developing new patient-level outpatient data extracts. These extracts will be sourced directly from hospital source systems and will remove the need to source data from the Open Architecture Clinical Information System. This process also aims to reduce manual processing associated with extracting data from the CDW for submission to the Commonwealth.

Risk exposure

The absence of formally documented and communicated procedures increases the risk of an inconsistent approach to collecting and validating patient-level outpatient data within outpatient data collection .

Recommendations

To address known data quality issues, SA Health should consider improving the processes associated with the accuracy of patient-level outpatient data. It is recommended that SA Health proceed with the revised approach for data extraction from hospital source systems.

As part of this process, SA Health should ensure that comprehensive documentation is developed and formally endorsed to outline the data requirements, validation checks and data submission process.

Agency response

SA Health responded that this finding relates to patient-level outpatient data, which is not currently utilised for funding purposes by SA Health at the State level, nor does the Commonwealth rely on this for funding allocations. The Commonwealth relies on the submission of aggregate-level data.

While patient-level outpatient data is submitted to IHPA and therefore within the broad remit of this review, this data is not used in any capacity that impacts SA Health. The process of capturing patient-level outpatient data is subject to further improvement efforts and will be addressed with the new approach being developed by SA Health.

Until such time as patient-level outpatient data forms the basis of funding, formal documentation will not be produced.

10.6.5 Clinical coding audit not performed since 2011

Coding teams within LHNs are responsible for reviewing patient activity data in the relevant hospital system. This process aims to ensure that patient activity has been correctly recorded and certain clinical attributes have been accurately coded.

In addition, SA Health undertakes coding and admission practice audits within LHNs. Where appropriate, remedial action is recommended to ensure that LHNs are complying with agreed coding definitions and standards.

We obtained and reviewed the 2010-11 clinical coding audit state-wide summary report and noted that this was the most recent audit performed.

As a compensating control, SA Health advised that it has implemented the Performance Indicators for Coding Quality (PICQ) software. This software is designed to identify records in admitted patient morbidity data sets that may be incorrectly coded based on Australian coding standards. SA Health advised that monthly reports from PICQ are being provided to hospital coding managers with requests that they correct certain specified errors.

Risk exposure

Where clinical coding audits are not regularly performed, there is a risk that critical clinical attributes are not being sufficiently reviewed. This increases the potential for inaccurate patient activity data being submitted to the Commonwealth, which may have funding implications.

Recommendation

SA Health should schedule a clinical coding audit within the next 12 months.

SA Health should conduct these audits on a regular basis (12-24 months) to ensure the accuracy of patient activity and clinical attributes.

Agency response

SA Health advised that although the last coding audit was conducted in 2011, in 2012 an admissions practice audit was conducted in lieu of a coding audit.

Since the last audit, SA Health has also expanded the role of one of the Health Information Managers to cover coding education responsibilities.

There is significant cost in undertaking a coding audit and there has been no recognised deficiency in this area that would suggest the need arises. However, in promoting quality assurance of coded data, SA Health has commenced using the PICQ software. This software is designed to identify patient episodes that may be incorrectly coded.

Monthly reports are provided by hospital coding managers with requests that 'fatal' and 'warning 1' errors identified by the software are corrected.

SA Health will continue to monitor the effectiveness of the PICQ software in identifying coding problems and, if required, will undertake a coding audit in the coming years.

10.7 Detailed findings – testing of activity based funding data

10.7.1 Emergency department data validation errors and extracting, transforming and loading process

Finding 1 – Emergency department data load process does not capture record corrections

We reviewed the process of submitting data to inpatient and emergency department data collections from hospital source systems.

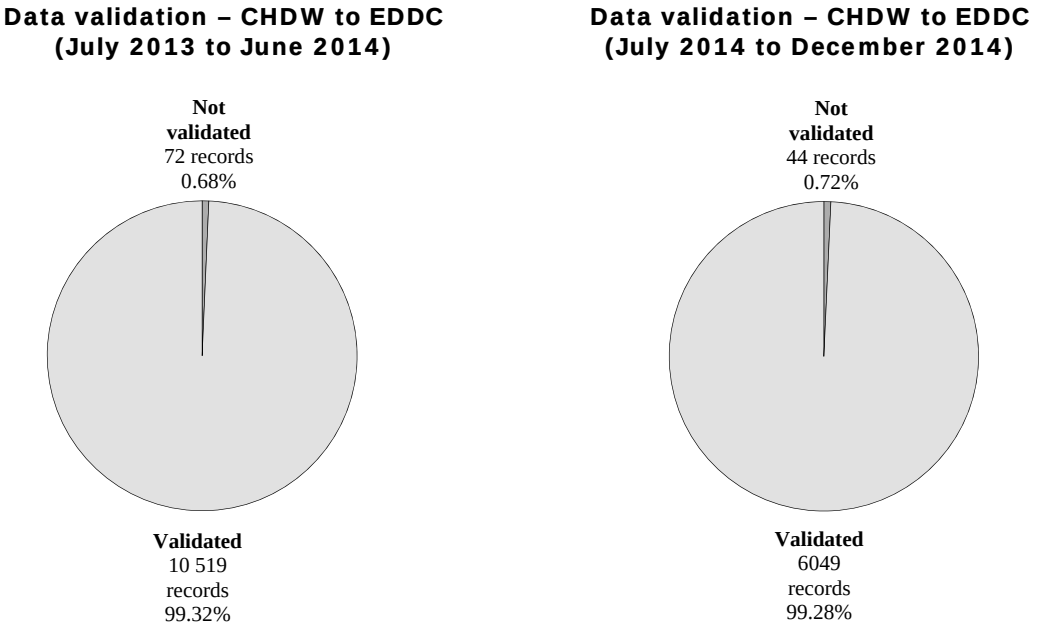
Hospital patient activity data is extracted from source systems and submitted to the SA Health Information Assembly Unit on a monthly basis via email. Inpatient and emergency department data submissions are submitted on the same day each month and contain data for the previous month only.

Where records are subsequently changed in source systems, these need to be manually submitted to the Information Assembly Unit for data correction in the emergency department data collections system. Correction requests can either be submitted to the Information Assembly Unit through additional data extract or through a corrections form.

We noted that where corrections are not submitted to the Information Assembly Unit in a timely manner, there will be a discrepancy between the source system and the corporate data collection.

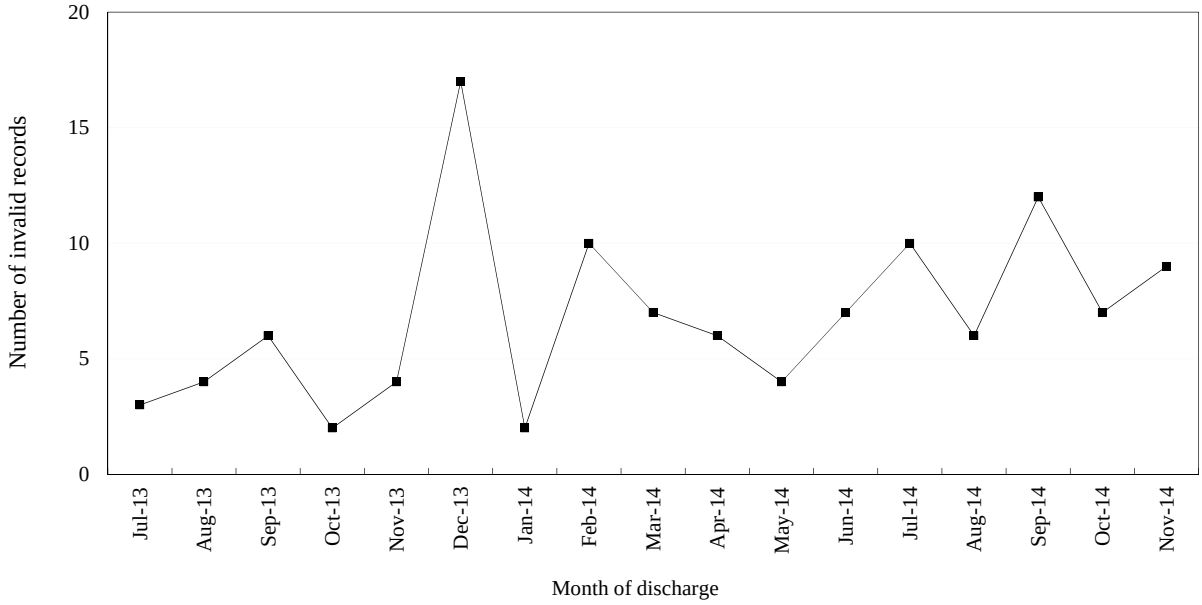
Finding 2 – Emergency department data matching exceptions identified – Whyalla Hospital

We reviewed data integrity between Whyalla Hospital data in the CHDW and the emergency department data collection (EDDC) for the sample period. This process identified 116 records (0.7% of total) that could not be matched between the systems:



SA Health advised that these records were not included in the data submission for loading in the emergency department data collection due to the records failing emergency department validation checks at the time of preparing the extract. These records have since been adjusted in the source system (Chiron) but have not yet been loaded in the emergency department data collection as they were not included in subsequent monthly extracts. This is due to the month-to-month nature of processing.

Additionally, SA Health advised that it is aware of delays in record processing at the Whyalla Hospital of up to three weeks due to insufficient resources, particularly in December 2013. This was confirmed in our review through the analysis of invalid/mismatched records by month:



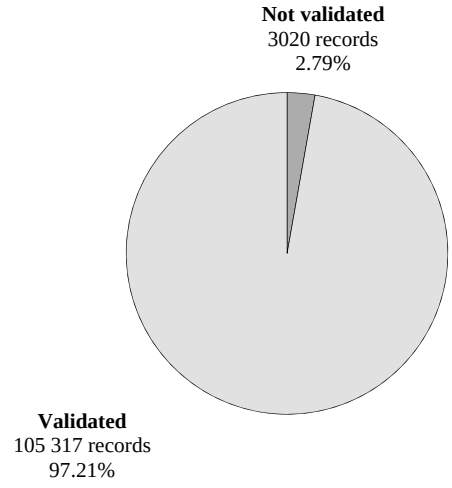
SA Health advised it is considering adjusting the current data load process to include year-to-date extracts of patient activity data for both metropolitan and country public hospitals.

Finding 3 – Emergency department data matching exceptions identified – RAH

We reviewed data integrity between the RAH Emergency Department Information System (EDIS) and the emergency department data collection. This process confirmed the completeness of RAH emergency department data in the emergency department data collection by verifying the number of records in each system.

In order to verify the accuracy and consistency of data in the emergency department data collection, we attempted to match all RAH EDIS records to the emergency department data collection using a composite key of departure date/time, medical record number and hospital code.

This process identified that 3020 emergency department records from data collection could not be matched back to EDIS. Additionally, 307 records could not be matched from EDIS to data collection.



SA Health advised that these discrepancies are due to changes in departure status codes, departure times and triage times in these records subsequent to the monthly emergency department data collection extract being submitted.

Risk exposure

Where invalid records in source systems have been subsequently corrected and have not been loaded to SA Health data collections, funding may not be provided for these episodes of care.

Where discrepancies exist between key data fields in hospital emergency department systems and SA Health data collections, the ability to assess data quality may be limited as data is transferred through the various systems and submitted for ABF.

Although the completeness of emergency department data in SA Health data collections was verified in this instance, the discrepancies identified may limit the ability for SA Health to confirm the consistency, accuracy and validity of data in data collections.

Recommendations

To address the above findings, SA Health should:

- adjust data collection processes to collect year-to-date data from hospital source systems, in order to reduce discrepancies caused by subsequent record corrections
- consider performing regular, documented compliance checks between hospital source systems and corporate data collections to assess the completeness, consistency, accuracy and validity of data in the emergency department data collection
- ensure appropriate resources are allocated in hospitals to enable records to be processed in a timely manner.

Agency response

SA Health responded that these findings relate to mismatches in data items within records in the hospital source system and the corporate data collection. The findings do not relate to missing records. The data submitted to the Commonwealth was complete.

There were 116 records identified at Whyalla Hospital and 3020 records at the RAH that could not be matched due to changes in data items. The vast majority of the records impacted had changes in times and this data item has no impact on the funding calculation.

When there are significant changes to data, hospitals are required to communicate with SA Health that a resubmission of data is required, as SA Health is not able to identify when this is necessary.

However, to mitigate this issue in future, SA Health will move from a monthly processing cycle to a year-to-date processing cycle. This will pick up the changes made by hospitals on an ongoing basis.

The target completion date is March 2016.

10.7.2 Medical record number mismatch – RAH admitted records

Assessment of the consistency and accuracy of data between the RAH's patient management system, APMS, and SA Health data collections identified that 191 records in APMS did not match records in data collections.

Similarly, 172 records for RAH admitted patient activity in data collections could not be matched to records in APMS.

SA Health advised that this discrepancy was caused by double registration of patients. This occurs when a patient is admitted under a new unique medical record number before determining that they have a pre-existing medical record number. These records were subsequently adjusted in APMS to reflect the patient's pre-existing medical record number.

Notification of these changes was not provided by RAH staff to SA Health for manual correction in data collections. Additionally, due to the month-to-month nature of data submissions, the corrections were not included in a subsequent monthly extract.

Risk exposure

Where discrepancies exist between key data fields in the patient administration systems and data collections, the ability to assess data quality may be limited as data is transferred through the various systems and submitted for ABF.

We acknowledge that, although the data is not consistent between systems, the completeness of data is not affected by the record number mismatch.

Recommendation

SA Health should review the exceptions identified and ensure that medical record numbers are correctly updated in data collections.

As noted above, SA Health should adjust the relevant data collection process to load year-to-date data on a monthly basis. This would reduce the incidence of discrepancies arising from corrected records.

Agency response

SA Health responded that this issue is similar to the findings under section 10.7.1 above, where retrospective changes in the source system have resulted in an immaterial number of records not being able to be matched to corporate data collections. The issue relates to a mismatch of data items within records (medical record number) and not the completeness of the data file submitted to the Commonwealth.

A temporary set of factors at the RAH caused this issue, which has since been amended. This finding has no impact on funding.

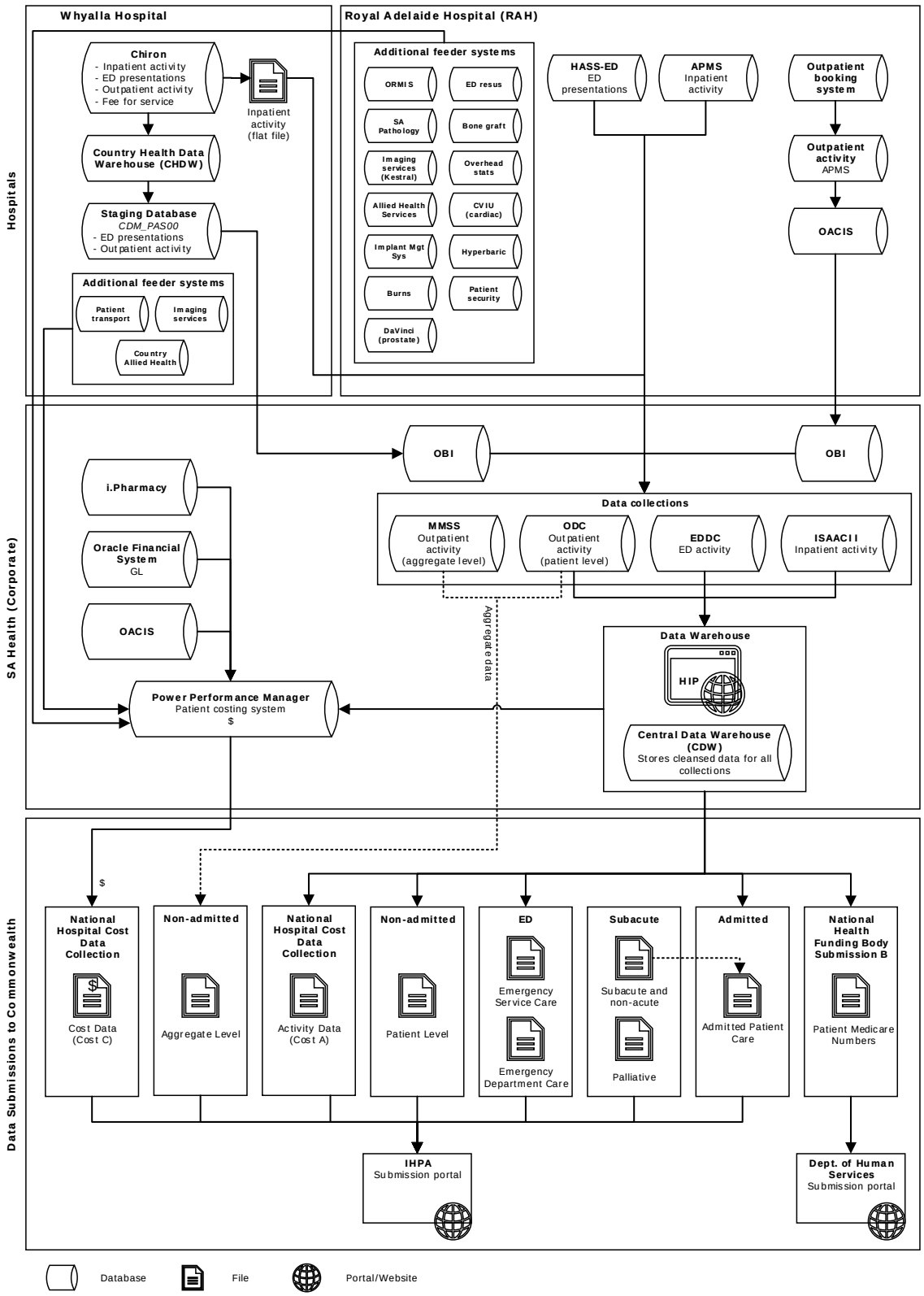
The recommendation for the loading of a year-to-date file to limit the potential for this type of issue to occur in the future is not a practical recommendation, as the size of year-to-date files would be problematic from a processing perspective. Hospitals already routinely provide additions and corrections to records relating to previous months to SA Health. These records are subsequently loaded into the central data collection.

Existing processes are sufficient to address changes to data items and completeness in data capture.

10.8 Systems and data

10.8.1 Activity Based Funding systems and data flows

The following diagram shows the relevant ABF data flows for the sample hospital sites reviewed, as well as SA Health corporate data collections.



10.8.2 Data obtained from SA Health

As part of this review, the following datasets were obtained from SA Health:

Source	System	Dataset	Date range
RAH	APMS	Inpatient	Jul 2013 to Dec 2014
	EDIS	Emergency department presentations	Jul 2013 to Dec 2014
	Outpatient booking system	Outpatient	Jul 2013 to Dec 2014
	Client Management Engine	Outpatient	Jul 2013 to Dec 2014
Whyalla	Chiron	Inpatient/Emergency department/Outpatient	Jul 2013 to Dec 2014
	CHDW	Inpatient/Emergency department/Outpatient	Jul 2013 to Dec 2014
SA Health	ISAAC	Inpatient	Jul 2013 to Dec 2014
	EDDC	Emergency department presentations	Jul 2013 to Dec 2014
	ODC	Outpatient	Jul 2013 to Dec 2014
	CDW (Admitted)	Inpatient	Jul 2013 to Dec 2014
	CDW (Emergency)	Emergency department presentations	Jul 2013 to Dec 2014
	CDW (Non-admitted)	Outpatient	Jul 2013 to Dec 2014
Commonwealth submissions	**ABF submission (six-monthly)**		
	Admitted Patient Care (APC)	Inpatient	Jul 2014 to Dec 2014
	Emergency Department Care	Emergency department presentations	Jul 2014 to Dec 2014
	Non-admitted (Patient)	Outpatient (patient level)	Jul 2014 to Dec 2014
	Non-admitted (Aggregate)	Outpatient (aggregate level)	Jul 2014 to Dec 2014
	NHFB Submission B (Medicare numbers)	Inpatient, emergency department presentations and outpatients	Jul 2014 to Dec 2014
	Costing submission (annually)		
	NHCDC Cost A (RAH)	Inpatient and emergency department presentations	Jul 2013 to June 2014
	NHCDC Cost A (Whyalla)	Inpatient and emergency department presentations	Jul 2013 to June 2014
	NHCDC Cost C (RAH)	Inpatient and emergency department presentations	Jul 2013 to June 2014
	NHCDC Cost C (Whyalla)	Inpatient and emergency department presentations	Jul 2013 to June 2014

10.9 Concluding comment

The accuracy and completeness of ABF data is important as it is used to determine the funding for public hospital services based on the number of services provided to patients and the price for delivering those services.

Our review examined certain aspects of data integrity relating to activity data provided to the Commonwealth for ABF under the National Health Reform Agreement. From our sample tested, we concluded that:

- ABF data integrity controls are operating effectively for admitted and emergency department activity data
- data integrity controls associated with non-admitted data in the Commonwealth submission files were operating effectively.

We identified some data matching discrepancies and certain shortcomings in need of management attention. In response to our review findings SA Health responded positively to our recommendations, with all remedial action to be completed by March 2016.

11 Enterprise Pathology Laboratory Information System

11.1 Introduction

EPLIS is planned to provide SA Health with a consolidated laboratory information system that provides functionality across all pathology disciplines.

EPLIS is expected to enable SA Pathology[8] to standardise end-to-end laboratory workflows to deliver increased efficiencies and service effectiveness. This includes improved tracking and timely reporting capabilities through electronic visibility of requests, reports and results across the entire organisation.

11.2 Audit objective and approach

The objective of this review was to obtain an understanding of the current EPLIS Program (the program) implementation status, budget and expenditure to date, key risks and the system's impact and readiness for the new RAH. This has involved relating with EPLIS and new RAH representatives and reviewing:

- the EPLIS business case
- new RAH EPLIS strategic planning documentation
- program status updates, board reports and minutes
- SA Health's eHSC meeting minutes
- SA Health's Risk Management and Audit Committee briefing notes
- Cabinet submissions.

11.3 Key findings

This review has noted the following key EPLIS risks, which are explained further in sections 11.12 and 11.13.

Key program risks and audit concerns potentially impacting the new RAH:

- program delays have occurred

[8] SA Pathology is the state-wide pathology service provider for the public and private health sector.

- lack of staff familiarity with EPLIS and associated workflows
- integration challenges potentially resulting in delays and workarounds
- procurement of the laboratory instruments and robotic tracks is yet to be finalised
- deficiencies in system contingency plans.

Key program risks and audit concerns:

- EPLIS budget and contingency may be insufficient to finalise all required program activity
- financial reporting and governance requires improvement
- lack of tracking and potential delays of program benefits realisation
- ongoing resource challenges exist
- pathology results reporting challenges to maintain private revenue
- program activities continued without a formally approved business case.

11.4 Program background and drivers

SA Pathology provides pathology services to all State public metropolitan and regional hospitals and a number of other private health providers.

In addition, SA Pathology has approximately a 37% share of all community pathology testing funded by Medicare in South Australia. This private testing helps SA Pathology to deliver current laboratory services across South Australia's public hospitals, especially in country areas.

In the 12 month period ending June 2013, SA Pathology completed 7.3 million tests.[9]

Despite this capacity, the current legacy pathology systems are experiencing problems and are not fit for purpose for sites such as the new RAH. The current laboratory information system, Centricity Cirdan Ultra (Ultra), and most of the peripheral systems are aged, have reached or are reaching end-of-life, and are increasingly problematic and costly to support. The two software versions of Ultra implemented across SA Heath sites are not compatible with each other and are increasingly prone to failures. Significant downtime can impact on service delivery to hospitals and emergency departments.

A key recommendation from an independent consultant review performed in 2008 of the SA Pathology environment was to replace its laboratory information system. The review recommended that, concurrent with the formation of a single state-wide pathology service, SA Pathology also needed to implement a common laboratory information system and a single patient database. Other more recent external and internal reports have supported the criticality of implementing an EPLIS.

In particular, the current laboratory information system used at the existing RAH is not fully integrated. Due to system limitations it cannot be expanded to include the addition of an onsite laboratory planned for the new RAH. The current laboratory information system

[9] Details taken from 'SA Health Enterprise Pathology Laboratory Information System (EPLIS) Final Business Case', Version 1.0, dated 12 May 2015.

cannot currently facilitate the hospital's reduced hardcopy paper workflow design through interfaced computer systems. It has also not been designed to receive inbound electronic messages from EPAS, the Open Architecture Clinical Information System or external medical practitioner software.

11.5 EPLIS tender and business case

In response to the above issues, SA Health introduced the program to replace the existing laboratory information system and associated work practices with a single modern IT solution. The aim was to integrate SA Pathology laboratories and standardise laboratory workflows.

In 2012, the State Budget Papers included an announcement of the procurement and implementation of an EPLIS. Following this announcement, the eHSC approved funding for the completion of the EPLIS feasibility stage.[10]

SA Health conducted a tender process and in November 2013 selected and approved Cerner Corporation Pty Ltd (Cerner) as the preferred EPLIS supplier. Contract negotiations with Cerner commenced in January 2014.

In September 2014, Cabinet approved the program's proposal submission and funding to enter into a software vendor contract and for the implementation of an EPLIS. The Cerner EPLIS solution is a commercial off-the-shelf product, comprising a number of software modules known as Cerner's Millennium Laboratory Information System Suite (Millennium).

Millennium integrated specialised modules include: Anatomical Pathology; Molecular Genetics; Microbiology and Infectious Diseases; Transfusion Medicine; and Australian Medicare-compliant billing. The package aims to provide inter-operability, visibility and reporting requirements across the SA Pathology business and is expected to be used by over 1400 laboratory staff.

The original EPLIS business case was developed and presented to the eHSC in December 2014. The business case, however, was not approved initially, with the eHSC requesting it be independently reviewed and revised. This has since occurred, with approval by the eHSC occurring in late May 2015.

11.6 EPLIS expected benefits

The EPLIS business case proposed that by mid-2017, SA Pathology will have a single state-wide EPLIS that improves healthcare outcomes for patients and harnesses new technology. It is planned to deliver the following benefits:

- a single system connecting all laboratories across metropolitan and regional South Australia
- standardised and improved workflow processes

[10] The original program scope identified in the 2012 preliminary business case expected that the EPLIS solution would be implemented into the existing RAH prior to the new RAH being finalised. As a consequence the new RAH was not taken into consideration in the original project planning or budget and was subsequently added to the program scope without the provision of any additional funding.

- integrated information and a consolidation of systems
- timely access to critical pathology diagnostic information.

The initiative to implement an EPLIS involves replacing most of the existing laboratory information systems. This includes replacing Ultra and approximately 30 other smaller IT systems, some in-house, that are required to support or supplement Ultra in the delivery of laboratory functionality.

It is anticipated this will allow for future changes in health system design and delivery and enable SA Pathology to meet increases in service demands without increasing its cost drivers. In addition, it should provide the ability to adopt continuing technological advances in information systems and pathology analyser automation, and provide improved business informatics for laboratory test ordering.

Reducing the number of laboratory supporting systems is also expected to provide certain IT efficiencies through reduced ongoing maintenance support requirements and system change requests.

11.7 EPLIS rollout schedule

Deployment of EPLIS is planned for a number of directorates and sites within SA Pathology, including eight metropolitan hospitals, 11 regional laboratories and 65 collection centres (38 metropolitan and 27 regional). The most recent rollout schedule was aligned to meet the required new RAH milestone dates.

Cerner and SA Health finished negotiating amendments to the EPLIS contract schedule in late November 2014.

The proposed rollout plan in the approved May 2015 business case included initial implementation at the new RAH and laboratories located on Frome Road, Adelaide by April 2016. A number of metropolitan sites were scheduled to follow, including:

- Women's and Children's Hospital – July 2016
- The Queen Elizabeth Hospital – July 2016
- Flinders Medical Centre – August 2016
- Repatriation General Hospital – August 2016
- Noarlunga Hospital – August 2016
- Lyell McEwin Hospital – October 2016
- Modbury Hospital – October 2016.

Selected regional sites were also planned for implementation, commencing in October 2016.

Subsequent to the May 2015 business case, a September 2015 Cabinet submission and negotiation settlement occurred between the Minister for Health and SAHP.[11] Following this negotiation settlement, the Government announced a delay to the opening of the new RAH. It is now expected to open by November 2016.

[11] The new RAH program is being delivered under a Public Private Partnership agreement with SAHP. SAHP is responsible for the design and construction of the new hospital facility.

At the time of this Report, the program had yet to determine the implications of this delay to the overall EPLIS rollout plan and the associated costs. However, subsequent discussions with program representatives have tentatively indicated that EPLIS may now be rolled out to another site before the new RAH.

11.8 Development of the EPLIS rollout and implementation approach

The planned deployment of the EPLIS solution involves certain configurations to meet SA Health's requirements, however no underlying changes are planned to be made to the functionality or operation of the software. As part of the program, new workflows will be developed and deployed across SA Pathology to meet the standard system functionality of the EPLIS solution. This will require end users to adapt to the way the product operates. As such, the program will run significant change management activities in parallel to providing the new system.

The May 2015 approved EPLIS business case noted three phases for the program:

- Phase 1 – services for detailed planning, including solution and technical design. This is to produce a detailed project plan for implementation and the information necessary for SA Health to complete a final business case
- Phase 2 – incorporates the licensing of software and the professional services to install, configure and implement the software and site activation following acceptance testing and end-user training by SA Health
- Phase 3 – provides for ongoing software maintenance and support.

As previously mentioned, the system is required to be configured to interface with certain SA Government systems and external entities to import and export information. This includes the functionality for receiving paper or electronic pathology requests from sources including other laboratories, commercial firms, other government departments (eg prisons), private hospitals, clinics and practices. EPLIS is also required to provide reports to various government health registries in either electronic or paper format.

These information flows require EPLIS to interface with different technologies such as pathology instruments and other software. Notably, providing the ability to send and receive electronic orders for pathology testing and results. This includes accepting electronic orders from EPAS[12] and other external sources and returning electronic results in a report format. EPLIS will also provide the capability for potential future integration with the Personally Controlled Electronic Health Record.

We were advised that the program is planning to develop a business-as-usual support structure for SA Pathology for handover on program completion. The structure will consist of ICT and clinical staff. Training is planned to be provided prior to the first site implementation.

In relation to the legacy system, SA Health expects Ultra will run in parallel with EPLIS following implementation at the new RAH (or the alternative first rollout site). Decommissioning of the legacy system was not originally expected to occur until May 2017, when EPLIS is implemented at all in-scope sites and a complete legacy data archiving strategy had been established. Given the potential changes to the EPLIS rollout plan this expected decommissioning date may now be altered.

[12] The EPAS Program will be responsible for developing and conducting training for clinicians within hospitals, including creating pathology requests and reading and interpret pathology results within EPAS.

11.9 Initial EPLIS budget

A budget of $30.365 million was announced in the State Budget Papers in May 2012. This budget was to procure and implement EPLIS, of which $1.89 million was approved by the eHSC to complete the feasibility stage.[13]

In September 2014, Cabinet approved the following program funding:

- $11.4 million to execute the contract and incur expenditure with the system vendor, and provide licensed software and services to support the implementation of an EPLIS over a five year period (2014-15 to 2018-19)

- approval for a re-profile and minor reclassification of existing project expenditure authority. This is to reflect the revised project expenditure cash flow required under the contract, including a further carryover of $139 000 from 2013-14 to 2014-15

- approval for authority to incur expenditure of $19.9 million over the period (2014-15 to 2016-17) from within existing SA Health budget allocations to fund the non-software vendor components of the program, within the total $30.365 million.

11.10 Current EPLIS budget

The EPLIS business case provided additional information relating to the program funding sources, including:

- capital costs of $30.365 million allocated to the program, which was approved by Cabinet in September 2014. Of this, $788 000 was reallocated to the SA Pathology billing system project to deliver the billing system requirements of EPLIS, for a net budget of $29.577 million

- operational expenditure of $7.137 million from the SA Pathology budget over five years. This funding is for additional infrastructure support and maintenance costs of EPLIS as well as supporting the legacy systems before they are decommissioned.

The business case also noted that SA Pathology would be required to identify expenditure offsets to absorb the increased recurrent costs, as there will be no budget supplementation. At the time of our review, the structure of how the operating budget will be monitored had not been determined.

Before the recent new RAH opening delay was announced, SA Health originally expected approximately 77% of the overall project budget to be expended by the time the first site rollout (new RAH) was completed. This expenditure included approximately $9.8 million in software and hardware costs and $7 million in vendor services, of which $5.6 million is payable on milestones up to and including the first site activation. SA Health also advised that the majority of the expenditure was attributed to solution implementation and was not proportional to the site-by-site rollout.

At the time of this Report, however, the original expenditure estimations were being reassessed by the program due to the new RAH opening delay.

[13] Details taken from 'SA Health Enterprise Pathology Laboratory Information System (EPLIS) Final Business Case', Version 1.0, dated 12 May 2015.

We consider that cost pressures remain to implement a fully functional and operational EPLIS. These cost pressures are further intensified with the new RAH opening delay and the potential impact to the rollout plan.

We also noted that contingency has been reserved for additional program resources and vendor travel arrangements and there are minimal contingency funds for the remainder of the program. A number of additional supporting activities also remain outstanding which are further discussed in section 11.13.1.

A summary of the program budget and expenditure as of 31 August 2015 is outlined in the below table.[14]

	Original approved budget (September 2014) $'000	Revised approved budget (May 2015 business case) $'000	Expenditure to date $'000	Remaining budget $'000
Phase 1 – program capital and operation expenditure	1 941	1 357	1 357	0
Phase 2 – program capital and operation expenditure	24 080	[15]26 789	6 804	19 985
Contingency	3 556	1 431	0	[16]1 431
Recurrent expenditure – SA Pathology	7 137	7 137	[17]0	7 137
Total budget (ex GST)	**36 714**	**36 714**	**8 161**	**28 553**

11.11 Detailed findings

The May 2015 EPLIS business case states that program governance is based on governance principles and guidelines set out by the eHealth Program Management Office. The EPLIS Program Board (the EPLIS Board) provides overall program responsibility, including approval of deliverables. Under this arrangement the eHSC provides program oversight and the program Operations Control Team acts as an advisory group to the program.

Regarding the implementation of EPLIS at the new RAH, additional new RAH Program governance arrangements have been established. These include a dedicated new RAH EPLIS ICT Project, which has been working closely with key stakeholders including the new RAH EPLIS Commissioning Manager, the program, SA Pathology and the new RAH ICT Program. Governance structures, including endorsement and approval channels, have also been established through the new RAH Operations Board and the new RAH Steering Committee.

The program has been presented with certain challenges, including scope adjustments that the various governance structures are managing. The July 2015 EPLIS risk register raised 18 active risks, of which eight were considered high and 10 moderate.

Notable risks impacting the program and our related concerns, particularly related to the delayed implementation at the new RAH, are discussed further below.

---

[14] The expenditure to date figures were extracted from SA Health's Oracle Corporate System ledger, which has not been audited by the Auditor-General.

[15] This amount includes both the remainder of Phase 1 expenditure and partial transfer of allocated contingency funding.

[16] For further information related to contingency funding refer to section 11.13.1.

[17] SA Health advised that a minimal amount of the budget has been spent to date (approximately $100 000).

11.12 Detailed findings – potentially impacting the new Royal Adelaide Hospital

11.12.1 Program delays have occurred

Implementation of EPLIS is a significant and complex program. Timely implementation of EPLIS is also essential for establishing an onsite laboratory at the new RAH.

We noted, however, that the project schedule and estimated completion date has been extended throughout the program's lifecycle. This is historically due to program interruptions caused by delays in governance approvals and portions of time when the program was put on hold. In addition the original implementation schedule was compressed and later considered logistically not feasible.

SA Health has indicated that other factors have also contributed to program delays and resolution of problems, including:

- program responsibilities and methods of engagement had initially not been formally established between SA Health IT and SA Pathology for an integrated approach to the delivery and ongoing support of EPLIS
- lack of project ownership clarity had originally restricted project communication and assignment of accountability, responsibilities and decision-making
- initial poor communication and understanding of the SA Health processes and environment existed between Cerner (software vendor) and eHealth Systems[18]
- software licencing procurement challenges resulting in a six week program delay to the implementation of the EPLIS development environment.

SA Health advised that these issues have since been addressed.

At the time of our review, program activities included software configuration, interface design and development, instrument interface design, infrastructure installation and commissioning, software installation, disaster recovery planning and data migration design.

Risk exposure

We note that the recent delay in the new RAH opening will provide additional time for the program to complete all required activities, thus reducing this risk.

Despite this additional time, further program delays may still lead to compromises in the scope and quality of delivery to meet the adjusted new RAH deadlines. This has the potential to result in a sub-optimal solution on initial operation at the new RAH and/or delayed patient pathology services being offered.

Recommendations

The EPLIS and new RAH Programs, with the assistance of the software vendor, should continue to update the program implementation plan to take into consideration the adjusted new RAH deadlines.

[18] eHealth Systems is an internal business unit of SA Health.

Strict program governance should continue to be applied to this revised program schedule.

The EPLIS and new RAH Programs should continue frequent communications with a complete understanding and agreement of all required milestone dates of the new RAH.

New EPLIS scope change requests should be strictly controlled.

Agency response

SA Health responded that EPLIS will continue to operate as per the recommendations. The schedule is monitored and reviewed monthly by the EPLIS Board. Exception reports regarding any material deviations to the program schedule and/or scope are prepared as required and are endorsed by the EPLIS Board and approved by the eHSC.

11.12.2 Lack of staff familiarity with EPLIS and associated workflows

In addition to the change requirement from implementing EPAS,[19] the planned implementation of EPLIS direct to the new RAH increases the extent of change that existing RAH and SA Pathology staff will be faced with in transitioning to the new hospital environment.

The program has acknowledged the large amount of business change that will be developed and deployed across SA Pathology to meet the required new system workflow practices. Significant change management activities are also required to run parallel to the provision of the new system.

Risk exposure

The risk of staff not being suitability competent in using EPLIS and the associated new workflow practices is an issue for all new implementation sites, including the new RAH.

Staff transitioning to the new RAH also have a number of additional pressures independent of EPLIS. These include commencing work in a new physical environment and other associated changes to work practices such as EPAS.

Recommendations

SA Health has advised that a number of strategies are being applied to mitigate the risk of using a new system and process workflows within the new hospital. We recommend these strategies continue to be diligently pursued. These notably include:

- maintaining strong governance arrangements and structure
- requirements analysis and approval process, identification of a future state operational model, walkthroughs of future workflows, user acceptance testing and dedicated site activation teams

[19] For details on the EPAS implementation and the potential impact to the new RAH refer to the Auditor-General's Supplementary Report for the year ended 30 June 2014 'Health ICT systems and the Camden Park distribution centre: June 2015'.

- a detailed business change management strategy, including communication and training plans, ensuring the provision of EPLIS 'change champions' and a locked down system configuration.

We also recommend SA Health ensure its business change management strategy effectively enables staff to engage in a timely manner and clearly understand the need for business change. Potential staff resistance or apprehension should be minimised through proactive planning.

Agency response

SA Health will continue with these strategies as recommended, including maintaining robust governance.

The EPLIS Communications and Stakeholder Management Strategy and the Testing Strategy have now been approved by the EPLIS Board. Other strategy documents such as the Change Management Strategy and the Training Strategy will be developed over the coming months.

The target completion date is November 2015.

11.12.3 Integration challenges potentially resulting in delays and workarounds

Delivery of planned functionality at the new RAH is reliant on the program performing activities for certain key interfaces to be operational. Key interfaces include:

- EPAS – expected to provide electronic pathology ordering and results viewing. It is also expected that the SA Pathology standard orders and results catalogue will be matched across EPAS and EPLIS
- Enterprise Master Patient Index – expected to provide individual patient health identifiers
- PowerHealth Billing & Revenue Collection (PBRC) system – expected to provide pathology billing functionality
- Oracle Corporate System – expected to feed pathology financial information to the SA Health general ledger
- Medical Device Interface – expected instrument interfaces with the EPLIS software.

Much of the integration requirements are expected to be provided through SA Health's Health Integration Broker.

At the time of this Report, the program had not yet made progress in relation to a number of these key interfaces, with the potential to impact functionality on initial operation at the new RAH.

Key interface challenges are discussed in more detail in sections 11.12.3.1 and 11.12.3.2, with associated risks and recommendations.

Risk exposure

Despite the new RAH opening being delayed, providing the program with additional time, there are still a number of integration challenges with other systems that need to be addressed prior to any SOC testing at the new RAH.

Recommendations

The program should place priority on developing required interfaces with other SA Health and third party systems to facilitate key information flows.

The program's revised implementation schedule should take into consideration system integration requirements, to enable all integration activity to be completed before the adjusted SOC testing deadline.

Agency response

SA Health responded that the schedule review being undertaken by the EPLIS Program team will take into account the opportunity to bring EPLIS integration activity into the SOC testing time frames where possible, within the constraints imposed by external dependencies (including the EPAS Program and procurement of new instrumentation for the new RAH laboratories).

The schedule review will also place priority on required interfaces with other SA Health and third party systems.

The target completion date is November 2015.

11.12.3.1 Electronic pathology ordering integration with EPAS is yet to be finalised

The program strategy for implementation at the new RAH is heavily reliant on an electronic ordering and reporting solution. SA Health advised that pathology orders from EPAS will be accepted by EPLIS, with results returned electronically. The aim is to create increased efficiency of work processes, and reduce manual data entry, manual handling, associated errors and report turnaround times for referring clinicians.

For electronic ordering functionality to be operational, development work is required within both EPAS and EPLIS to match the SA Pathology order and results catalogue.

Although the program originally scheduled EPAS integration testing to be completed in May 2015, at the time of our review Cerner was still developing the SA Pathology order and results catalogue in EPLIS. This catalogue is now expected to be finalised by mid-October 2015.

On completion, the order and results catalogue will be provided to the EPAS Program for integration into the pathology order and results interface. Until completion, the EPAS Program's associated development costs and timelines for completion remain outstanding.

Prior to the recent new RAH opening delay being announced, we noted that the EPAS Program originally underestimated the time and effort required to perform all associated

development, testing and staff training in readiness for initial operation at the new RAH. Integration testing of the electronic ordering interface between EPAS and EPLIS was originally scheduled to commence at the end of November 2015 and be completed by February 2016.

Given the delays, SA Health is currently working on a contingency option should electronic pathology ordering not be available at the new RAH.

The preferred contingency involves performing manual workarounds using paper forms. Our review of the EPLIS Board minutes, however, noted that representatives indicated that there may not be enough ancillary staff to support this option. We noted that additional work was required on this contingency option and was requested to be presented back to the EPLIS Board at a later date. At the time of this Report, this was in progress.

As discussed in section 11.13.1, SA Health has not yet determined the source of the funding required for pathology electronic ordering at the new RAH.

Risk exposure

As mentioned, the unavailability of a suitable electronic ordering solution may result in manual pathology ordering through paper request forms as a contingency, supported by printers and barcode readers.

No interface with EPAS increases the risk of not being able to appropriately control costs through electronic pathology ordering using the standard test catalogue order sets.

Potential delays may occur in the realisation of expected program benefits.

Recommendations

Despite the new RAH opening being delayed, providing the program with additional time, we recommend the program continue:

- to place priority on the development of pathology electronic ordering dependencies. Any activities that can be performed in parallel should be identified
- regular communication with the EPAS Program and Cerner to monitor progress
- to work to develop the required contingency workflow requirements for the new RAH and communicate regularly with the new RAH Program to ensure that all required workflows are in line with contract agreement with SAHP.[20]

Agency response

SA Health responded that the EPLIS Program will continue with the activities as per the recommendations.

This will be an ongoing process.

[20] The executed project agreement and schedules that outline the contractual obligations of the State and SAHP.

11.12.3.2 Integration challenges with PowerHealth Billing & Revenue Collection

One objective of the EPLIS implementation includes adopting a more effective automated billing process for private and public patients within the SA Health environment and private sector.

The PBRC Billing Project aims to deliver a fully functional billing solution. The solution is required to reproduce certain functionality of the current billing processes of Ultra as well as providing additional expected benefits, including reducing billing process re-work and lost revenue, and enhancing management reporting.

Phase 1 of the PBRC Billing Project, to build the invoice and billing solution, has been significantly delayed from late 2014 to August 2015. We were advised that the delay has been due to:

- increased work on the adopted billing solution due to its complexity and highly customised nature, which has increased build work and extended the testing period
- extended build and testing periods due to the project being under-resourced.

This is a heightened concern as a stable billing environment is required prior to Phase 2 commencing in October 2015, which involves interfacing with EPLIS.

We were advised that the program provided the PBRC Billing Project with a 0.5 FTE resource from April to mid-July 2015 to assist with testing and to help mitigate further delays.

At the time of our review, the program was in the planning stage of Phase 2 of the PBRC Billing Project. The program requires Phase 1 to be completed and all issues addressed before this interfacing can commence.

Prior to the recent new RAH opening delay being announced the critical date for Phase 1 delivery was mid-October 2015.

Risk exposure

A fully functional billing solution is required for the first go-live site (new RAH or alternate go-live site). Until the billing solution has been developed and integrated with EPLIS, the risk remains of increased manual billing processes, the potential for lost revenue and reduced management reporting.

Potential delays may occur in the realisation of expected program benefits.

Recommendations

Frequent communication should continue between the PBRC Billing Project and the program, to monitor progress and ensure all required tasks are completed in a timely manner.

The program should identify billing contingency options in a timely manner, with established key decision points. This is to enable sufficient time to determine required workflows and effectively manage stakeholder expectations through business change processes and clear communications.

Agency response

SA Health responded that Phase 1 of the PBRC Billing Project went live on 1 October 2015 and as the solution is now up and running (including disaster recovery), no contingency option is required.

Phase 2, which involves interfacing with EPLIS, commenced in October 2015. The target completion date is currently being determined as part of the EPLIS schedule review.

11.12.4 Procurement of the laboratory instruments and robotic tracks is yet to be finalised

Timely delivery of the new RAH laboratory instruments and robotic tracks are a dependency for the program. These procurements are being managed by the new RAH Program.

Although the EPLIS and new RAH Programs now conduct regular meetings, we identified an initial lack of visibility of the current status of procurements being managed by other SA Health projects and/or business units.

Integration testing of the EPLIS software and supporting middleware is expected to take approximately three months to complete and is highly dependent on delivery of the laboratory instruments. As of early September 2015, the procurement of the new RAH laboratory instruments and robotic tracks had not been finalised.

SA Health noted that any further procurement delays would impact on the overall EPLIS Program timeline as all schedule contingencies have been exhausted.

Risk exposure

The program is heavily reliant on the timely delivery of the laboratory instruments and robotic tracks.

A high degree of business process change is expected to meet the requirements of EPLIS. Future state business pathology workflows will not be completely understood until EPLIS is integrated with pathology instruments, including analysers, tracks and point of care devices.

Recommendations

Despite the new RAH opening being delayed, the new RAH Program should continue to place priority on finalising the procurement of the laboratory instruments and robotic tracks planned for the new RAH.

To reduce further pressure on the overall program schedule contingency, the program should continue to closely monitor the status of the procurements. This should be through frequent communication with the dedicated procurement resource(s), the new RAH Program and SA Pathology.

Agency response

SA Health responded that the EPLIS Program will continue with the activities as per the recommendations.

This will be an ongoing process as the program liaises closely with the new RAH procurement team.

11.12.5 Deficiencies in system contingency plans

SA Health has identified certain controls and treatments to mitigate the risk of not implementing EPLIS functionality into the new RAH.

We noted that the main contingency for EPLIS is the continued use of the current Frome Road Laboratories. This contingency would use couriers and point of care testing.

However, at the time of our review, there was significant point of care testing equipment with no planned linkage to the new RAH pathology solution. To help address this issue, further work was being conducted by SA Pathology with the assistance of the new RAH ICT Program.

SA Health contingency planning has indicated that the legacy Ultra system would be required to log pathology requests and record results. Due to certain technical limitations with Ultra, all pathology testing would follow existing workflows currently operating at the Frome Road Laboratories, rather than the revised workflows EPLIS requires.

SA Health advised that a number of workshop discussions were conducted between SA Pathology and the EPLIS and new RAH Programs in August 2015, to analyse and determine all preferred contingency options related to EPLIS at the new RAH. Subsequently, a briefing on contingency plans for EPLIS at the new RAH was presented to the eHSC in late August 2015. From this process the eHSC requested more detailed work be performed on these contingency plans.

Risk exposure

SA Health advised that a lack of instrument interfaces for the new RAH tracks and analysers will require manual specimen splitting, storage and loading as well as manual results entry into Ultra. This will impose significant additional manual workload and increased risk of specimen mismatch and transcription errors.

The contingency plans may not contain the required level of detail to completely and accurately reflect all required workflows, should the EPLIS solution not be available for initial operation at the new RAH.

Recommendations

The EPLIS and new RAH Programs should ensure that appropriate priority and management attention is applied to contingencies, which includes allocating time to perform suitable due diligence and planning.

Contingency planning should include a thorough assessment of all associated business impacts and the identification and application of controls to reduce the impacts on pathology service operations at the new RAH.

Agency response

SA Health responded that contingency planning has now been introduced into the EPLIS program schedule and is being managed in collaboration with SA Pathology and the new RAH ICT Program. The plans will include evaluation of business impacts and controls.

The target completion date for the development of detailed contingency plans is January 2016.

11.13 Detailed findings – general program issues

11.13.1 EPLIS budget and contingency may be insufficient to finalise all required program activity

In April 2015, the eHSC approved an Exception Report to reserve contingency of $1.95 million, leaving a contingency balance of $1.431 million. The reserve contingency comprised additional resources, additional funding for vendor travel and resource costs for extended duration of the implementation phase, which was expected to be 20 weeks longer than originally anticipated. At the time of approval, the eHSC noted that there are minimal contingency funds remaining for the remainder of the project.

Despite this, SA Health has acknowledged that further work is to be undertaken on the following items, and current estimated effort exceeds the remaining contingency:

- Electronic pathology ordering – the new RAH laboratory was designed on the assumption that electronic pathology ordering would be received through EPAS. At the time of our review, SA Health was working on identifying the extent of work and cost of this solution. In addition, the source of funding to deliver this functionality is yet to be determined. Should this functionality not be delivered in time for initial operation at the new RAH, a suitable contingency is required. This is further discussed in section 11.12.3.1.

- Archiving legacy data – SA Health has indicated that the provision of an appropriate data archiving solution is not within the program scope and hence any cost savings realisable from decommissioning the legacy laboratory information system cannot be fully achieved unless the scope is modified. Funding for implementation of an archiving strategy that is compliant with regulatory requirements was also not part of the approved EPLIS business case. SA Health has indicated that preliminary cost estimates for decommissioning the Ultra systems and implementing a data archiving strategy could be up to $3.6 million. At the time of our review, the program and SA Pathology ICT were in the process of investigating cost options and developing a strategy to address the archiving of historical data.

- Disaster recovery solution – the program operated under the initial assumption that a single high availability data centre solution was an appropriate disaster recovery solution in the event of a planned or unplanned outage. Further advice indicated that an additional evaluation is required of the risk of having a single data centre solution and a detailed costing for a secondary data centre solution. Preliminary estimates indicate a secondary data centre solution could be up to $5 million, which is not costed within the current budget. At the time of our review, the program was working with Cerner to identify a suitable disaster recovery option.

Risk exposure

Given the project time frames and the minimal contingency funds remaining for the remainder of the project, there is a high risk that SA Health will not have sufficient approved funding to support the implementation of the new EPLIS and its ongoing operations.

Recommendations

SA Health should review and confirm estimated costs to complete the outstanding work requirements discussed above to support the EPLIS implementation.

SA Health should maintain up-to-date expenditure monitoring to facilitate responses to identified budget risks. It should also continually reassess and report on the program's budget position to the EPLIS Board and eHSC.

Agency response

SA Health responded that the EPLIS Program is working on assessing the cost for the three items flagged in the final business case as potentially needing funding from contingency.

The EPLIS Program and the EPLIS Board will continue to monitor budget expenditure closely.

The EPLIS budget position is reported as part of the monthly Program Report to the governance bodies.

These activities are ongoing as the program progresses.

11.13.2 Financial reporting and governance requires improvement

Program governance is based on the principles and guidelines set out by the eHealth Program Management Office.

The monthly board report provides certain financial information including original budget, variations and contingency, actual cost to date recorded in the Oracle Corporate System and estimated completion costs. It also provides a breakdown of expenditure by expense type for the month.

We were advised that program issues and their potential program budget impact are discussed by exception only. Any program issues that result in impacts on the program budget are then raised via an exception report to be presented to the EPLIS Board for discussion. We were also advised that if the program is operating within budget and the available budget is sufficient to cover the completion forecast then there is no discussion at the meeting.

We consider, however, given the ongoing program budget and contingency pressure (as discussed in section 11.13.1), the extent of assessment by the EPLIS Board and associated record of such dialogue and related decisions should be strengthened.

Risk exposure

Budget pressures may not be adequately considered by the EPLIS Board, with outcomes documented in a timely manner.

Recommendation

The rigour of the EPLIS Board's monitoring and assessment of the programs budget and expenditure should be increased, with sufficient documentation of matters discussed in the meeting minutes.

Agency response

SA Health responded that the EPLIS Program Director will specifically address the financial status in the monthly board reporting.

SA Health will ensure minutes and meeting papers of the EPLIS Board's deliberations on budget matters are recorded in more detail in future to provide evidence of budget governance oversight.

The target completion date is October 2015.

11.13.3 Lack of tracking and potential delays of program benefits realisation

The September 2014 approved Cabinet submission noted that Phase 1 included a requirement for SA Health to complete a final business case. The submission also noted that the preparation of the final business case was to include a review of the ongoing operating expenditure requirements and realisable benefits associated with the program.

The May 2015 EPLIS final business case contained expected savings to a net benefit of $854 000 p.a. over five years, commencing in 2017-18. These expected benefits are made up of staff savings, improved client service and a reduction in printing costs. SA Health noted that these benefits are part of the overall operating expenditure savings of $1.6 million p.a. that SA Pathology will be required to achieve from 2015-16 onwards.

As indicated in section 11.13.1, there are minimal contingency funds remaining and certain outstanding solution requirements to be met to support the implementation and operation of EPLIS. These requirements include appropriate data archiving and disaster recovery solutions, which at the time of this Report, were not included as part of the current EPLIS Program budget. Therefore, these requirements have the potential to further delay the expected realisation of program benefits.

The EPLIS Board minutes for June 2015 noted that program benefits realisation tracking has not been completed due to a lack of project management resources. The current recruitment process has caused delays in obtaining resources in a timely manner.

The EPLIS Program Status Report for June 2015 also advised that increased benefits management reporting is pending the finalisation of the benefits realisation plan.

Risk exposure

Due to a lack of timely tracking and reporting, the program may not have a clear indication of the realisation of expected program benefits identified in the May 2015 EPLIS final business case.

There is the potential for further reduction in expected benefits, due to a current lack of contingency funding available to meet outstanding EPLIS solution requirements.

Recommendations

SA Health should address any program recruiting challenges to ensure that appropriate resources are obtained in a timely manner.

SA Health should regularly track predicted tangible benefits and update accordingly as the program evolves.

The relevant program governance boards should be updated in a timely manner of any material changes in predicted tangible benefits. Consideration should also be given to updating Cabinet on relevant outcomes.

Agency response

SA Health responded that the EPLIS Program has addressed the recruiting challenges with the appointment of a program resource to manage these activities.

The EPLIS Program is currently drafting the Benefits Realisation Plan, as well as establishing the baseline for the future measurements. Benefits realisation will be monitored on a monthly basis in time for the first Go Live (as no benefits will be materialised prior to the rollout commencing).

The target completion date for the Benefits Realisation Plan is December 2015.

11.13.4 Ongoing resource challenges exist

SA Health and SA Pathology ICT resource availability and support for program phases has continued to place pressure on deliverables and time frames. SA Health advised that the program has experienced difficulties accessing resources due to the program's complexity, schedule dependencies and competing priorities, including supporting legacy systems and other SA Health ICT projects.

The program made significant recruiting progress in January 2015, which included the commencement of a Project Manager, Pathology Systems Analyst, Technical Lead and the recruitment of a Communications Officer, Change Manager and Project Scheduler.

SA Health advised that the program budget underestimated the amount of effort required to implement EPLIS. This included limited resource allocation to effectively plan and develop change management strategies, which encompassed training, adoption and deployment to ensure all key stakeholders are appropriately managed.

As a result, the resource plan was revised to reflect the increasing staff requirements. This revised plan was incorporated into the final business case approved by the eHSC in late May 2015.

Risk exposure

The inability of the program to access timely resources, including competing business as usual priorities and the delivery of other major SA Health projects, may cause delays in program activities.

There is no contingency in the program schedule to absorb any potential delays.

There may be a lack of business acceptance of the EPLIS solution work practices.

Recommendation

SA Health should proactively monitor the resource plan as the program progresses and ensure timely actions are taken, including communications and approvals, where resource constraints or issues are identified.

Agency response

SA Health responded that the EPLIS resource plan is being actively managed on an ongoing basis.

11.13.5 Pathology results reporting challenges to maintain private revenue

A briefing note was presented for endorsement by the EPLIS Board in January 2015, requesting approval to investigate the costs of a commercially available product to replace the legacy Electronic Data Interchange (EDI) solution.

The briefing note stated that there is an ongoing requirement to feed results data from the SA Pathology laboratory information system to general medical practices to maintain private revenue. The current EDI solution delivers pathology reports to Flinders Private Hospital (Web PAS system) and other external organisational requestors. In addition, EDI acts as a gateway service to send medical imaging reports to general practitioners from the existing RAH, the Women's and Children's Hospital, The Queen Elizabeth Hospital and the Lyell McEwin Hospital.

Results are sent from the existing Ultra through the current EDI to a number of different private medical practice management software packages used by private clinicians, including general practitioners and specialists. EPLIS is able to interface with the Health Integration Broker to send out data results (eg to EPAS), however private medical practices do not have access to EPAS, and EPLIS does not have the functionality to directly interface with private medical practice software through its external interface engine. Therefore, private clinicians are reliant on the existing EDI.

The May 2015 EPLIS final business case noted that the current EDI system is included in the scope of the program. At the time of our review, the program was working at ensuring that the existing legacy EDI solution is appropriately interfaced with EPLIS to feed the required results data, until a replacement solution is sourced.

From an SA Pathology business perspective, we were advised a long-term interface solution is imperative to provide private clinicians not only with the ability to view pathology results, but to also order pathology results electronically. At the time of our review, we were advised that a solution has yet to be determined.

Risk exposure

The current EDI solution services over 1000 practitioners, sending one million messages per month. A loss of this service would result in more paper reports and potential loss of referring doctors and associated revenue.

Recommendations

SA Health should continue to work towards ensuring the existing EDI is appropriately configured and tested to interface with EPLIS and consider contingency options in the event of the EDI not being interfaced with EPLIS.

Should the existing EDI not provide SA Health with a long-term interface solution with private medical practices, SA Health should continue to investigate a replacement solution. When a viable replacement solution is available it should be procured as soon as possible to avoid erosion of SA Pathology revenue from private clinicians.

Agency response

SA Health responded that the EPLIS Program will undertake the work required to configure and test the EDI interface as per the program schedule.

A replacement EDI solution may be considered in due course.

These activities are ongoing as the program progresses.

11.13.6 Program activities continued without a formally approved EPLIS business case

The feasibility stage of the program included vendor planning, which involved a tender issue to market, detailed evaluation and validation and the completion of a statement of work. This phase also included completion and approval of a formal business case.

As previously noted the EPLIS final business case was not approved when originally submitted to the eHSC in December 2014. The eHSC requested that the business case instead be independently reviewed and revised. Further delays were also experienced due to questions raised by SA Health Corporate Finance relating to program total cost of ownership estimates.

Phase 2 of the program was originally only to be commenced if the detailed planning and final business case met the requirements of SA Health. It was also dependent on eHSC approval of the business case and access to the funding for the implementation phase.

Despite this requirement, we noted that program activities continued without an approved business case, including program implementation activities and the procurement of hardware and software. We do note, however, that in the interim the eHSC had approved expenditure from the implementation budget pending the submission of this final business case.

The EPLIS final business case was subsequently approved by the eHSC in late May 2015.

Risk exposure

Despite expenditure authority of the program implementation budget, approval of the business case remained outstanding for a significant period (December 2014 to May 2015). In the interim, program activities continued that were potentially not in line with expected business outcomes.

Recommendation

SA Health should ensure that ongoing program activities and expected outcomes accurately reflect the May 2015 revised business case.

Agency response

SA Health responded that the EPLIS governance bodies will monitor the program against the May 2015 business case and ensure any deviations are managed by exception reports.

These activities are ongoing as the program progresses.

11.14 Concluding comment

The program has experienced a number of interruptions and changes. This can be attributed to delays in governance approvals, inadequate early program planning and portions of time when the program was put on hold. These issues have put pressure on the program to modify the implementation schedule, including the requirement in the May 2015 business case for the new RAH to be the first rollout site.

Despite modifying the implementation approach and the announcement of the new RAH opening delay, there is still a risk that EPLIS will not initially be fully operational as per the program's implementation schedule. In terms of the new RAH, the program schedule is dependent on other SA Health programs and vendor requirements. There is also significant change facing new RAH pathology staff in transitioning to the new hospital environment.

Given these challenges, significant focus will be required on the business change management strategy and tasks to ensure a fully functional implementation is finalised in a timely manner. These tasks include interface integration of key components, close monitoring of the status of pathology hardware procurements, proactive monitoring of resourcing as the program progresses and thorough contingency planning.

There is minimal contingency funding available for the remainder of the program and recently a number of additional activities have been identified. These activities are required to produce the planned EPLIS functionality, support ongoing operations and ensure benefits are realised through a successful transition. We consider that the program may require additional funding to complete all program necessities, with expected benefits potentially delayed.

12 Pharmacy systems implementation at the new Royal Adelaide Hospital

12.1 Introduction

The State Pharmacy Management System is an enterprise system that was rolled out to all SA Health sites in a program managed and supported internally by eHealth Systems from 2008 to 2012.

The new RAH Program includes a number of sub-projects to deliver current and new ICT services to the facility, including the new RAH ICT Pharmacy Project (the project).

The end-state pharmacy implementation at the new RAH is based on the principles of closed loop medication management (CLMM), which is intended in the longer term to support the hospital's model of care.

Elements that support a CLMM are planned to be progressively implemented at the new RAH following initial operation over an approximately 18 month period. This model is designed to feed outcomes from medication processes into a set of integrated systems. The aim is to improve information flow between clinicians and departments, enabling hospitals to progress toward the safest delivery of patient care.

12.2 Audit objective and approach

The objective of this review was to obtain an understanding of the project implementation status for the pharmacy systems at the new RAH. This includes expected benefits and costs, key risks and the systems' impact and readiness.

To conduct this review, we related with the new RAH Program, in particular Pharmacy project representatives. We also reviewed project governance documentation, including the project plan, project reports and briefing notes, risk registers, high level system designs and the eHSC and Internal Audit meeting minutes.

During the finalisation of this Report a September 2015 Cabinet submission and negotiation settlement occurred between the Minister for Health and the SAHP.[21] Following this negotiation settlement, the Government announced a delay to the opening of the new RAH. It is now expected to open by November 2016.

At the time of this Report, the project has yet to determine the implications of this delay to the pharmacy project plan and associated costs.

12.3 Key findings

Our 2014-15 review, finalised in September 2015, has noted the following key project risks, which are explained further in section 12.7:

- inadequate Project Board reporting of milestone changes and evidence of matters discussed
- new RAH pharmacy solution schedule challenges
- procurement delays
- certain functionality may not be available on initial operation of the new RAH.

12.4 Pharmacy background and drivers

On 4 December 2006, Cabinet approved a submission on pharmaceutical reforms in South Australia. This submission included approval to enter a tender process for the procurement of a replacement pharmacy management system (known as i.Pharmacy).

The pharmacy management system was required as the previous state-wide pharmacy system, ASCribe, was assessed as being incapable of processing Pharmaceutical Benefits Scheme claims. This was deemed critical to support pharmaceutical reforms.

On 14 April 2008, SA Health engaged iSOFT (now known as CSC) for the supply, installation and support of the i.Pharmacy solution at 11 in-scope hospitals. An additional three sites were subsequently added to the scope. The intention was for i.Pharmacy to provide administrative aspects, including medication dispensing and inventory control.

[21] The new RAH Program is being delivered under a Public Private Partnership agreement with SAHP. SAHP is responsible for the design and construction of the new hospital facility.

We were advised the rollout of the enterprise i.Pharmacy software commenced in December 2008 and was completed in September 2010, at an approximate cost of $5.5 million.

12.5 New Royal Adelaide Hospital pharmacy design approach

The design of the pharmacy implementation at the new RAH is based on the principles that support the new hospital's model of care.

The planned model of care requires the successful transition of health care services from the existing RAH to the new RAH. One such system that requires transitioning is i.Pharmacy.

The unique design for the new RAH is notably different to the pharmacy management solution rolled out to other SA Health sites, including the existing RAH. This design includes two pharmacies, located on Level 1 (inpatient) and Level 3 (outpatient). The new RAH pharmacy architecture design also includes the provisioning of an automated storage and distribution system, in-pharmacy robotics, for medications in each pharmacy location. This system is known as the Automated Pharmacy Distribution System.

The automated solution includes integration with 81 Automated Dispensing Cabinets (ADCs) located throughout the hospital. The intention is to provide authorised staff with timely access to securely stored and verified patient medications.

SA Health advised that the physical movement of medications can be performed either by way of Automated Guided Vehicles, the Pneumatic Tube System or manual delivery by pharmacy staff. Once delivered to the patient wings the pharmacy assistants load medications in the ADCs.

To facilitate a CLMM, the pharmacy implementation requires the commissioning of a number of complex activities. This includes certain ICT elements to enable key pharmacy functions to operate, notably:

- prescribing processes
- distribution processes and associated inventory management functions
- pharmacy manufacturing (production) processes
- medication dispensing and administration (to patients)
- clinical pharmacy services
- integration with hospital administration and clinical systems.

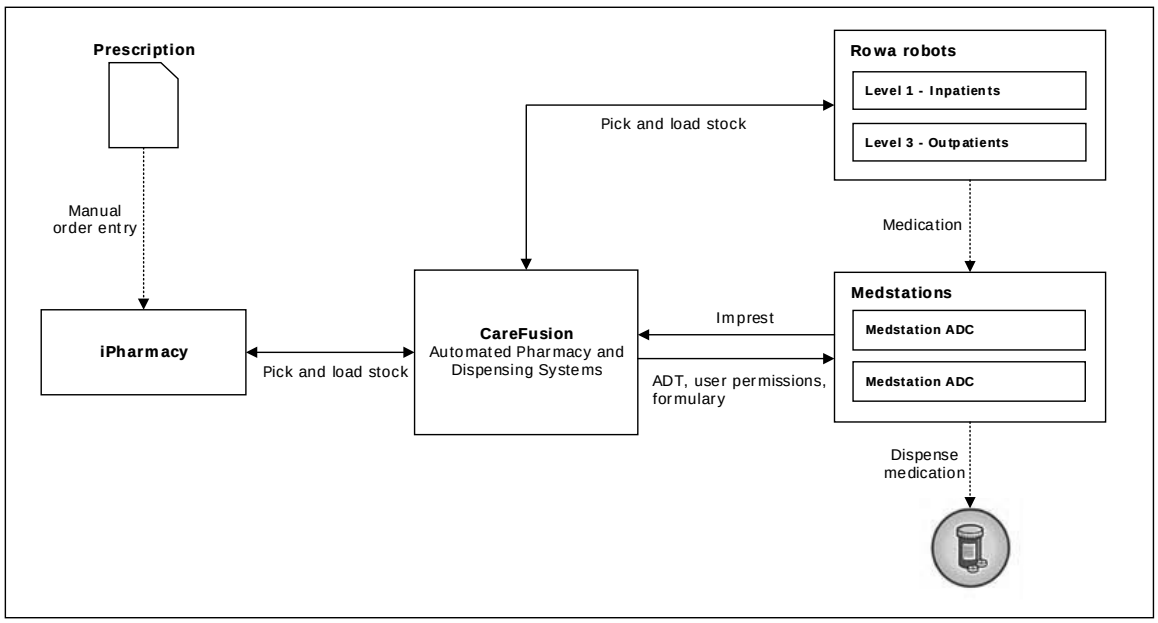
The project plan, states that for the CLMM to be implemented over an extended period will require the eventual integration of a number of systems, notably:

- EPAS[22] – Allscripts system
- APDS, in-pharmacy robotics – CareFusion Rowa system
- ADC – CareFusion Pyxis system

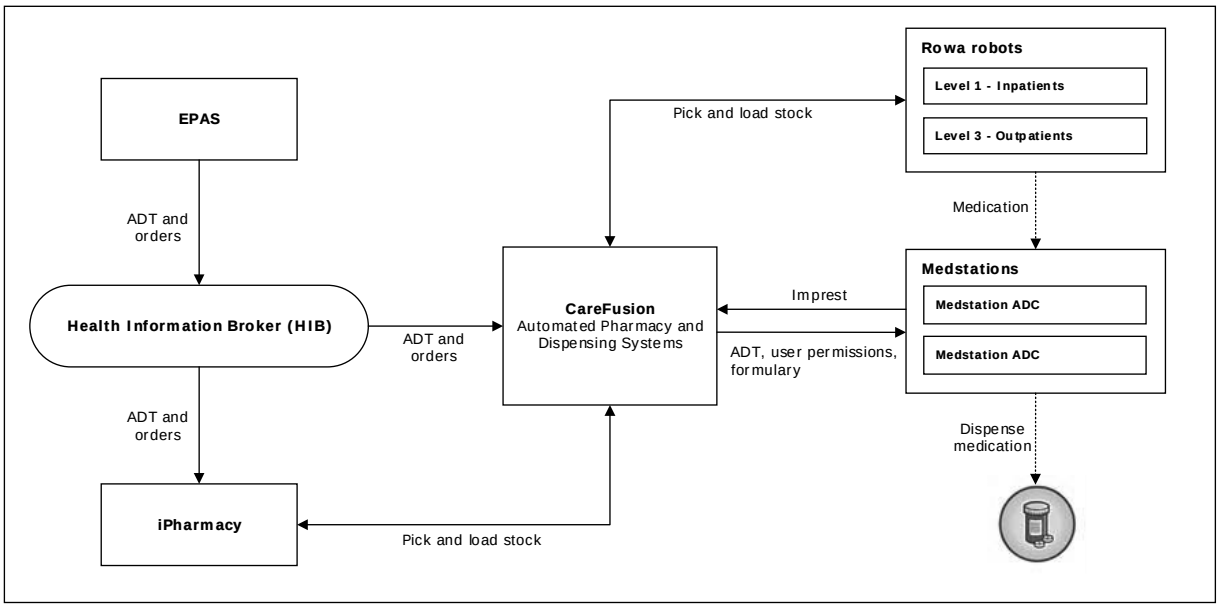
[22] The project is also working concurrently with the broader new RAH ICT Program on a contingency option in case EPAS is not available for initial operation of the new RAH. In this situation the current patient administration system solution at the existing RAH, APMS, will be used as the contingency.

- Pharmacy management system – CSC i.Pharmacy system
- Health Information Broker[23] – electronic data interchange.

The following diagram provides a high-level summary of the expected pharmacy solution data flows for initial operation at the new RAH.[24]



The following diagram provides a high-level summary of the expected key end state CLMM pharmacy solution data flows at the new RAH.



[23] Health Information Broker is a central electronic data interchange used to exchange information between SA Health enterprise systems.

[24] At the time of this Report, the project has yet to determine any implications on the expected initial data flows as a result of the recent announcement to delay the new RAH opening.

Other key systems included in the overall pharmacy information workflow planned for the new RAH include:

- Pharmacy Camera Verification System
- Oracle Corporate System for pharmacy patient billing and procurement and supply chain management
- Patient Queuing and Wait Management System – pharmacy outpatient management.

To help achieve the project implementation objectives, a detailed project plan was completed in March 2015. This plan included: identifying and defining the major products of the project and methods for delivery; major activities and time frames; dependencies, assumptions and constraints; major risks; and resource requirements.

In order to deliver on these project objectives, the project was divided across a number of work packages, with individual deliverables that address the system implementation components and associated interfaces. To support project delivery of these work packages, multiple reference groups were established, which included a number of SA Pharmacy[25] business representatives, designed to provide specialist input, knowledge and recommendations.

At the time of this Report, the project had yet to determine the implications of the new RAH opening delay to the pharmacy project plan.

12.6 Summary of pharmacy project expected benefits and costs

The project is expected to realise benefits, including an APDS, that allow a reduction of central stock value of 20% and a reduction in stock waste between 4% and 10%. Other expected benefits of an APDS at the new RAH include a reduction in dispensing times for patients, increased time for pharmacists' clinical work, quick recall of medication, improved stock visibility and nursing time savings.

In the original new RAH APDS business case, SA Health estimated the value of savings could be up to $71 million over the life of the APDS asset (15 years). SA Health is in the process of developing an assessment of the overall anticipated benefits to be realised from the new RAH CLMM solution. This assessment will be based on assumptions outlined in the business case.

In terms of costs, the project is consolidated into the overall budget for the new RAH ICT Program, with oversight from the new RAH ICT Board. Some costs are shared between the new RAH ICT Program and SA Pharmacy.

The new RAH ICT Program costs and resourcing roles were included in an approved September 2014 Cabinet submission. The submission also noted that new RAH ICT more broadly has a requirement for pharmacy ICT to be operational and integrated with the in-pharmacy robotics and ADCs. The submission included the rollout of other enterprise

[25] SA Pharmacy provides publically managed and operated pharmacy service to LHNs. SA Pharmacy services involve a range of activities aimed at enhancing the safe and effective use of medicines. These activities include the supply, manufacture and distribution of medicines, patient specific professional services and system wide services such as teaching, training and research.

systems to the new RAH, together totalling an estimated $2.6 million. Approximately $500 000 of the $2.6 million budget was originally allocated to the i.Pharmacy implementation.

However, as previously mentioned, there are a number of system components contributing to the eventual commissioning of a CLMM and the achievement of the estimated $71 million of savings. This includes the capital cost of the in-pharmacy robotics and APDS and complete workflow integration of pharmacy systems.

Expenditure to date directly attributed to the new RAH pharmacy solution is being managed by the new RAH ICT Program.

We note that the anticipated costs associated with implementing the pharmacy solution may require some revision due to the new RAH opening delay.

12.7 Detailed findings

The new RAH model of care assumes a fully integrated ICT system is adopted, allowing for CLMM to be implemented. At the time of this Report, the project was in the build phase and was working on a number of work packages spanning across systems that make up the pharmacy solution.

A number of work package activations are planned to cross over with the SOC period, which involves testing of all new hospital operations ready for commercial acceptance.[26] SA Health advised that these activities were in progress and being managed by SA Pharmacy and the new RAH Pharmacy Commissioning Manager.

SA Health advised that the project is progressing as expected and the delay in the new RAH opening will provide additional time for the project to complete all required activities. SA Health has also acknowledged that a number of challenges and issues remain outstanding. These challenges and issues, discussed further below, present certain risks to delivering the pharmacy solution to the new RAH in a timely manner and to the required quality.

12.7.1 Inadequate Project Board reporting of milestone changes and evidence of matters discussed

From a project governance perspective, we noted that the new RAH Pharmacy Project Board (the Project Board) was established at the commencement of the project in March 2015. The purpose of the Project Board is to provide overall direction, essential governance and decision-making functions for the project.

We obtained and reviewed a number of new Project Manager Reports that are presented to the Project Board on a monthly basis. We noted throughout the course of the project that a number of the work package forecast completion dates have been pushed back. We do acknowledge, however, SA Health's advice that due to site access restrictions until technical completion,[27] certain activities cannot occur until the SOC testing period.[28]

---

[26] Commercial acceptance is the current contractual date the new RAH is to be delivered and accepted by the State.

[27] Technical completion is the contractual date all required building works are to be delivered. The original date was 18 January 2016. This contractual date has since been delayed by 76 days to 4 April 2016.

[28] The SOC testing period was originally January-April 2016. This testing period has since been delayed to April-July 2016.

Despite this, other work packages not impacted by these site access restrictions had their forecast end dates extended. Notable examples include:

- solution architecture
- requirements and workflows
- test plan and test case preparation
- EPAS to Pharmacy integration
- APMS configuration (contingency)
- training and communications.

The completion dates for these work packages are presented to the Project Board on a regular basis, however variances between the baseline and current forecast completion dates are not clearly articulated through the available reports.

For a number of these work packages, we were unable to identify any clear explanations for the change in completion dates in the Project Manager Reports presented to the Project Board. In addition, there was no documented evidence identified in the Project Board meeting minutes to support discussion of the program schedule changes. Therefore the extent of understanding and discussion of these matters by the Project Board was unclear.

Risk exposure

There is a risk that project schedule changes are not appropriately presented to the Project Board for formal discussion. A lack of information presented to the Project Board may impact its ability to make informed decisions impacting the project.

There is a risk that significant project changes are made without formal discussion and endorsement from the Project Board.

Recommendations

The project should determine the implications of the new RAH opening delay and highlight any alterations to work package forecast completion dates to the Project Board in a timely manner.

Any adjustment to the project schedule, including clear justification, should be appropriately highlighted to the Project Board for formal discussion.

Discussion of significant matters impacting the project should be formally documented, including key decision points.

Agency response

SA Health responded that the Project Manager has noted the recommendation and will take steps to ensure changes to milestone dates are minuted at future Project Board meetings.

The implications of the revised opening date for the new RAH will be analysed and highlighted to the Project Board as per standard reporting processes, noting the recommendation for further detail of the discussions to be evidenced in the associated minutes.

The target completion date is October 2015.

12.7.2 New Royal Adelaide Hospital pharmacy solution schedule challenges

We noted that SA Health only formally initiated the project in March 2015.

Although the recent delay in the new RAH opening will provide additional time for the project to complete all required activities, we consider that challenges remain that are discussed further in this Report.

12.7.2.1 Certain work packages activities allocated to State Operational Commissioning testing period

At the time of our review, the original project timeline listed a number of work package activities to be completed during the SOC testing period, including APDS, ADC and Pharmacy Camera Verification System related activities.

As previously mentioned, SA Health advised that due to site access restrictions certain activities must occur on site during the SOC testing period. These activities include configuration (medication stock loading) and acceptance testing of pharmacy hardware and certain integration requirements. Of particular note, ICT systems related activities were also originally scheduled during this period. Such activities include a scheduled upgrade and configuration of the i.Pharmacy software and subsequent integration with APDS, to interface components between the i.Pharmacy and the CareFusion in-pharmacy robotics (further discussed in section 12.7.4.3).

As a partial mitigating control, SA Health advised that some pharmacy ICT software configuration and integration activities can be performed in isolation and are therefore not fully dependent on the delivery of pharmacy hardware.

Risk exposure

The original project schedule included configuration, integration and user acceptance testing for the new RAH during the SOC testing period. Any issues identified during configuration, integration or user acceptance testing may not have been resolved by the commercial acceptance date for the new RAH, potentially resulting in increased manual workarounds.

The recent new RAH opening delay announcement may reduce the pressure to perform some project work package activities during the revised SOC testing period. However, at the time of this Report, it was unclear whether this risk had been sufficiently mitigated.

Recommendations

Where possible, priority should be placed on completing certain works prior to the revised SOC testing period. These include ICT related works that are assessed as potentially impacting initial operations at the new RAH.

Where scheduled work timing cannot be altered, appropriate contingency plans should be established.

The project should ensure that all requirements are being performed in line with milestone commitments in the contract agreement with SAHP.

Agency response

SA Health responded that the recommendation has been noted by the project, however no further action has been deemed necessary. All project activities have been sequenced (and are regularly reviewed) to minimise delivery risk prior to the SOC period, and are being performed in line with milestone commitments in the contract agreement with SAHP.

The target completion date is April 2016.

12.7.2.2 External dependencies exist that may impact time frames and resourcing

The pharmacy implementation at the new RAH is planned as a phased approach, from system configuration through to full implementation. These phases were planned based on certain system integration and functionality complexities.

The project is presented with certain challenges in implementing an integrated pharmacy solution at the new RAH. These include the significant reliance on other external dependencies, including:

- the vendor's physical delivery and installation of the pharmacy hardware (APDS and ADCs), managed by the new RAH Pharmacy Commissioning Team
- workflow development cannot be finalised until the vendor delivers the pharmacy hardware and provides the necessary training
- the timely state-wide i.Pharmacy software version upgrade to meet new RAH requirements (discussed further in section 12.7.4.3), managed by the application owners (SA Health's eHealth Systems and SA Pharmacy).

In addition, we note that ICT implementation aspects, such as local servers, network connectivity, system configuration and activation activities, remain the responsibility of the new RAH ICT Program and will be coordinated with the installation and commissioning of the APDS.

SA Health advised that the required pharmacy ICT infrastructure is challenging to design and configure due to complex networking and server vendor requirements. At the time of this Report, the project had completed solution architecture design work and had commenced the build phase.

Risk exposure

Despite the recent new RAH opening delay announcement reducing this risk, external dependency delays or issues experienced may still impact the new RAH implementation time frames and workflows, and place additional pressure on the available project resources.

Recommendation

The project should continue to monitor the progress of these external dependencies to ensure any impact on the pharmacy implementation at the new RAH is minimised.

SA Health response

SA Health responded that the recommendation has been noted by the project and external dependencies will continue to be monitored in line with dependencies across the broader new RAH ICT Program.

The target completion date is April 2016.

12.7.3 Procurement delays experienced

As mentioned above, the new RAH pharmacy design model includes an automated medication dispensing solution (APDS and ADCs).

To meet this requirement, SA Health advised that a full market request for tender process was conducted and the tender closed in November 2012. The purchase recommendation, however, was not approved until December 2014.

In April 2015 a contract was signed with the preferred vendor (CareFusion) for APDS and ADCs. The contract included providing the pharmacy hardware (inpatient and outpatient services) for automated stock handling, associated software (Rowa and Pyxis), installation, maintenance and support.

The delay in formalising this contract has restricted the ICT component of the project because CareFusion resources required to identify, plan and execute design and configuration activities could not be engaged and allocated. The delay contributed to the original project schedule having limited available contingency if problems occurred in the delivery of the pharmacy hardware.

To minimise any potential impact, SA Health has advised that significant work on commissioning and physical configuration has been undertaken in parallel with formalising the contract. In addition, SA Health has worked with CareFusion on a project execution plan to deliver and install the specified components of the pharmacy solution. This was originally anticipated to be completed by December 2015, but this date may now need to be revised as a consequence of the new RAH opening delay, the readiness of the builder (SAHP) and any related building modifications.

Risk exposure

A number of program activities remain dependent on timely delivery and installation of the pharmacy hardware.

Despite the recent new RAH opening delay announcement reducing this risk, there may still be insufficient time available for testing of pharmacy requirements and workflows prior to initial operation at the new RAH. Any issues identified during the SOC testing period may require refinement following initial opening of the new RAH.

Recommendations

SA Health and CareFusion should maintain regular communication and activity status updates to ensure any potential delays are highlighted and addressed in a timely manner.

To minimise any potential impact of procurement delays SA Health should consider all contingencies to reduce the risk to the pharmacy implementation at the new RAH.

Agency response

SA Health responded that the revised opening date for the new RAH has not impacted the focus on project delivery but has increased available contingency should a delay be experienced.

The recommendation has been noted by the project and weekly management and ICT meetings continue with the pharmacy hardware vendor with decisions from each meeting recorded. No additional remediation actions have been deemed necessary.

The target completion date is April 2016.

12.7.4 Certain functionality may not be available on initial operation of the new Royal Adelaide Hospital

As previously mentioned, elements that support a CLMM are planned to be progressively implemented at the new RAH following initial operation over an approximately 18 month period. In the interim certain functionality may not be available. These are discussed below.

12.7.4.1 Electronic medications management

Electronic medications management requires configuration activities on both the requesting system, EPAS (for electronic prescription ordering), and the receiving system, i.Pharmacy (for receipt of electronic transmission through the Health Information Broker).

A review of Project Manager Reports identified that in April 2015, a decision was still pending on the delivery of EPAS electronic prescribing functionality for initial operations at the new RAH.

Certain constraints of EPAS current system functionality have presented challenges to pharmacy electronic prescribing. These include barcode scanning functionality for consistent identification and administration of medication to patients, and the complexity and effort required to configure matching patient medication profiles across systems.

SA Health originally advised that there would not be an electronic prescribing interface from EPAS to i.Pharmacy for initial operation of the new RAH. As such, prescription orders appearing in EPAS will require printing and a manual check if the medication is available in the ward ADC. At the time of this Report, SA Health had not indicated whether the new RAH delay will allow this functionality to now be available at initial operation.

In addition, the project has noted a risk that electronic receipt of transmission orders may only be available through an additional i.Pharmacy licence module (electronic prescribing module). CareFusion has also indicated that profiling in ADCs is not possible unless an electronic prescribing module is operational.

Where the medication is not available from the ward ADC, and should the CareFusion electronic prescribing module be active, orders will have to be manually entered into i.Pharmacy, as is the current process at the existing RAH. These orders require the medication to be sourced from the in-pharmacy robotics.

At the time of this Report, the electronic prescribing module had been procured and further analysis was required by the EPAS Program and the project to develop and integrate the module with EPAS.

Although SA Health advised that the project and the EPAS Program have increased communications to address these requirements, the two parties only commenced formal meetings in May 2015.

Risk exposure

There may be added costs of manual workarounds and inefficiency in the delivery of patient medication.

Pending project decisions in relation to electronic medications management have the potential to impact the project work plan and may cause inconsistencies with the pharmacy workflows being developed.

Recommendations

SA Health should reassess whether the new RAH delay provides sufficient time to provide electronic medications management functionality at the hospital's initial operation. Should this functionality not be available, any impacts on workflows and resource allocations should be assessed in the development of appropriate contingency plans.

The project should continue frequent communication with other relevant SA Health programs, including the EPAS Program, with timely consideration of forward planning.

Agency response

SA Health responded that the project maintains frequent dialogue with EPAS and other SA Health areas with regards to electronic medications management functionality.

Discussions have commenced regarding the scope of EPAS as a result of the revised opening date of the new RAH. A formal decision is yet to be made on the specific matter of electronic medications management functionality.

The recommendation has been noted by the project with the clarifications above.

The target completion date is April 2016.

12.7.4.2 Electronic patient billing

The new RAH ICT Pharmacy Project Manager's Report, dated April 2015, indicated that financial management functions at the new RAH will be performed through Oracle Corporate System and the EPAS financial module (Sunrise Financial Manager). However, the EPAS financial module does not currently have the functionality to process pharmacy patient billing.

At the time of this Report, the project was working with SA Heath Corporate Finance to identify an appropriate pharmacy patient billing system for the new RAH. SA Health advised that a patient billing discussion paper was due to be presented to the Board.

We consider that this matter relating to the new RAH pharmacy solution can be at least partially attributed to the delay in timely activation of the project and SA Health programs operating in a siloed manner. We also consider there to be insufficient forward planning and cross-team communication mechanisms.

Risk exposure

Pending project decisions in relation to the billing solution have the potential to impact the project work plan and may cause inconsistencies with the pharmacy workflows being developed.

The absence of a fully functional, appropriately tested and operational pharmacy patient billing system for the new RAH has the potential to result in loss of patient billing revenue through inaccurate or incomplete patient billing processes. We note, however, that this risk is reduced with the additional time now available to develop a solution.

Recommendations

SA Health should identify any patient billing functionality that may not be available at initial operation at the new RAH. Any impacts on workflows and resource allocations should be assessed in the development of appropriate contingency plans.

The project should continue frequent communication with other relevant SA Health programs and relevant business units, with timely consideration of forward planning.

Agency response

SA Health responded that a pharmacy patient billing solution using the Oracle Corporate System to support current workflows was proposed and endorsed at the Project Board meeting on 7 September 2015.

The proposed solution is yet to be approved through the SA Health eHealth governance process and a default position of implementing the current manual process (as used at all non-RAH i.Pharmacy sites) will be activated.

The recommendation has been noted by the project with the clarifications above.

The target completion date is April 2016.

12.7.4.3 Interface solution between the i.Pharmacy and in-pharmacy robotics

In April 2015 the existing state-wide SA Health standard pharmacy management system (i.Pharmacy) software was upgraded from version 5.7 to 6.7.3. This upgrade included system enhancements required to comply with vendor requirements and maintain the support agreement.

SA Health also intends to implement further software upgrades to versions 8 and 9 to facilitate communication with multiple in-pharmacy robots and ensure medication dispensing and stock control activities at the new RAH. The i.Pharmacy vendor (CSC), however, has indicated that version 8 will not be released until 2016.

As a result of the initial new RAH deadline, an interim solution was deemed necessary to provide the functionality intended by upgrading to versions 8 and 9. In response, the project and CSC were working to develop a specifically adapted bespoke solution to interface i.Pharmacy and APDS (CareFusion Rowa). The development of this solution requires a contract variation to the existing i.Pharmacy master agreement with CSC, placing additional pressure on new RAH implementation time frames.

Installation of this functionality specific to the new RAH requires an additional state-wide version update (from 6.7.3) scheduled for February 2016.

Risk exposure

The recent delay in the new RAH opening will provide additional time for the project. However, any unexpected delivery and configuration problems with the adapted bespoke solution has the potential to impact the pharmacy implementation.

Recommendations

SA Health should reassess its position with regard to the implementation of the interim bespoke solution. If still required, priority should be placed on developing this solution and facilitating, as relevant, the timely finalisation of the contract variation to the i.Pharmacy master agreement with CSC.

SA Health should identify the medication dispensing and stock control functionality that may not be available at initial operation at the new RAH. Any impacts on workflows and resource allocations should be assessed in developing appropriate contingency plans.

Agency response

SA Health responded that the revised opening date for the new RAH has not impacted the delivery date or continued focus on implementation of the bespoke solution, but has increased available contingency.

SA Health has already received and is in the process of installing and validating the bespoke adapter module from CSC in an SA Health test environment.

The recommendation has been noted by the project and frequent contact with CSC continues. No additional remediation actions have been deemed necessary.

The target completion date is April 2016.

12.8 Concluding comment

When fully implemented, the proposed pharmacy systems at the new RAH are expected to improve information flow between clinicians and departments, enabling the hospital to progress toward the safest delivery of patient care.

Throughout the project the forecast deliverable dates have been revised as the project continues to work through a number of issues and challenges. It is considered that these issues and challenges can be partially attributed to the delay in commencing the project. This resulted in the original plan having ambitious time frames and an underestimation of the effort required for a number of elements of the pharmacy solution planned for the new RAH.

We consider, however, that the recent new RAH opening delay announcement should reduce the implementation risks and audit concerns raised in this Report. Despite this risk reduction, it is imperative that the project and the new RAH Program completely understand and document the associated impact of the new RAH opening delay and all workflows planned for the pharmacy solution for its initial operation. All responsibilities and key decision points should be clearly identified and understood between pharmacy stakeholders, with appropriate planning communicated through the relevant governance and reference groups.

Appendix

Acronyms used in this Report

Acronym	Description
ABF	Activity Based Funding
ADT	Admissions, discharges and transfers
AD	Active Directory
APDS	Automated Pharmacy Distribution System
APMS	Acute Patient Management System
CDW	Central Data Warehouse
CHDW	Country Health Data Warehouse
CSC	CSC Australia Pty Ltd
DCSS	Distributed Computing Support Services
DPC	Department of the Premier and Cabinet
eHSC	eHealth Steering Committee
EPAS	Enterprise Patient Administration System
EPLIS	Enterprise Pathology Laboratory Information System
HP	Hewlett Packard Australia Pty Ltd
ICT	Information and Communications Technology
IHPA	Independent Hospital Pricing Authority
ISMF	Information Security Management Framework
ISMS	Information Security Management System
LHN	Local health network
NEC	National efficient cost
NHFB	National Health Funding Body
ODG	Office for Digital Government
PPM	Power Performance Manager
RAH	Royal Adelaide Hospital
SAHP	SA Health Partnership Nominees Pty Ltd
SA Health	Department for Health and Ageing
SNS	StateNet Services
SOC	State Operational Commissioning