



ACT
Government

ACT Health

FOI19-20



Dear 

Freedom of Information Request: FOI19/20

I refer to your application under section 30 of the *Freedom of Information Act 2016* (the Act), received by ACT Health Directorate on 7 April 2019 in which you sought access to:

"I would like copies of all internal audit reports prepared for ACT Health during 2017-18;

- *ACT Health Internal Audit related to IT Governance and strategic planning performed in 2017-18;*
- *ACT Health Internal Audit related to the effectiveness of ACT Health's implementation of recommendations relating to Data Integrity performed in 2017-18;*
- *ACT Health Internal Audit related to patient safety and Quality Governance processes performed in 2017-18;*
- *ACT Health Internal Audit related to the IT Disaster Recovery Plan performed in 2017-18;*
- *ACT Health Internal Audit related to the University of Canberra Hospital (UCH) project governance;*
- *ACT Health Internal Audit related to asset stocktaking;*
- *Briefings prepared for the Minister for Health and the Director-General of ACT Health regarding the outcome of these reports."*

I am an Information Officer appointed by the Director-General of ACT Health under section 18 of the Act to deal with access applications made under Part 5 of the Act. ACT Health Directorate was required to provide a decision on your access application by 27 June 2019.

Decision on access

Searches were completed for relevant documents and 6 documents were identified that fall within the scope of your request.

I confirm that no written briefings were prepared for the Minister for Health & Wellbeing or the Director-General, ACT Health Directorate, regarding the outcomes of the Internal Audit Reports. Internal Audit Reports are provided to the independently chaired Audit and Risk Management Committee, which endorses and oversees the implementation of recommendations within the Directorate.

I have included as Attachment A to this decision the schedule of relevant documents. This provides a description of each document that falls within the scope of your request and the access decision for each of those documents.

I have decided to grant access in full to 5 documents relevant to your request and partial access to 1 document, as I consider it to be information that would, on balance, be contrary to the public interest to disclose under the test set out in section 17 of the Act.

I have decided to grant access, under section 50 of the Act, to copies of documents with deletions applied to information that I consider would be contrary to the public interest to disclose.

My access decisions are detailed further in the following statement of reasons and the documents released to you are provided as Attachment B to this letter.

In reaching my access decision, I have taken the following into account:

- The FOI Act;
- The contents of the documents that fall within the scope of your request;
- The views of relevant third parties; and
- The Human Rights Act 2004.

Document 6 of the identified documents contains information that I consider, on balance, to be contrary to the public interest to disclose under the test set out in section 17 of the Act as the information could reasonably be expected to divulge business information of a non-government third party.

Public Interest Factors Favouring Disclosure

I have identified that there are no factors favouring disclosure of this information under Schedule 2, section 2.1.

Public Interest Factors Favouring Non-Disclosure

The following factors were considered relevant in favour of the non-disclosure of the documents:

- Schedule 2.2 (a) (xi) Prejudice trade secrets, business affairs or research of an agency or person.

If you have any queries concerning ACT Health Directorate's processing of your request, or would like further information, please contact the FOI Coordinator on (02) 5124 9829 or email HealthFOI@act.gov.au.

Yours sincerely

A handwritten signature in black ink, appearing to be 'John Fletcher', with a long horizontal stroke extending to the right.

John Fletcher
Executive Group Manager
Corporate & Governance

27 June 2019

On balance, the information identified is contrary to the public interest and I have decided not to disclose this information.

Charges

Processing charges are not applicable to this request.

Online publishing – disclosure log

Under section 28 of the Act, ACT Health maintains an online record of access applications called a disclosure log. Your original access application, my decision and documents released to you in response to your access application will be published in the ACT Health disclosure log not less than three days but not more than 10 days after the date of this decision. Your personal contact details will not be published.

Ombudsman review

My decision on your access request is a reviewable decision as identified in Schedule 3 of the Act. You have the right to seek Ombudsman review of this outcome under section 73 of the Act within 20 working days from the day that my decision is published in ACT Health's disclosure log, or a longer period allowed by the Ombudsman.

If you wish to request a review of my decision you may write to the Ombudsman at:

The ACT Ombudsman
GPO Box 442
CANBERRA ACT 2601
Via email: ACTFOI@ombudsman.gov.au.

ACT Civil and Administrative Tribunal (ACAT) review

Under section 84 of the Act, if a decision is made under section 82(1) on an Ombudsman review, you may apply to the ACAT for review of the Ombudsman decision.

Further information may be obtained from the ACAT at:

ACT Civil and Administrative Tribunal
Level 4, 1 Moore St
GPO Box 370
Canberra City ACT 2601
Telephone: (02) 6207 1740
<http://www.acat.act.gov.au/>

FREEDOM OF INFORMATION REQUEST SCHEDULE

Please be aware that under the *Freedom of Information Act 2016*, some of the information provided to you will be released to the public through the ACT Government's Open Access Scheme. The Open Access release status column of the table below indicates what documents are intended for release online through open access.

Personal information or business affairs information will not be made available under this policy. If you think the content of your request would contain such information, please inform the contact officer immediately.

Information about what is published on open access is available online at: <http://www.health.act.gov.au/public-information/consumers/freedom-information>

NAME	WHAT ARE THE PARAMETERS OF THE REQUEST	File No
<div style="background-color: black; width: 100px; height: 20px; margin-bottom: 5px;"></div>	<p>I would like copies of all internal audit reports prepared for ACT Health during 2017-18;</p> <ul style="list-style-type: none"> • ACT Health Internal Audit related to IT Governance and strategic planning performed in 2017-18; • ACT Health Internal Audit related to the effectiveness of ACT Health's implementation of recommendations relating to Data Integrity performed in 2017-18; • ACT Health Internal Audit related to patient safety and Quality Governance processes performed in 2017-18; • ACT Health Internal Audit related to the IT Disaster Recovery Plan performed in 2017-18; • ACT Health Internal Audit related to the University of Canberra Hospital (UCH) project governance; • ACT Health Internal Audit related to asset stocktaking; • Briefings prepared for the Minister for Health and the Director-General of ACT Health regarding the outcome of these reports. 	<p style="text-align: center;">FOI19/20</p>

Ref No	No of Folios	Description	Date	Status	Reason for non-release or deferral	Open Access release status
1.	1 - 24	Synergy - IT Governance and strategic planning review DRAFT Audit Report: 2016-17/2	7 June 2017	Full		Yes
2.	25 - 74	Synergy - Effectiveness of ACT Health's Implementation of Recommendations relating to data integrity	8 May 2018	Full		Yes
3.	75 - 97	PWC - Review of Patient Safety and Quality Governance processes and recommendation implementation	February 2017	Full		Yes
4.	98 – 117	Callida - Internal Audit of Disaster Recovery Arrangements	June 2017	Full		Yes
5.	118 – 136	Callida - Internal Audit of the UCPH Project Governance Review	14 September 2017	Full		Yes
6.	137 - 196	Axiom - Internal Audit of Asset Stocktaking	November 2017	Partial	Schedule 2.2 (a) (xi) Prejudice trade secrets	Yes
Total No of Docs						
6						



IT governance and strategic planning review DRAFT Audit Report: 2016-17/2

Prepared for
Health Directorate (ACT Health)
7 June 2017





Contents

1	Executive summary	3
1.1	Background	3
1.2	Objectives and scope	3
1.3	Conclusion against objectives	4
2	Background	7
2.1	COBIT 5 processes	7
2.2	Process capability assessment overview	7
3	Capability assessment results	9
3.1	Overview of capability assessment	9
3.2	COBIT 5 domain: Evaluate, Direct and Monitor (EDM)	10
3.3	COBIT 5 domain: Align, Plan and Organise (APO)	19
	Appendix A – Definition of COBIT 5 process capability levels	22
	Appendix B – COBIT 5 process descriptions	23
	Appendix C – COBIT 5 RACI (Responsible, Accountable, Consulted, Interested) chart	24



1 Executive summary

1.1 Background

ACT Health is undergoing a major reform agenda involving changes to ICT systems and services, particularly with the introduction of the University of Canberra Public Hospital (UCPH) and supporting new technologies. As part of this reform program, the directorate is also managing a 'Systems Innovation Program', involving over 60 ICT projects.

This Internal Audit of IT Governance and Strategic Planning was approved as part of the *ACT Health 2014-16 Strategic Internal Audit Plan (SIAP)*. An audit, or maturity assessment, in this area will provide a baseline for ACT Health, which can be used in future assessments to determine whether maturity is increasing over time.

Improving IT governance and management brings benefits to organisations, including increased efficiencies, better decision making. A capability assessment against ISACA's COBIT 5 framework¹ addresses key facets of IT governance; being the only governance framework that covers the complete lifecycle of IT investment.

COBIT 5 provides a comprehensive framework for the governance and management of enterprise information and related technologies. The framework is intended to help organisations govern and manage IT in a holistic manner taking in the full end-to-end business and IT areas while considering interests of internal and external stakeholders.

The COBIT 5 framework is based on five domains:

- ▶ Evaluate, Direct and Monitor (EDM)
- ▶ Align, Plan and Organise (APO)
- ▶ Build, Acquire and Implement (BAI)
- ▶ Deliver, Service and Support (DSS)
- ▶ Monitor, Evaluate and Assess (MEA)

Underlying these domains, 37 processes describe the life cycle of governance and management of enterprise IT. This audit utilised the COBIT5 Process Assessment Model (PAM) to assess the capability maturity² of ACT Health's IT activities against seven of these processes specific to IT governance and strategic planning:

- ▶ EDM01 Ensure governance framework setting and maintenance
- ▶ EDM02 Ensure benefits delivery
- ▶ EDM03 Ensure risk optimisation
- ▶ EDM04 Ensure resource optimisation
- ▶ EDM05 Ensure stakeholder transparency
- ▶ APO01 Manage the IT management framework
- ▶ APO02 Manage strategy

1.2 Objectives and scope

The objectives of the review were to provide assurance to ACT Health that initiatives being implemented to strengthen governance structures and arrangements over management of IT 'business as usual' are sound, being managed effectively and progressing appropriately.

¹ www.isaca.org/cobit5

² Refer to Appendix A for a description of the maturity levels used in this review.



1.3 Conclusion against objectives

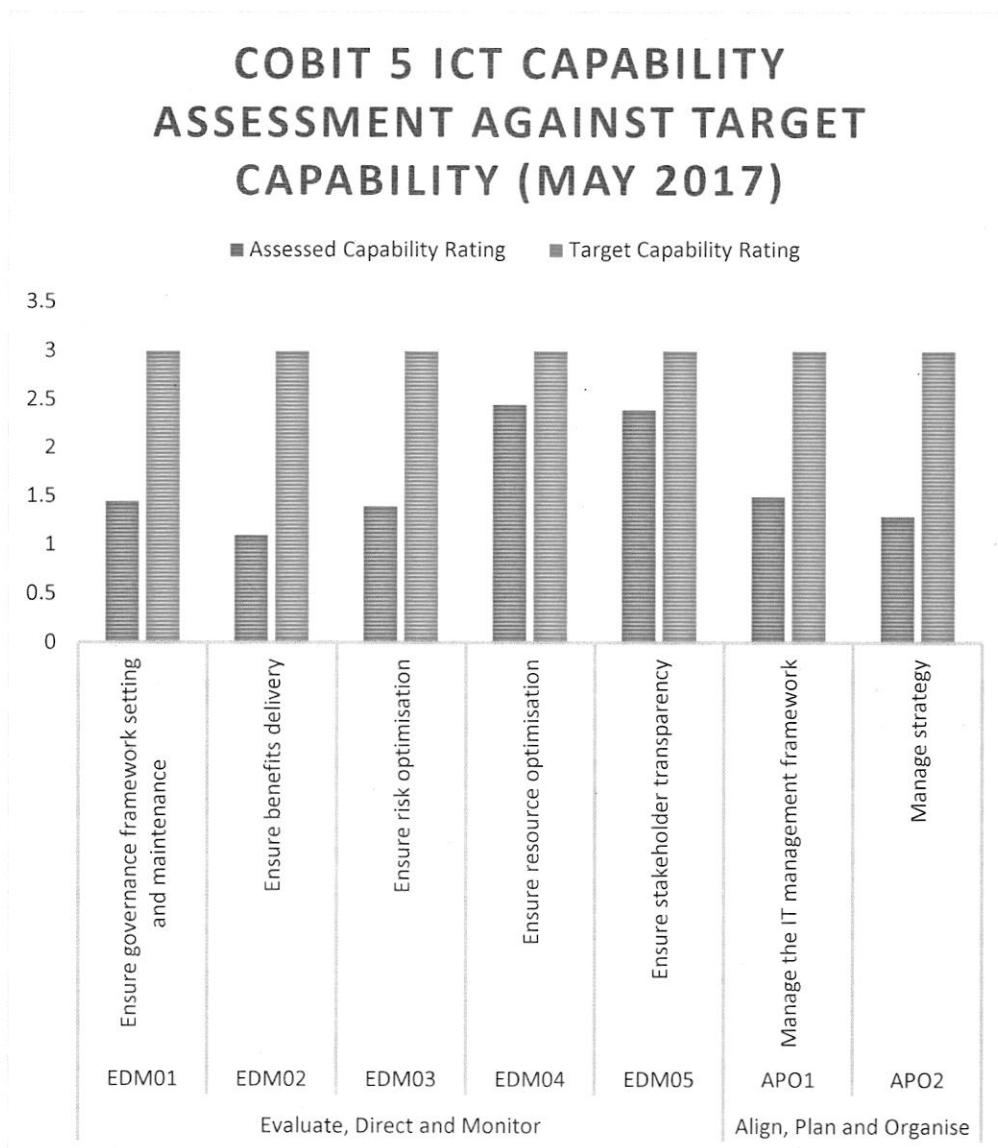
ACT Health’s IT environment has recently undergone significant change and restructure. The Chief Information Officer (CIO) has acknowledged a need to apply more rigour and structure around IT management and enabling processes with recent IT improvement activities a testament to this. However, ACT Health’s Digital Solutions Division (DSD) should focus on endorsing and implementing the new Digital Health Strategy and ensuring that benefits, risks and resources are appropriately assessed and managed.

The CIO has indicated a preference to achieve a capability maturity target of ‘3 – Established’ for all IT processes reviewed. Assessment of the agreed seven COBIT 5 processes relating to IT governance and strategic planning indicates all processes need further maturing to meet that target maturity rating.

This report identifies gaps between target capability levels and actual capability levels with a recommendation that ACT Health review its progress against achieving the target maturity level in 12 months.

A summary of the process assessment results can be found in the following section. The assessment should help to provide a way forward to assist ACT Health improve its overall IT governance, management arrangements and mitigate potential risks.

A summary of process capability assessment ratings is shown below:



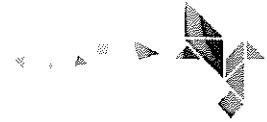


Recommendations

Two recommendations have been identified to assist ACT Health in achieving greater levels of maturity in the IT governance and strategic planning processes.

This includes business improvement opportunity that may further assist ACT Health in maturing its IT processes overall.

Recommendation 1	Based on the issues identified and the capability ratings it is suggested that ACT Health re-assess its capability maturity for, at a minimum, the seven processes relating to IT governance and strategic planning in 12 months. This will determine if the planned changes and initiatives are having a positive effect on process maturity.
Rating	High
Management Comments	Agreed ACT Health through the internal audit process will seek a reassessment of its ICT capability maturity in 12 months.
Action Officer	Director, Future Capability and Governance, Digital Solutions Division
Timeframe for Implementation	31 October 2018
Recommendation 2	Conduct a full COBIT 5 capability maturity assessment (covering all 37 processes) against prioritised IT goals to establish a baseline for all IT development, operations, service delivery, support and governance processes. This will assist to focus resources, and improvements, on the most critical processes.
Rating	Business Improvement Opportunity
Management Comments	Agreed ACT Health through the internal audit process will seek a full COBIT 5 capability maturity assessment.
Action Officer	Director, Future Capability and Governance, Digital Solutions Division
Timeframe for Implementation	30 June 2018



Management sign off

This report has been reviewed and discussed with management of the ACT Health Directorate. Management has had the opportunity to express any comments on the findings and recommendations outlined in this report.

Peter O'Halloran, Chief Information Officer

Digital Solutions Division

ACT Health

Shaun Strachan, Deputy Director-General

Corporate

ACT Health

Johan Pretorius

Internal Audit

ACT Health

Diana Hamono

Director

Synergy Group





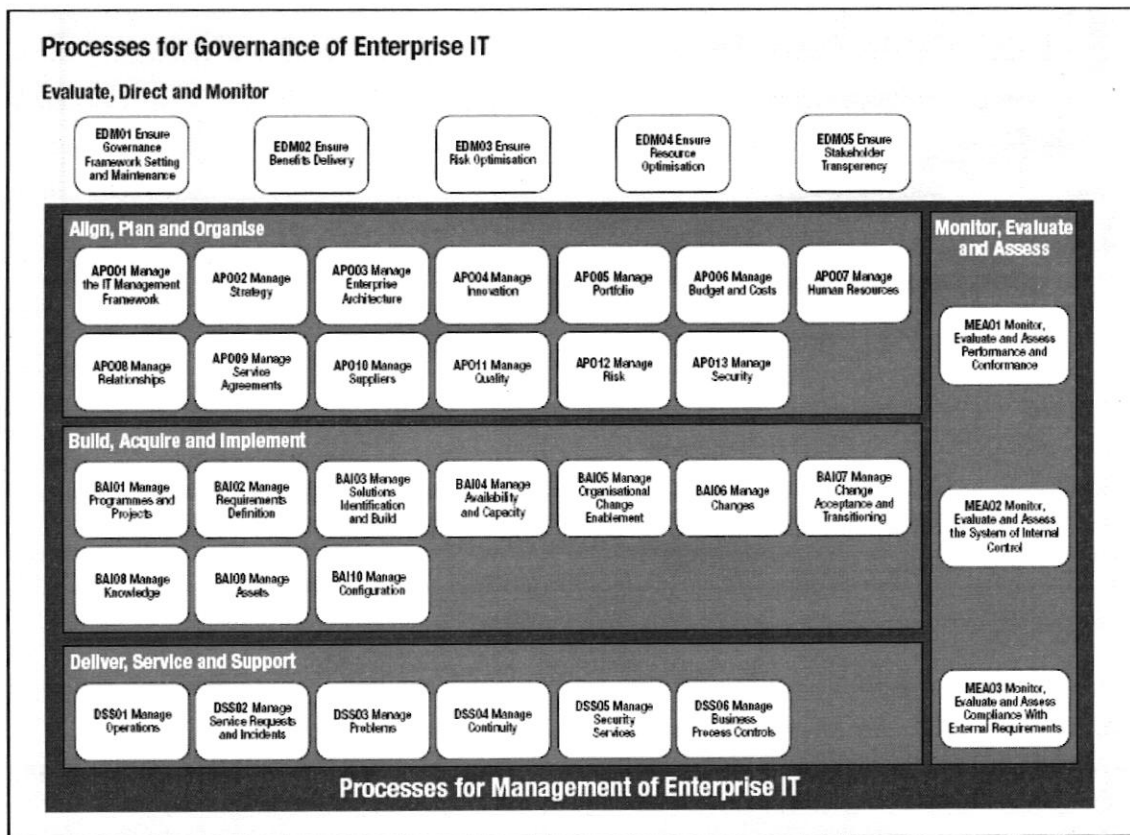
2 Background

2.1 COBIT 5 processes

COBIT 5 is an IT governance framework used across the world by organisations to help improve in the governance and management IT. For ACT Health (Digital Solutions Division, DSD), assessing the processes relevant to IT governance and strategic planning will assist in prioritising resources to help increase process capability maturity levels and bring greater efficiencies, IT service delivery, management and control.

Shown below is an overview diagram of the COBIT 5 process framework (ISACA, 2013) showing the five domains and 37 supporting processes for the governance of enterprise IT.

Diagram 1: COBIT 5 Processes for Governance and Enterprise IT (Source: COBIT® 5, Figure 16. © 2012 ISACA® All Rights Reserved)



2.2 Process capability assessment overview

What is a process capability assessment?

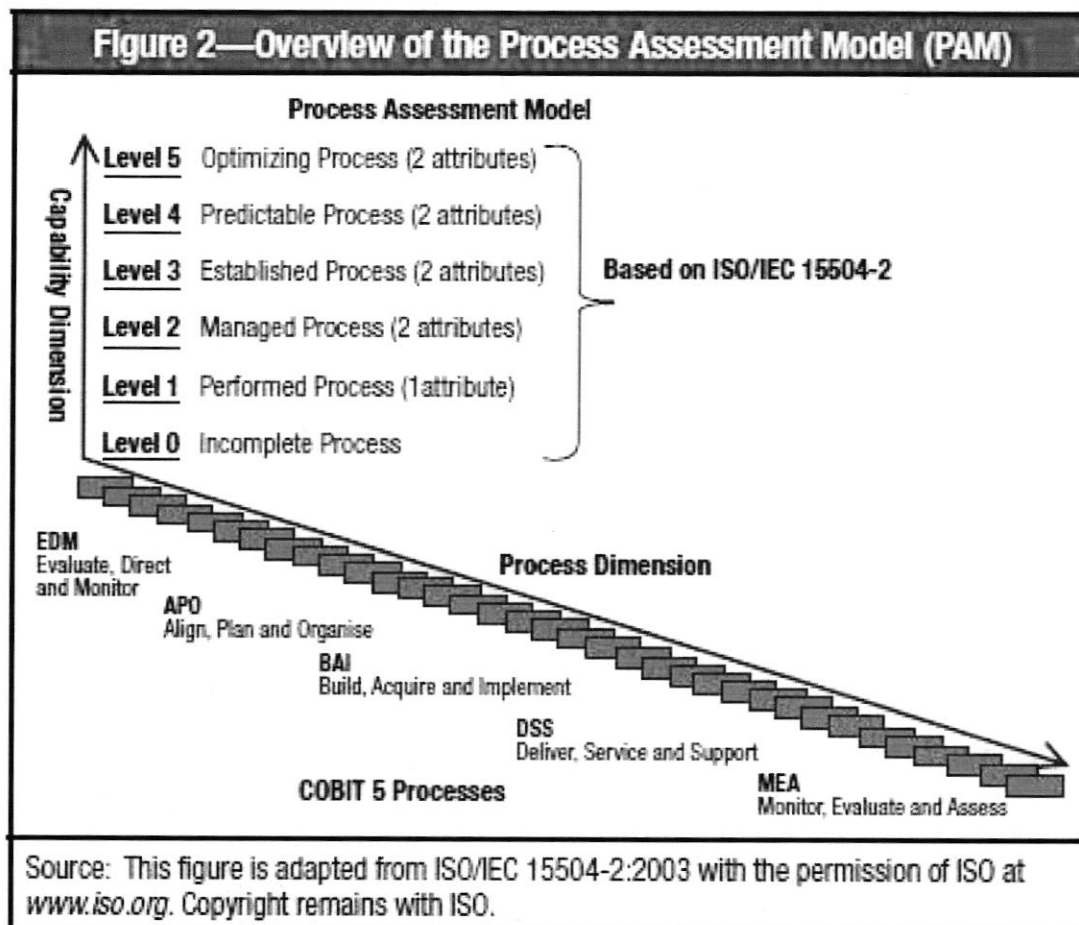
This process capability assessment of ACT Health's IT environment used the guidance of ISACA's COBIT 5 Process Assessment Model (ISACA, 2013) to assess capability ratings for each of the seven related COBIT 5 processes shown in the above diagram.

The assessment results provide ACT Health with a determination of process capability that can be used for process improvement, delivering value to the business, measuring the achievement of current or projected business goals, benchmarking, consistent reporting and organisational compliance with regulatory requirements.



The rating scale involved six (6) capability levels:

Diagram 2: Overview of the Process Assessment Model (Figure 2, COBIT 5 Process Assessment Model (PAM): Using COBIT 5, 2013)



An

explanation of each of these ratings can be found in Attachment A.

How were the processes assessed?

The COBIT 5 Process Assessment Model (PAM) was used as a guide to assess each of the seven processes. Coupled with the information in the COBIT PAM, a COBIT 5 self-assessment tool (available through ISACA) was tailored by the audit team to enable an assessment of ACT Health's capability for the seven selected IT processes.

Key people were interviewed together with a high-level review of a range of relevant documentation. Note that the COBIT 5 process assessment approach followed did not require a detailed assessment of the processes and did not require evidentiary requirements in support of the assessment. In other words, this is not an audit, rather a maturity assessment.

Results from the interviews and the documentation review were analysed to assess the most relevant rating for each process. These ratings were captured in the assessment tool, summarised and graphed.

Based on the issues identified and the capability ratings it is suggested that ACT Health re-assess its capability maturity for these processes in 12 months. This will determine if the planned changes and initiatives are having a positive effect on process maturity.

This process and the results were discussed and agreed with DSD management and are described in the following section.



3 Capability assessment results

3.1 Overview of capability assessment

	Level 0 Incomplete	Level 1 Performed	Level 2 Managed	Level 3 Established	Level 4 Predictable	Level 5 Optimizing
		PA 1.1	PA 2.1 PA 2.2	PA 3.1 PA 3.2	PA 4.1 PA 4.2	PA 5.1 PA 5.2
	Process Performance Performance Management Work Product Management Process Definition Process Deployment Process Measurement Process Control Process Innovation Process Optimization					
LEGEND	Partially Achieved Largely Achieved Fully Achieved					
ALL SELECTED PROCESSES						
EDM01 Ensure Governance Framework Setting and Maintenance						GOAL LEVEL 3
EDM02 Ensure Benefits Delivery						GOAL LEVEL 3
EDM03 Ensure Risk Optimisation						GOAL LEVEL 3
EDM04 Ensure Resource Optimisation						GOAL LEVEL 3
EDM05 Ensure Stakeholder Transparency						GOAL LEVEL 3
APO01 Manage the IT Management Framework						GOAL LEVEL 3
APO02 Manage Strategy						GOAL LEVEL 3

3.2 COBIT 5 domain: Evaluate, Direct and Monitor (EDM)

EDM01: Ensure governance framework setting and maintenance

Purpose: To provide a consistent approach integrated and aligned with the enterprise governance approach. To ensure that IT-related decisions are made in line with the ACT Health strategies and objectives, ensure that IT-related processes are overseen effectively and transparently, compliance with legal and regulatory requirements is confirmed, and the governance requirements for board members are met.

	Assess whether the following outcomes are achieved.	Criteria	Audit comments	Not Achieved	Partially Achieved	Largely Achieved	Fully Achieved
Level 0 Incomplete	The process is implemented or achieves its process purpose.	At this level, there is evidence of achievement of the process purpose.	ACT Health is showing signs of wanting to integrate a consistent approach across the organisation. Recent activities such as a restructure, replacement of the CIO, new governance structures / framework will assist ACT Health move towards a fully achieved EDM01 - Ensuring Governance Framework Setting. This element of the process has been rated as largely achieved.			✓	
Level 1 Performed	PA 1.1 The implemented process achieves its process purpose.	The following process outcomes are being achieved: EDM01-O1 Strategic decision-making model for IT is effective and aligned with the enterprise's internal and external environment and stakeholder requirements. EDM01-O2 The governance system for IT is embedded in the enterprise.	ACT Health's IT strategic decision-making model is partially effective. This rating has been assigned as at the time of review the governance model was in draft. Once fully operational, this should support a better alignment, with both internal and external stakeholders. The governance system within ACT Health has historically not provided the benefits expected. However, improvements are being planned in this area, including review of policies, procedures, updated committee structures and better communication, which should help to reap the benefits of good		✓		

	Assess whether the following outcomes are achieved.	Criteria	Audit comments	Not Achieved	Partially Achieved	Largely Achieved	Fully Achieved
		EDM01-03 Assurance is obtained that the governance system for IT is operating effectively.	<p>governance. ACT Health has not historically assessed the effectiveness of its IT governance arrangements until recently.</p> <p>Internal Audit has not conducted any audit activities across the IT environment in recent years. It was noted however that some reviews had been commissioned by ACT Health for example the Protiviti Financial Assessment Review of E-Healthy Future Program.</p>				

EDM02: Ensure benefits delivery

Purpose: To secure optimal value from IT-enabled initiatives, services and assets; cost-efficient delivery of solutions and services; and a reliable and accurate picture of costs and likely benefits so that ACT Health's business needs are supported effectively and efficiently.

	Assess whether the following outcomes are achieved.	Criteria	Audit comments	Not Achieved	Partially Achieved	Largely Achieved	Fully Achieved
Level 0 Incomplete	The process is implemented or achieves its process purpose.	At this level, there is evidence of achievement of the process purpose.	ACT Health's achievement around benefits realisation is ad hoc. The establishment of the Project Management Office in 2017 should lead to improved management of benefits across all projects and the alignment to strategic objectives.			✓	
Level 1 Performed	PA 1.1 The implemented process achieves its process purpose.	<p>The following process outcomes are being achieved:</p> <p>EDM02-O1 The enterprise is securing optimal value from its portfolio of approved IT- enabled initiatives, services and assets.</p> <p>EDM02-O2 Optimum value is derived from IT investment through effective value management practices in the enterprise.</p> <p>EDM02-O3 Individual IT- enabled investments contribute optimal value.</p>	Some projects have aligned their benefits with strategic goals and have plans to manage these throughout the life of the project. Though this practice is ad hoc and is not fully embedded into general practice across the organisation.	✓			

EDM03: Ensure risk optimisation

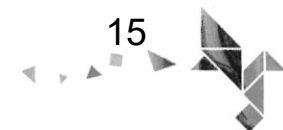
Purpose: To ensure that ACT Health’s IT-related risks do not exceed risk appetite and risk tolerance, the impact of IT risk to ACT Health’s value is identified and managed, and the potential for compliance failures is minimised.

	Assess whether the following outcomes are achieved.	Criteria	Audit comments	Not Achieved	Partially Achieved	Largely Achieved	Fully Achieved
Level 0 Incomplete	The process is implemented or achieves its process purpose.	At this level, there is evidence of achievement of the process purpose.	<p>The DSD has developed a risk management process (April 2017) that is aligned to ACT Health's Risk Management Framework and covers the tiers of governance (e.g. organisational, group, divisional, team/program/project).</p> <p>At the time of this review, Internal Audit did not see evidence to support the operationalisation of this risk management process.</p>			✓	
Level 1 Performed	PA 1.1 The implemented process achieves its process purpose.	<p>The following process outcomes are being achieved:</p> <p>EDM03-O1 Risk thresholds are defined and communicated and key IT- related risk is known.</p> <p>EDM03-O2 The enterprise is managing critical IT-related enterprise risk effectively and efficiently.</p> <p>EDM03-O3 IT-related enterprise risk does not exceed risk appetite and the impact of IT risk to enterprise value is identified and managed.</p>	<p>While ACT Health manages risks across IT projects, the risk appetite is not formally articulated which may lead to difficulties in the ongoing monitoring of risks throughout the life of the projects.</p> <p>DSD's new risk management process outlines the requirements for managing risks for ACT Health IT developments. Key IT-related risks are being provided to the Executive Directors Council.</p> <p>A risk register for Tier 3 DSD projects is being maintained but is marked as Draft. A Tier 2 risk register exists, but is not being maintained.</p>		✓		

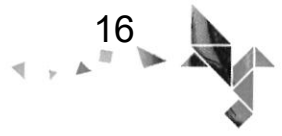
EDM04: Ensure resource optimisation


Purpose: To ensure that ACT Health’s resource needs are met in the optimal manner, IT costs are optimised, and there is an increased likelihood of benefit realisation and readiness for future change.

	Assess whether the following outcomes are achieved.	Criteria	Audit comments	Not Achieved	Partially Achieved	Largely Achieved	Fully Achieved
Level 0 Incomplete	The process is implemented or achieves its process purpose.	At this level, there is evidence of achievement of the process purpose.	<p>ACT Health is undergoing an IT strategic planning exercise (with the development of a new Digital Health Strategy) and has established an enterprise architecture team (January 2017).</p> <p>Until the strategic direction and future projects are known and approved, ACT Health is not in a position to fully understand its resource requirements.</p> <p>The financial management of ACT Health's IT activities was reviewed in October 2016 by Protiviti. That review identified a number of weaknesses. However, improvements have since been made, with changes to the way budgeting, expenditure tracking and software capitalisation is conducted.</p>				✓
Level 1 Performed	PA 1.1 The implemented process achieves its process purpose.	<p>The following process outcomes are being achieved:</p> <p>EDM04-O1 The resource needs of the enterprise are met with optimal capabilities.</p> <p>EDM04-O2 Resources are allocated to best meet enterprise priorities within budget constraints.</p>	<p>Financial needs are determined each year as part of a budget planning and forecasting exercise. This is done in conjunction with ACT Health Central Finance team and the broader requirements of ACT Treasury.</p> <p>Since November/ December 2016, changes to how budgets are prepared and monitored have improved financial management in DSD.</p>				✓



	Assess whether the following outcomes are achieved.	Criteria	Audit comments	Not Achieved	Partially Achieved	Largely Achieved	Fully Achieved
Level 2 Managed	PA 2.1 Performance Management - A measure of the extent to which the performance of the process is managed.	<p>EDM04-O3 Optimal use of resources is achieved throughout their full economic life cycles.</p> <p>The following process outcomes are being achieved:</p> <p>A) Objectives for the performance of the process are identified.</p> <p>B) Performance of the process is planned and monitored.</p> <p>C) Performance of the process is adjusted to meet plans.</p> <p>D) Responsibilities and authorities for performing the process are defined, assigned and communicated.</p> <p>E) Resources and information necessary for performing the process are identified, made available, allocated and used.</p> <p>F) Interfaces between the involved parties are managed to ensure both effective communication and also clear assignment of responsibility.</p>	<p>Improvements are underway in helping to optimise resources in ACT Health's DSD.</p> <p>Full cost/benefits management is not currently occurring. Further work needs to occur on realising benefits as part of improving project benefits management processes.</p>				

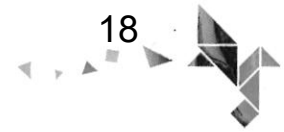



	Assess whether the following outcomes are achieved.	Criteria	Audit comments	Not Achieved	Partially Achieved	Largely Achieved	Fully Achieved
	PA 2.2 Work Product Management - A measure of the extent to which the work products produced by the process are appropriately managed. The work products (or outputs from the process) are defined and controlled.	The following process outcomes are being achieved: A) Requirements for the work products of the process are defined. B) Requirements for documentation and control of the work products are defined. C) Work products are appropriately identified, documented, and controlled. D) Work products are reviewed in accordance with planned arrangements and adjusted as necessary to meet requirements.	DSD are continuing to refine their processes around resource management. Responsibilities are assigned and the DSD finance team is working closely with Treasury and the ACT Health central finance team to improve budgeting, forecasting and reporting arrangements. Further bedding down of these responsibilities and processes is still occurring.				

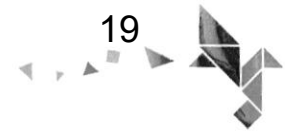
EDM05: Ensure stakeholder transparency

Purpose: To make sure that the communication to stakeholders is effective and timely and the basis for reporting is established to increase performance, identify areas for improvement, and confirm that IT-related objectives and strategies are in line with ACT Health’s strategy.

	Assess whether the following outcomes are achieved.	Criteria	Audit comments	Not Achieved	Partially Achieved	Largely Achieved	Fully Achieved
Level 0 Incomplete	The process is implemented or achieves its process purpose.	At this level, there is evidence of achievement of the process purpose.	<p>Stakeholder communication in ACT Health occurs through the recently updated governance arrangements (e.g. tiered governance model).</p> <p>Policies, procedures and other stakeholder communication and engagement occurs through publishing of information on the intranet, staff tutorials, emails, newsletters etc.</p>				✓
Level 1 Performed	PA 1.1 The implemented process achieves its process purpose.	<p>The following process outcomes are being achieved:</p> <p>EDM05-O1 Stakeholder reporting is in line with stakeholder requirements.</p> <p>EDM05-O2 Reporting is complete, timely and accurate.</p> <p>EDM05-O3 Communication is effective and stakeholders are satisfied.</p>	<p>Stakeholder engagement is occurring at all levels from within ACT Health's IT area. This includes IT strategic planning down to project level communications and outage reporting.</p> <p>As part of this review, Synergy did not undertake an assessment on whether stakeholders are satisfied. Though the DSD Governance team does endeavour to capture satisfaction levels with stakeholders through various means, including evaluations of communications throughout the projects as documented in the Change Management Plans.</p> <p>The DSD Governance team also conduct project Post Implementation Reviews and complete project closure documentation, where considered necessary or appropriate.</p> <p>Additionally, DSD run System Administration forums to</p>			✓	



	Assess whether the following outcomes are achieved.	Criteria	Audit comments	Not Achieved	Partially Achieved	Largely Achieved	Fully Achieved
			capture feedback around specific applications. Staff are requested to log jobs in the SSICT Service Now tool, specific to ACT Health, for issues pertaining to ICT and then they track and work through priority issues.				
Level 2 Managed	PA 2.1 Performance Management - A measure of the extent to which the performance of the process is managed.	<p>The following process outcomes are being achieved:</p> <p>A) Objectives for the performance of the process are identified.</p> <p>B) Performance of the process is planned and monitored.</p> <p>C) Performance of the process is adjusted to meet plans.</p> <p>D) Responsibilities and authorities for performing the process are defined, assigned and communicated.</p> <p>E) Resources and information necessary for performing the process are identified, made available, allocated and used.</p> <p>F) Interfaces between the involved parties are managed to ensure both effective communication and also clear assignment of responsibility.</p>	<p>DSD is working on Key Performance Indicators (KPIs) for measuring the effectiveness of IT services. They are currently implementing changes to DSD support and early engagement areas of DSD. It is intended that KPI's will be captured and reported through the Tier 1 ICT and IM Executive Committee, however this may not be completed until early to mid-2018.</p> <p>DSD is consolidating 17 different ICT support lines in through one call manager / help desk. These measures will help to improve the engagement with stakeholders and provide greater transparency over the activities of DSD.</p>				



3.3 COBIT 5 domain: Align, Plan and Organise (APO)

APO01: Manage the IT management framework

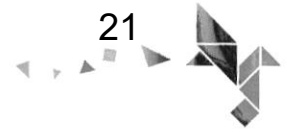
Purpose: To provide a consistent management approach to enable ACT Health's governance requirements to be met, covering management processes, organisational structures, roles and responsibilities, reliable and repeatable activities, and skills and competencies.

	Assess whether the following outcomes are achieved.	Criteria	Audit comments	Not Achieved	Partially Achieved	Largely Achieved	Fully Achieved
Level 0 Incomplete	The process is implemented or achieves its process purpose.	At this level, there is evidence of achievement of the process purpose.	<p>Since the appointment of new DDG and CIO, ACT Health's IT management arrangements are showing positive signs of improvement.</p> <p>Roles and responsibilities are being progressively defined, with roles being aligned within the governance framework. For example, recent recruitment activity for a dedicated contract manager has been aligned to DSD's strategic objectives. The revised governance framework includes more appropriate structures within DSD, including the repositioning of the IT infrastructure business unit to report up to the CIO.</p>			✓	
Level 1 Performed	PA 1.1 The implemented process achieves its process purpose.	<p>The following process outcomes are being achieved:</p> <p>APO01-O1 An effective set of policies is defined and maintained.</p> <p>APO1-O2 Everyone is aware of the policies and how they should be implemented.</p>	<p>The establishment of an enterprise architecture team (January 2017) will help to focus the work of DSD on strategic priorities. ACT Health recently revised its governance structures, including tier 1, 2, 3 and 4 committees (depending on the nature of the project/program). These are yet to be endorsed by Executive Management Group.</p>		✓		

APO02: Manage strategy

Purpose: To align strategic IT plans with business objectives. Clearly communicate the objectives and associated accountabilities so they are understood by all, with the IT strategic options identified, structured and integrated with the business plans

	Assess whether the following outcomes are achieved.	Criteria	Audit comments	Not Achieved	Partially Achieved	Largely Achieved	Fully Achieved
Level 0 Incomplete	The process is implemented or achieves its process purpose.	At this level, there is evidence of achievement of the process purpose.	<p>ACT Health has a current Digital e-Health Strategy 2015-2017. It was acknowledged that the value of this strategy is questionable, and is no longer aligned with current structures and direction.</p> <p>Plans are underway to develop a new Digital Health Strategy to be launched in September / October 2017.</p>				✓
Level 1 Performed	PA 1.1 The implemented process achieves its process purpose.	<p>The following process outcomes are being achieved:</p> <p>APO02-O1 All aspects of the IT strategy are aligned with the enterprise strategy.</p> <p>APO02-O2 The IT strategy is cost-effective, appropriate, realistic, achievable, enterprise-focused and balanced.</p> <p>APO02-O3 Clear and concrete short-term goals can be derived from, and traced back to, specific long-term initiatives, and can then be translated into operational plans.</p>	<p>The current Digital e-Health Strategy does not fully achieve the outcomes of this process.</p> <p>Full achievement of the process outcomes should be met with the introduction of the updated Digital Health Strategy.</p>	✓			



	Assess whether the following outcomes are achieved.	Criteria	Audit comments	Not Achieved	Partially Achieved	Largely Achieved	Fully Achieved
		<p>APO02-04 IT is a value driver for the enterprise.</p> <p>APO02-05 There is awareness of the IT strategy and a clear assignment of accountability for delivery.</p>					



Appendix A – Definition of COBIT 5 process capability levels

Capability Level	Explanation
Level 0 Incomplete process	The process is not implemented or fails to achieve its process purpose. At this level, there is little or no evidence of any systematic achievement of the process purpose.
Level 1 Performed process	The implemented process achieves its process purpose.
Level 2 Managed process	The previously described <u>performed</u> process is now implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.
Level 3 Established process	The previously described <u>managed</u> process is now implemented using a defined process that is capable of achieving its process outcomes.
Level 4 Predictable process	The previously described <u>established</u> process now operates within defined limits to achieve its process outcomes.
Level 5 Optimising process	The previously described <u>predictable</u> process is continuously improved to meet relevant current and projected business goals.

Source – COBIT5 Process Assessment Model (PAM): Using COBIT5 (ISACA, 2013)

Appendix B – COBIT 5 process descriptions

This attachment describes each of the seven COBIT 5 processes assessed during this review.

Evaluate, Direct and Monitor

COBIT5 Process	Purpose
EDM01 – Ensure governance framework setting and maintenance	Provide a consistent approach integrated and aligned with the enterprise governance approach. To ensure that IT-related decisions are made in line with the enterprise’s strategies and objectives, ensure that IT-related processes are overseen effectively and transparently, compliance with legal and regulatory requirements is confirmed, and the governance requirements for board members are met.
EDM02 – Ensure benefits delivery	Secure optimal value from IT-enabled initiatives, services and assets; cost-efficient delivery of solutions and services; and a reliable and accurate picture of costs and likely benefits so that business needs are supported effectively and efficiently.
EDM03 – Ensure risk optimisation	Ensure that IT-related enterprise risk does not exceed risk appetite and risk tolerance, the impact of IT risk to enterprise value is identified and managed, and the potential for compliance failures is minimised.
EDM04 – Ensure resource optimisation	Ensure that the resource needs of the enterprise are met in the optimal manner, IT costs are optimised, and there is an increased likelihood of benefit realisation and readiness for future change.
EDM05 – Ensure stakeholder transparency	Make sure that the communication to stakeholders is effective and timely and the basis for reporting is established to increase performance, identify areas for improvement, and confirm that IT-related objectives and strategies are in line with the enterprise’s strategy.

Align, Plan and Organise

COBIT5 Process	Purpose
APO01 – Manage the IT management framework	Provide a consistent management approach to enable the enterprise governance requirements to be met, covering management processes, organisational structures, roles and responsibilities, reliable and repeatable activities, and skills and competencies.
APO02 – Manage strategy	Align strategic IT plans with business objectives. Clearly communicate the objectives and associated accountabilities so they are understood by all, with the IT strategic options identified, structured and integrated with the business plans.



Effectiveness of ACT Health's Implementation of Recommendations Relating to Data Integrity: Phase Four Review (March 2018)

INTERNAL AUDIT FINAL REPORT

Prepared for
ACT Health Directorate
8 May 2018

Contents

1	Background	3
2	Audit scope and focus	3
3	Audit objective	3
4	Method and approach	4
5	Final assessment	4
	5.1 Summary of final assessment	5
	5.2 Effectiveness of implementation activities for completed recommendations	11
	Appendix A – Full list of recommendations and status as at March 2018	28
	Appendix B – Statement of responsibility	50



1 Background

From 2012 to 2016 the ACT Health Directorate endured a range of external reviews to investigate issues faced regarding data management and reporting. Resulting from these reviews, 175 recommendations were made with the intention of addressing these issues. In early 2017, the Minister for Health announced that a System-Wide Review of ACT Health Data (SWR) be undertaken.

On 28 March 2017, the Terms of Reference (ToR) for the SWR was released in the ACT Legislative Assembly with work to be conducted through until 31 March 2018. Some of the activities within the SWR included managing the implementation of the 175 recommendations over the 14-month period.

An ACT Health Internal Audit was commissioned to provide an independent, progressive, assessment of the effectiveness of progress made against the implementation of the 175 recommendations over the 14-month SWR period.

2 Audit scope and focus

As mentioned previously, the ACT Health Directorate has 175 recommendations resulting from at least eight different reviews over the last five years by the ACT Audit Office and external service providers. These reviews resulted in:

- ▶ seven PwC reports (40 recommendations)
- ▶ two Auditor-General's Office reports (30 recommendations)
- ▶ two independent reports (89 recommendations)
- ▶ one Standing Committee on Public Accounts report (16 recommendations)

A team within ACT Health Directorate's Performance, Reporting and Data Branch (formerly the Business Performance Information Decision Support (BPIDS) Branch) has been established to address the recommendations and other aspects of the SWR.

The activities of the SWR, including addressing the recommendations, have been divided across six pillars of work with varying deliverables and targets:

- ▶ Milestone One – 30 June 2017 addresses a range of activities within the SWR ToR under Pillars 2, 3 and 5
- ▶ Milestone Two – 30 September 2017 addresses a range of activities within the SWR under Pillars 1, 3 and 6.
- ▶ Milestone Three – 31 March 2018 – this is the final milestone and addresses activities within the SWR under Pillars 2 and 4.

3 Audit objective

In a phased approach, the objective of this internal audit is, for:

- ▶ each recommendation, provide an independent assessment of progress (i.e. not started, underway, ongoing, completed, or no longer relevant¹)
- ▶ completed recommendations, evidence the control effectiveness of the implementation.

This phased audit is to assess and complete a [provided] spreadsheet on the implementation of the recommendations every three months. An initial baseline review was completed at the end of June 2017. Three progress reviews were subsequently conducted at the end of September 2017, end of December 2017 and end of March 2018.

¹ Noting that the 'no longer relevant' status was previously referred to as 'not applicable'



This report summarises the final assessment outcomes in relation to the implementation effectiveness of the 175 recommendations.

4 Method and approach

To date, this review has followed the following approach:

- ▶ Obtained the reports associated with each of the 175 recommendations.
- ▶ Reviewed reports to appropriately understand the underlying finding and associated risk.
- ▶ Liaised with the SWR team to:
 - ◆ Confirm the status of recommendations and the actions taken to address the original recommendation / risk.
 - ◆ Obtain supporting evidence to verify the stated status of the recommendations.
- ▶ For all recommendations, based on the evidence provided, rate the implementation status as follows:
 - ◆ Completed – the recommendation has been completed.
The action taken meets the intent of the recommendation and sufficient supporting evidence was provided to Internal Audit to demonstrate action taken.
 - ◆ Underway – various activities have commenced to address the recommendation with the following reasons for non-completion:
 - Action taken was less extensive than recommended, fell short of the intent of the recommendation, or only addressed some of the identified risks.
 - The business unit may have established a process or procedure to address an issue, however, the specific action noted in the recommendation was not complete at the time of the assessment.
 - The business unit may have commenced action to address a recommendation but subsequent policy changes may influence how it might be implemented.
 - ◆ Not started – no work has commenced to address the recommendation with the following reasons for non-commencement:
 - There is no supporting evidence that action has been undertaken.
 - The action taken does not address the recommendation.
 - ◆ Ongoing – the nature of the recommendation requires work to be done as an ongoing activity. There is no possibility of this recommendation being completed.
 - ◆ No longer relevant – the recommendation is no longer relevant in the current environment.
 - ◆ Under investigation – Internal Audit is still investigating the progress of the implementation of the recommendation. This status was used during the first stage review of recommendations in June 2017.
- ▶ For recommendations in progress, determined whether current implementation actions, once implemented, will meet the intent of the recommendation.
- ▶ Identified and reported any instances where the completed recommendation has not been implemented and the original risk remains.
- ▶ Provided a summary of the assessment of progress against recommendations at the end of each phase review.
- ▶ Provided a final assessment of the progress of the recommendations to align with the final SWR report at the end of March 2018.

5 Final assessment

In March 2018 (the end of the 14-month SWR period), Synergy undertook the final assessment of the progress towards implementing all 175 recommendations. In this final assessment, the effectiveness of the activities implemented to address the 'completed' recommendations were also determined.

Similar to the previous assessments, discussions were held with relevant staff identified as being the owner/s of the recommendations within the ACT Health Directorate, The Canberra Hospital and Calvary Hospital. The



spreadsheet used in the previous assessments was updated to reflect the status of each recommendation. Where recommendations were deemed to have been completed during this final assessment period, sufficient and available evidence was sighted or obtained and an assessment was made as to whether the recommendation had been effectively completed.

5.1 Summary of final assessment

In the nine months since Synergy commenced the audit, noticeable data management and governance improvements are evident. Since the release of the Terms of Reference for the “System-Wide Review of Data” on 28 March 2017, the Directorate has made considerable progress to improving processes for how data is collected, secured, stored, altered, validated and reported. Some of these activities include:

- ▶ New governance arrangements, including structural changes, to provide for greater consideration to be given to complex data management related issues.
- ▶ IT system changes and improvements have occurred.
- ▶ Improvements to security and access to key systems through the introduction of single sign on and identify and access management systems by the Digital Solutions Division (DSD).
- ▶ Training and e-learning packages and processes now incorporate security awareness information.
- ▶ Improvements in quality assurance over clinical coding in the hospitals.

The implementation of the newly developed *ACT Health Performance Reporting and Data Strategy*, including the nine Health Informatics Domains² and 57 related activities, or projects, will address many of the recommendations, or the intent of those recommendations. For example, Synergy's final assessment concludes that 13 recommendations that are currently 'underway' are being addressed through 'Activity D2.5 - Data Governance, Assurance and Management Framework' and 10 recommendations that are currently 'underway' are being addressed through 'Activity D1.5 – System Upgrade'.

Diagram 1 on the following page illustrates how all 'underway' recommendations will be addressed by the Informatics Domain activities and projects.

While some recommendations are taking longer than originally expected to complete, when implemented, the Directorate should be in a good position as it moves into a period where high quality, repeatable and instant reporting is demanded.

This final audit assessment concludes that:

- ▶ 69 recommendations have been completed with reasonable evidence to support the effectiveness of the implementation of the recommendation, or the original intent of the recommendation.
- ▶ 70 recommendations are underway. The Directorate is progressing with a range of activities, such as the:
 - ◆ full development and use of the new data warehousing capability
 - ◆ finalisation and endorsement of a range of data related policies, procedures and templates
 - ◆ establishment and implementation of a Change Control Board and process that incorporates data and report changes
 - ◆ implementation of over 50 informatics related activities, including a metadata management model, and a data quality framework.
- ▶ 15 recommendations remain ongoing. These recommendations relate to activities considered to be 'improvement' or 'business as usual' activities that will continue to occur into the future. This includes various elements of the *ACT Health Performance Reporting and Data Strategy* such as staff training and awareness, clinical coding quality checking and system access monitoring activities.
- ▶ 21 recommendations are no longer considered relevant in the current environment. For example, the new data warehouse capability and technology now being developed will allow for different methods

² The nine domains are: D1 Data Management, D2 Data Governance, D3 Data Quality, D4 Metadata Management, D5 Data Security and Privacy, D6 Workforce, D7 Communications, D8 Change Management and D9 Information and Insights.

of validating data entering the warehouse, thereby negating some very specific recommendations made in the previous reports.

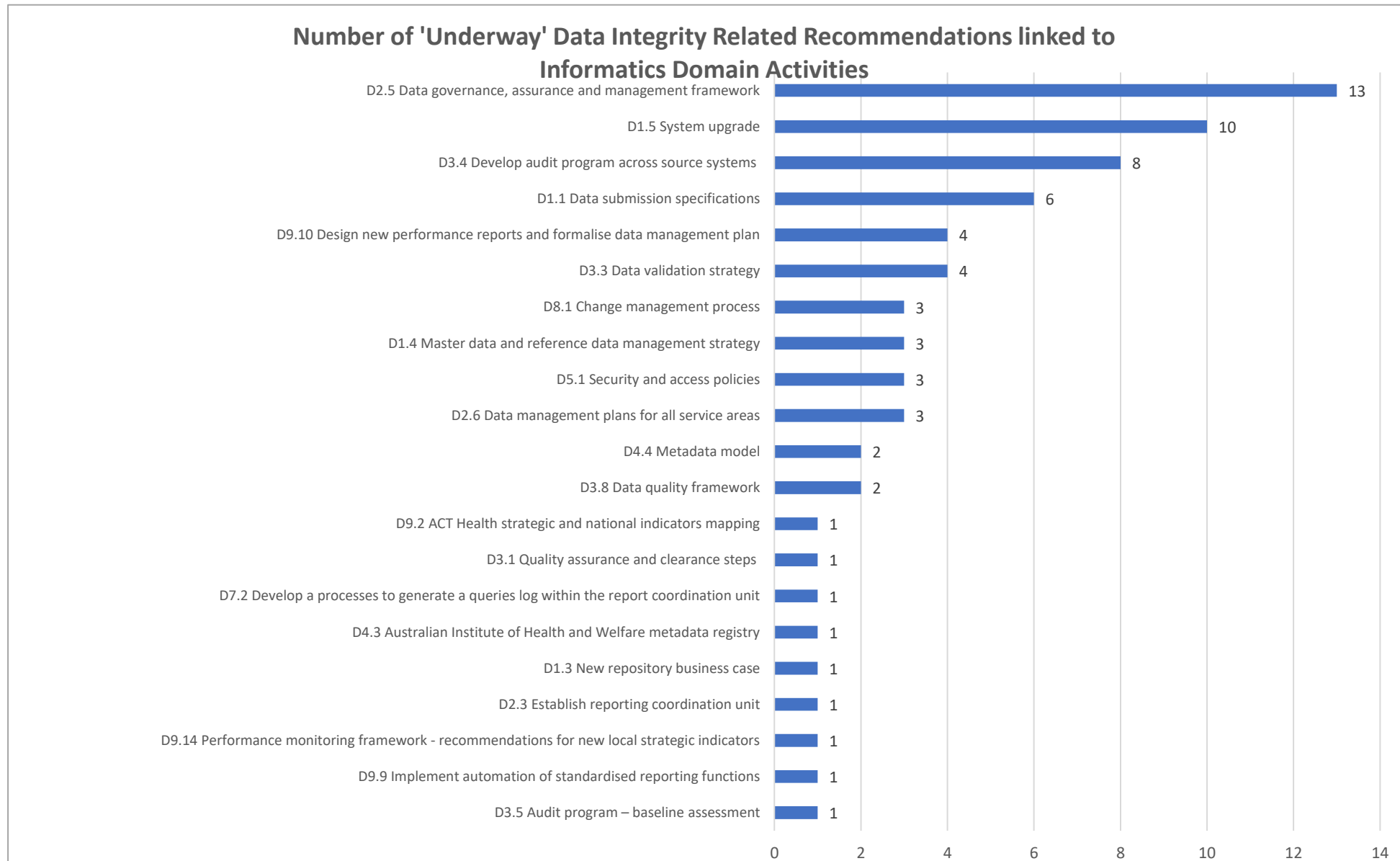


Diagram 1: Number of data integrity related recommendations assessed as ‘underway’ and linked to Informatics Domain Activities (31 March 2018)



A summary of the analysis of the progress made is shown in the table below:

Reco. status	As at Jun 17	As at Sep 17	As at Dec 17	As at Mar 18	Internal audit analysis
Completed	32	56	66	69	<ul style="list-style-type: none"> ▶ Completion rate of recommendations has progressed significantly over the 14 months of the SWR, increasing from 18% to 39% of recommendations completed.
Underway	96	89	83	70	<ul style="list-style-type: none"> ▶ Reduction of the number of recommendations with 'Underway' status was due to the progress made towards the implementation of recommendations. <ul style="list-style-type: none"> ◆ 3 recommendations with 'Underway' status as of December 2017 were completed in the last 3 months. ◆ 3 recommendations with 'Underway' status as of December 2017 were moved to 'No longer relevant' due to recent decisions and changes. ◆ 8 recommendations have moved from 'Underway' in December 2017 to 'Ongoing' ◆ 1 recommendation was moved from 'Not Started' to 'Underway'.
Ongoing	7	7	7	15	<ul style="list-style-type: none"> ▶ These recommendations do not have an expected completion date. Their implementation requires ongoing monitoring. ▶ For example, Recommendation 21 from the Michael Reid & Associates Report of December 2012 stated that <i>"An assessment of the skills and competencies of people involved in data management and dissemination should be undertaken. Targeted education and training should be provided to accommodate identified skills deficiencies."</i> The first part of this recommendation occurred, while the second part is an activity that will continue to occur on an ongoing basis.
Not started	27	7	1	0	<ul style="list-style-type: none"> ▶ All 175 recommendations have now been addressed and assessed as either completed, underway, no longer relevant or ongoing.
No longer relevant	13	16	18	21	<ul style="list-style-type: none"> ▶ Upon assessment and enquiries, it was determined that no further action is required to implement these recommendations. ▶ The recommendations are either are no longer relevant or the recommendations do not address the underlying risks (the risks are being/were addressed by alternative solutions). ▶ An additional 3 recommendations were deemed 'no longer relevant' in the March 2018 assessment as alternative activities have superseded the recommendations.

The outcomes of this audit assessment of the progress of the implementation of the 175 recommendations will be used as input into the final SWR report produced by the PRD Division. The updated spreadsheet of recommendations was provided to the DDG, PRD and the SWR team at the end of this final assessment. Graphs summarising the progress made since the June, September and December 2017 assessments are presented on the following pages.

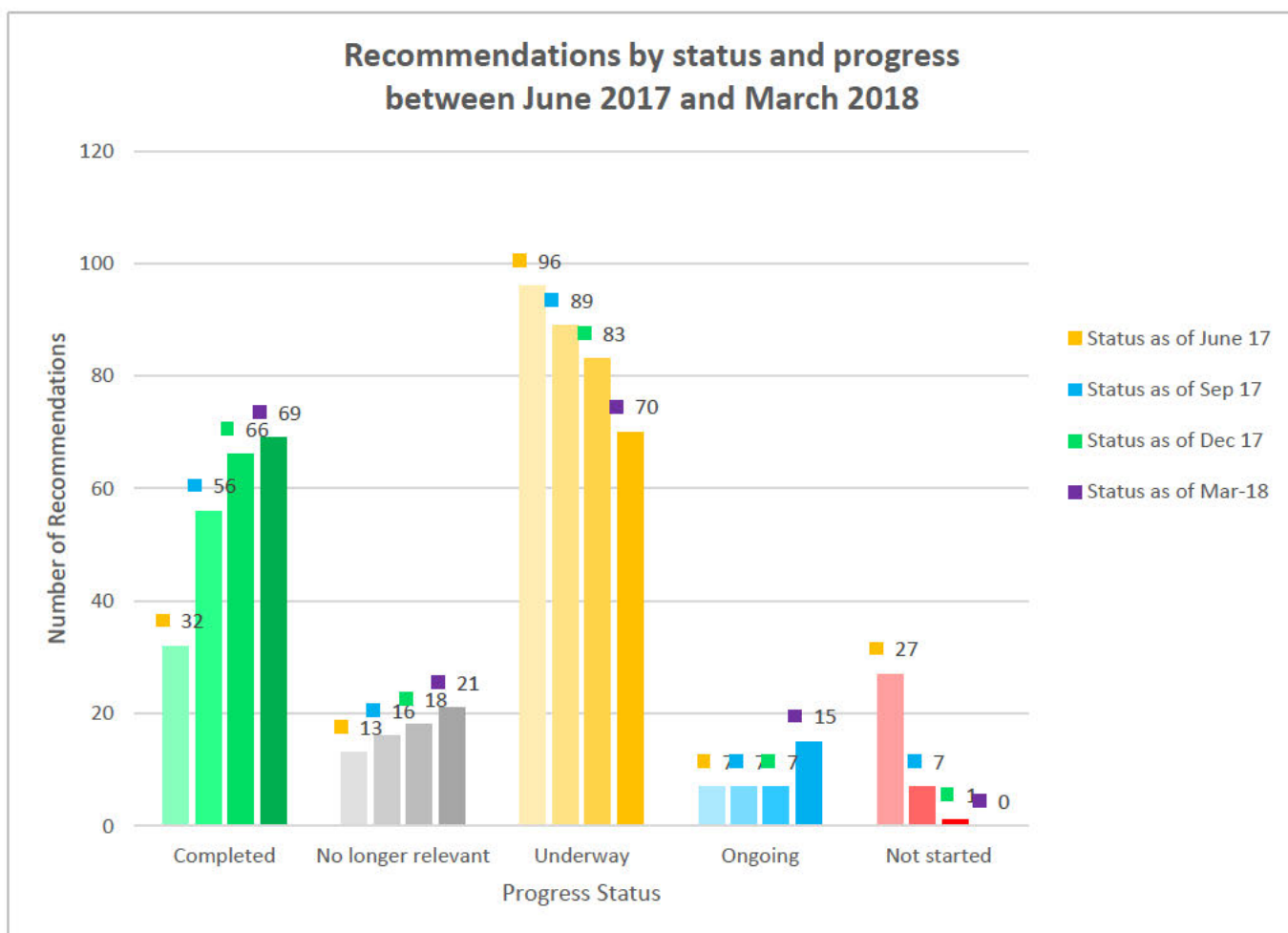


Diagram 2: Recommendations by status and progress between June 2017 and March 2018

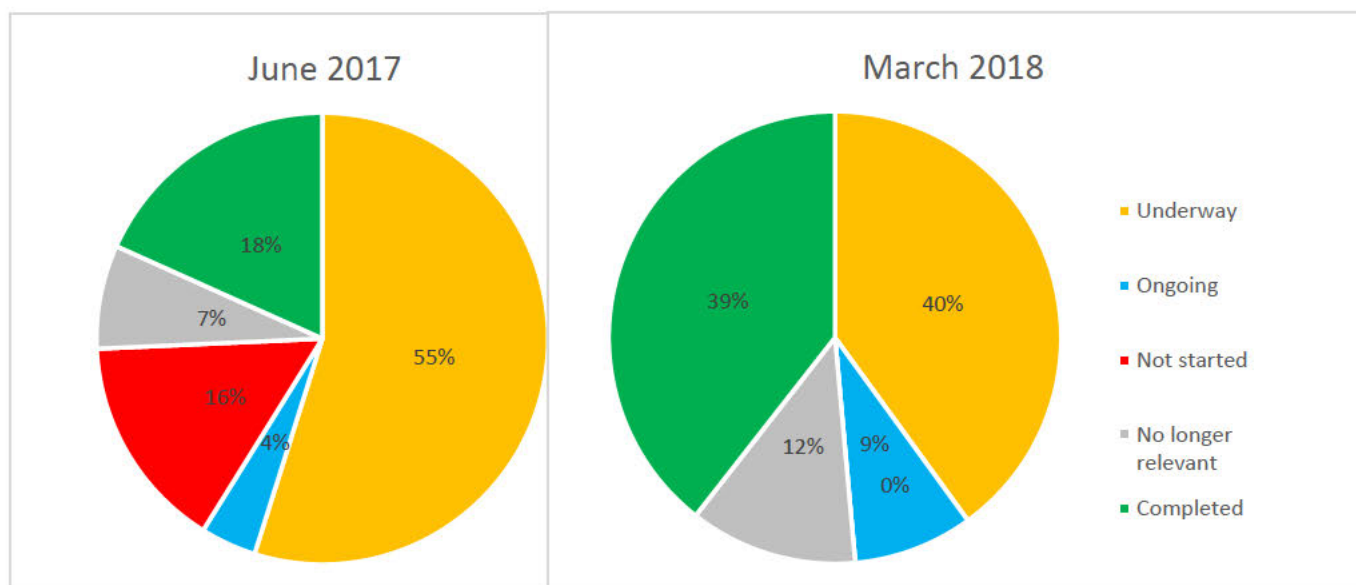


Diagram 3: Progress made on implementation of recommendations over 9 months (June 2017 to March 2018)

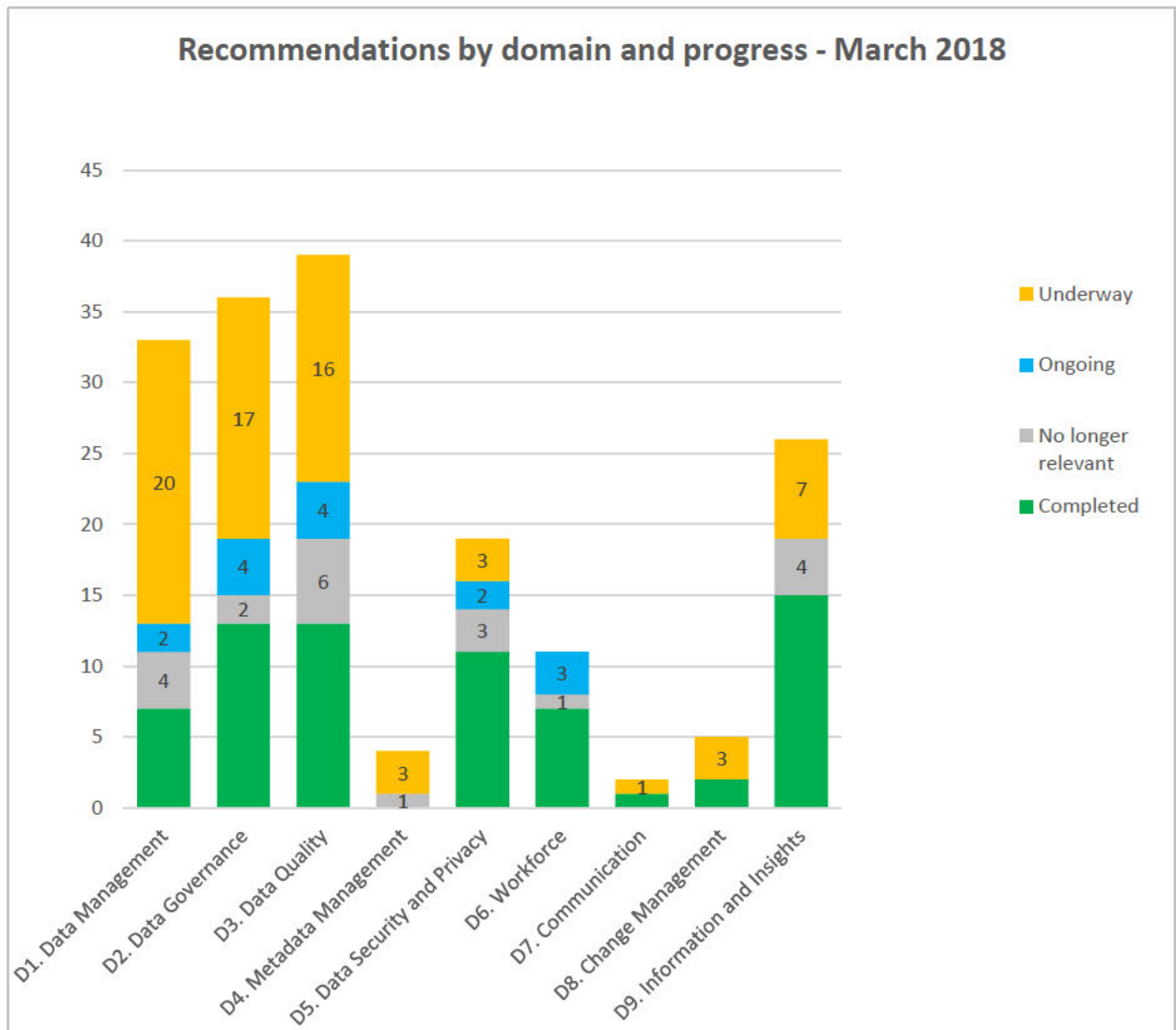


Diagram 4: Recommendations by domain and status of implementation - March 2018

5.2 Effectiveness of implementation activities for completed recommendations

The final audit assessment concludes that 69 of the 175 recommendations (over 39%) are now complete with reasonable evidence to support the effectiveness of implementation of the recommendations. These recommendations have been mapped to the relevant informatics domains with comments summarised against each in the below sections.

5.2.1 Data Management

Seven (7) recommendations have been mapped to the Data Management domain and mainly pertain to consideration and use of new technologies, system changes regarding IT access, and improved coordination of reporting processes. See table below for data management related recommendations:

Rec UID #	Report Rec #	Identifier	Recommendation	Audit comments as at 31 March 2018
54	6	SCPAR6	The Committee recommends that, consistent with the recommendation of the Auditor-General, the rapid sign-on system be implemented as soon as practicable and that the Government of the day report to the ACT Legislative Assembly at the earliest opportunity on its implementation.	Rapid Sign On has been implemented. ED was the pilot site. Most clinical areas are now using rapid sign-on - AMC, Mental Health, Alcohol/Drug with new MAGIC ER s/w are using this system.
59	41	PWCR41	Consider introducing new technologies	The development of the new d/w is considering a range of available technologies. The Directorate will continue to consider new technologies as part of ongoing improvements to systems.
90	19	PWCR19	Identify appropriate additional resource/s who will require 'run' access to support current single resource for CHARM.	CHARM automated process provides data extract monthly into a folder for input into the DW.
91	8	MR8	Operational information systems that generate data and reports: that system development plans for any business system component include a comprehensive schedule of interfaces and tabulation of the interface metadata references and particulars.	The UCPH core integration work has been mapped into the DSD EA tool. A new Change and Release Manager commenced in January 2018 and has introduced the use of the EA tool extensively. There is still active work happening in this space. ACT Health does have solution design documents for each system that does at times include information flows. Deloitte were engaged to review 254 systems and refine what is determined as govt critical. This is reducing the number of govt critical systems down to about 30-31 systems deemed to be government critical - based on a risk management approach and practical use of existing resources. DSD now have solution designs and interface specifications which allows for information flows to be understood. Whenever a change to a system occurs, they document the changes to the interface specifications. A core integration framework exists and is supported by other documents.



Rec UID #	Report Rec #	Identifier	Recommendation	Audit comments as at 31 March 2018
168	3	RR3	In undertaking this 'accreditation', the ED P&I Branch should assess the appropriateness of the continuation of the external provision of data by Divisions or whether alternative arrangements are proposed. It is expected there will be some circumstances where information, currently distributed within the Directorate and/or to the national agencies without the involvement of the P&I Branch, will need in future to be formally cleared through P&I Branch.	The Reporting Coordination Unit (RCU) is now in place. It has assessed all reports being provided and ranked them in terms of 'Essential & priority - External' and 'Essential - internal'. A Data Requests Register has been established and is maintained in accordance with a new policy and procedures around data change requests. Some other areas of the Directorate, including Population Health, send their reports to the DDG PRD Division for clearance. Wherever deemed appropriate, all reports that are released externally are cleared through this position.
169	4	RR4	Once the data sets are on the register, accredited and the arrangements are deemed appropriate, the data should continue to be provided by the relevant Division.	This is now part of the data requests sign-off process and the Master Reports Register established by the RCU. Reporting still happens from the Divisions, but where appropriate the reports are cleared through the DDG PRD.
172	14	RR14	Innovative tools to enable a more cost-effective data capture be identified and evaluated by the ICT Management Committee.	As part of the new data warehouse options, the Directorate have been investigating innovative technologies for data capture and analysis.

5.2.2 Data Governance

Thirteen (13) recommendations have been mapped to the Data Governance domain, see table below for details:

Rec UID #	Report Rec #	Identifier	Recommendation	Audit comments as at 31 March 2018
8	7	RR7	Information management issues should be a regular agenda item for discussions by the ICT Management Committee. The terms of reference and membership of this committee will need to be reviewed in light of this broadened scope.	ICT&IM Executive Committee (ExCo) still exists, and issues are being discussed in relation to IM. New Governance Model was tabled at ExCo and agreed.
17	16	PWCR16	Undertake full review of BPIDS response to Auditor-General Recommendations.	The full review of BPIDS response to the Auditor-General Recommendations has occurred (as part of the SWR and this Internal Audit).
19	12	SCPAR12	The Committee recommends that the Government of the day detail to the ACT Legislative Assembly, at the earliest possible opportunity, what action the Health Directorate has taken to assess whether a prevailing organisational culture at the Canberra Hospital contributed to the	An internal RCA occurred in late 2017. A secondary RCA was conducted in Feb/March 2018. The Annual Report of 2012-13 assessed this recommendation as complete. The response in the Annual Report was "A response is provided in the government's submission to the assembly. The



Rec UID #	Report Rec #	Identifier	Recommendation	Audit comments as at 31 March 2018
			circumstances surrounding the alteration and misreporting of performance information.	<i>response noted the work undertaken to assess organisational culture and systems in place to address issues raised from that assessment."</i>
21	11	SCPAR11	The Committee recommends that clear guidelines be established concerning external communication regarding matters concerning the ACT Health Directorate, the Canberra Hospital and Calvary Public Hospital.	The Annual Report of 2012-13 assessed this recommendation as complete. <i>"Clear guidelines and agency representation exist for all major national committees and organisations. Responsibilities are clearly articulated to relevant executives"</i> .
22	2	AG12R2	The Health Directorate and Calvary Public Hospital should develop essential EDIS governance documentation, including: a) an overarching governance statement that describes: i. the purpose and use of the system; ii. its business owner, system administrator and all roles and responsibilities associated with the system and its support (including third party stakeholders such as Shared Services ICT); iii. the security classification of the system and its data; iv. applicable policy and administrative guidance; v. record-keeping obligations; vi. training requirements; and vii. what is monitored and audited to ensure compliance with policy and supporting system documentation. b) standard operating procedures for all roles and responsibilities associated with the system and its use; c) training material that covers all dimensions of EDIS including user roles and responsibilities, processes described in standard operating procedures and specific policy that is applicable to the system; and d) a System Security Plan, which is informed by a risk assessment and risk management plan.	EDIS has a System Security Plan (SSP). All systems have SSPs. EDIS System Administration will change - under review by CIO, he is trying to pull all SA's into one area. DSD have to review the eLearning packages for EDIS, its not about how to use EDIS, rather what data fields are needed. This is now an ongoing activity for regular reviews.
25	7	AG12R7	The Health Directorate should develop policy and administrative guidance for EDIS data validation activities for the two Canberra hospitals. The policy and administrative guidance should identify and document: a) agreed Emergency Department actions which constitute 'clock starting' and 'clock stopping' moments for the purpose of EDIS timeliness records; and b) protocols for	Policies are in place for parts a) and b) of this recommendation. Policies are available on the ACT Health Policy Register. <ul style="list-style-type: none"> • Emergency Department Information System (EDIS) Compromised Data Integrity Escalation Procedure • Emergency Department Information system (EDIS) Data Validation • Emergency Department Information system (EDIS) • Time to Treatment in the Emergency Department Policy



Rec UID #	Report Rec #	Identifier	Recommendation	Audit comments as at 31 March 2018
			data validation activities in the day(s) following a patient's presentation to the Emergency Department.	
31	1	MPR1	Registers be established and maintained of reports issued and data holdings maintained and that these registers be developed as the key control mechanism for the report release authorization and recording process.	A register of requests and calendar of reports are maintained. If it is a subscription report, the distribution list becomes part of the clearance package.
33	1	MR1	A record of reports issued and data sources: that a register of statistical and management reports (Register of Reporting – RoR) be prepared and maintained by P&I Branch from monthly returns from each of the areas using and analysing data.	Report Coordination Unit has been established and maintains a register of data requests and data outputs (reports). The work that was done as part of Milestone One (Essential Reports etc.) was the foundation of this work. Performance and programs management hub/unit has a master report tracker that can pull off statistics and it is used on a daily basis.
42	1	RR1	A register of all Directorate external data provision should be developed and maintained.	The RCU is maintaining a register (Master Report Tracker) of all external and internal data provision. The RCU has not yet been launched across the Directorate.
85	9	AG12R9	The Director-General of the Health Directorate and the ACTPS Head of Service note the findings of this report with respect to the executive who has admitted to manipulating hospital records, and consider whether this executive has engaged in misconduct in breach of section 9 of the Public Sector Management Act 1994 and their executive contract.	The Executive Officer was dismissed.
87	13	SCPAR13	The Committee recommends that, given the Health Directorate's failure to protect the privacy of the Executive who admitted to altering data—prior to any civil, criminal or administrative proceedings—the Health Directorate should: (i) issue a public apology to the individual concerned; and (ii) take appropriate steps to acknowledge the individual's contributions to the operation and administration of the Canberra Hospital.	Based on the Government Response to the SCPA Report No. 29, this recommendation was completed.
151	9	SCPAR9	The Committee recommends that the Government of the day detail to the ACT Legislative Assembly, at the earliest possible opportunity, how it will address and improve issues about achievements against throughput and triage targets as they relate to the Emergency Department at the Canberra Hospital.	These targets fall under the existing indicators that are relevant for the day. These get updated yearly.

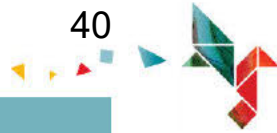


Rec UID #	Report Rec #	Identifier	Recommendation	Audit comments as at 31 March 2018
170	16	SCPAR16	The Committee recommends that the 8th ACT Legislative Assembly Standing Committee on Public Accounts should give due consideration to conducting an inquiry into the process of future delivery of health care services across the Canberra Hospital and Calvary Public Hospital.	Closed as per Government response to recommendations, refer ACT Health Annual Report 2012-13, page 203.

5.2.3 Data Quality

Thirteen (13) recommendations have been mapped to the Data Quality domain, see table below for details:

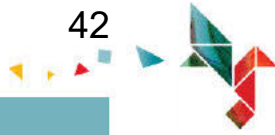
Rec UID #	Report Rec #	Identifier	Recommendation	Audit comments as at 31 March 2018
26	8	AG12R8	The Health Directorate should implement additional review and assurance controls over the preparation and reporting of Emergency Department timeliness performance information. These review and assurance controls should address both Canberra Hospital and Calvary Public Hospital performance information. The Health Directorate should consider whether the additional review and assurance controls should be applied to other performance information.	<p>Policies for such assurance and controls are in place. Policies are available on the ACT Health Policy Register.</p> <ul style="list-style-type: none"> • Emergency Department Information System (EDIS) Compromised Data Integrity Escalation Procedure • Emergency Department Information system (EDIS) Data Validation • Emergency Department Information system (EDIS) • Time to Treatment in the Emergency Department Policy
27	5	AG15R5	<p>Patient Record Close Period:</p> <p>a) Calvary Public Hospital should align its EDIS record close period (i.e. the period after which records are locked) with that of Canberra Hospital.</p> <p>b) The Health Directorate should undertake a monthly assessment to monitor changes to patient records after the close period.</p>	A process was established to lock down the patient record close period whereby the EDIS vendor now needs to be contacted to unlock the record and make any changes. As changes now cannot be performed by Directorate staff, the need for monitoring monthly is not required. In effect, this recommendation has been completed.
30	18	AG15R18	<p>Clinical Coding: Canberra Hospital and Calvary Public Hospital should improve their clinical coding with the following process changes.</p> <p>a. Where coding is completed before the availability of the discharge summary, the medical record should be flagged, to facilitate subsequent identification of potentially incorrectly coded episodes.</p>	For TCH: A report has been developed from PAS that provides information about which records were processed before the discharge. When coding for the month has been completed it will show incomplete records, they track when they receive the notes, when the discharge summary was met. A doco query process exists, where they keep a spreadsheet of the query and the response and review the coding. The PAS report (Discharges coded without Discharge Summaries) is done monthly and allocated by the Clinical Coding



Rec UID #	Report Rec #	Identifier	Recommendation	Audit comments as at 31 March 2018
			<p>b. Where the discharge summary directly conflicts with information in the record, a query should be forwarded to the treating clinician for clarification. These queries should be followed-up and documented for future reference.</p>	<p>Manager to the coders. The process that the clinical coders follow was also in place and sighted. A scan of the discharge summary (attached to the patient medical record) is also referred to, to check coding.</p> <p>For Calvary: They responded with a letter to ACT Health Directorate 4/12/15 to Head of BPIDS (Phil Ghiaradello). Louise provided me with a copy of this letter which sets out the response to the AG report. Toni has done further work since. A process for coding for part a there is a manual workaround in process. Further work on another report / changed report for electronic tracking is underway. All things implemented, a report from ACTPAS (modified for Calvary). to show coded without discharge summary. They have also put in place SOPs for the coders. The new process and report is working well. They have noticed good coding, their days to code is reducing over time. They only really need to code less than 1% of records to fix up. Coding query forms are also used, similar to TCH.</p>
86	10	AG12R10	<p>The Health Directorate reinforce to Health Directorate employees, especially executive staff, the need to act with integrity with respect to the maintenance of health records and associated data.</p>	<p>This has occurred - evidence was sighted of one such 'all staff' communique.</p>
107	44	MR44	<p>Data falsification risk management: that coding standards are to be applied and that professional ethics are reinforced relating to correct and even-handed application of coding standards and reports metadata definitions.</p>	<p>PRD reports analysts run validation reports. When coding audits are conducted it is the Calvary and Canberra Hospital clinical coding staff that check the codes. TCH - documentation queries are still being done. They do 30 record random sample of each of the coders using ResiCat (tool) to select the sample, with relevant exclusions. They have auditors/educators that they used to check the coding. If errors are identified then training or doco will be remediated or training will occur. Recent new coding standards came in July, so this will form part of some targeted audits. TCH does internal audits and the external audits are done by independents. There are a number of validation checks and edit checks on the data, cross field validation checks, based on the Aust Coding Standards, they have a tool (PICQ - Performance Indicators of Coding Quality) to ensure the data being coded is in accordance with these standards. They do reinforce the professional ethics to the coders and the clinicians in documentation queries. Calvary - Coding standards are applied, the staff are trained and checked to make sure they follow them. The coding audits are done internally - targeted audits are done as well as</p>



Rec UID #	Report Rec #	Identifier	Recommendation	Audit comments as at 31 March 2018
				random sample audits. They audit 30 in their sample set. They have a program schedule in place and a calendar.
129	10	RR10	P&I Branch should review its external liaison arrangements with Divisions to improve engagement with EDs/Clinical Directors on enhancing data quality. As one practical suggestion, the Branch should be present at monthly Divisional meetings to discuss scorecard data. Similarly, the ED of the Branch should be present at that part of the Executive Council meeting which discusses the Directorate scorecard.	ED, PRD attends monthly Divisional meetings (Executive Directors meeting). CIO also sits on Exec Council meeting with DDG each week and discusses the scorecard.
148	15	PWCR15	Provide QA oversight of the Quarterly Performance Report Q4 process.	Advised to AG Dec 2016 per COR16/16228.
149	27	PWCR27	Apply validation controls to subscription reports that enables checking of content prior to distribution for completeness and accuracy.	Validation controls are applied across the underlying data for ED data. The process runs every night with validation checks across the datasets. The PIP Portal is accessible by Calvary staff as it was installed at Calvary 2 1/2 - 3 yrs ago. A check on the the system was that key staff have view only access (which is appropriate). The data that the reports rely upon is being validated (MORBID datasets). The validation checks are running across the datasets. This was sighted via the PIP Portal.
154	15a	AG15R15a	Risk Based Approach to Investigations: The Health Directorate should undertake further investigation into the inconsistencies and anomalies identified by the data analytics, taking a risk-based approach to the investigation and focussing on the areas that have the potential to materially affect ABF data and funding.	The Health directorate now takes a risk-based approach to investigating data errors that impact ABF-funding as articulated in the recommendation. The most work is put into Admitted services (which on a per-episode basis receives the most funding), then ED, then Non-admitted services. IHPA weight the validations so the fatal errors can be rectified ahead of the non-fatal data errors.
156	13	AG15R13	Analytical Review of Reporting: The Health Directorate should perform an analytical review to quality assure the six-monthly ABF data submission before it is sent to IHPA.	Evidence of this review was sighted.
157	16	AG15R16	Length of Stay, Overlapping Admissions and Type of Visit a. Canberra Hospital and Calvary Public Hospital should review patient records on a random and weekly basis with a focus on the fields that are included in ABF reporting. b. Canberra Hospital and Calvary Public Hospital should conduct refresher training for Emergency Department clerical staff on how to appropriately classify the 'type of	This is occurring at both hospitals and evidence was sighted. As a follow on to this, the PRD team are planning to design/develop a rolling program of randomly sampled audits across key systems to check that records have been recorded accurately and completely.



Rec UID #	Report Rec #	Identifier	Recommendation	Audit comments as at 31 March 2018
			visit' for patients presenting to the Emergency Department.	
166	7	SCPAR7	The Committee recommends that all ACT Government directorates and agencies should have effective practices and processes in place to review all reports of the Auditor-General, and to assess the relevance of the findings and recommendations to their agency, regardless of whether the agency was involved in a specific audit.	The performance audit reports, based on relevance, are discussed at the Audit and Risk Management Committee meeting.
173	15	RR15	The workload of clinical coders' assessed and appropriate adjustments made to ensure the targets proposed for coding timelines are achieved.	The workload of the clinical coders has been assessed. Contract coders have been utilised which has allowed KPIs to be met. There is work in the branch to develop a longer-term strategy to continue to address this issue. TCH is working on a Coding Strategy for both Calvary and TCH, there is push for a single coding service strategy. This includes skills, resourcing etc. Also with the Enterprise Agreement, a better pay structure for clinical coders has been put forward. For Calvary - working off 100% in 30 days and they are meeting these standards. Within 14 days of discharge. Coders need to be liaising with clinicians and they need to be on the ground. They do lots of education with clinicians and need to build relationships.

5.2.4 Data Security and Privacy

Eleven (11) recommendations have been mapped to the Data Security and Privacy domain, see table below for details:

Rec UID #	Report Rec #	Identifier	Recommendation	Audit comments as at 31 March 2018
23	4	AG12R4	The Health Directorate and Calvary Public Hospital should: a) review the current distribution of access to EDIS throughout the hospital and remove any users who do not have a specific and documented requirement for access to the system; and b) develop policies, administrative procedures and system controls (if possible) that restrict the use of generic user	This is tightly controlled. All generic user accounts have been removed.



Rec UID #	Report Rec #	Identifier	Recommendation	Audit comments as at 31 March 2018
			accounts outside the Emergency Department work environment.	
24	5	AG12R5	The Health Directorate and Calvary Public Hospital should: a) identify and document responsibilities for user access management and log monitoring for EDIS; and b) develop a process to monitor user activity within EDIS and how to report and escalate unusual activity to the appropriate authorities.	Limited audit ability in the current version of EDIS. They can monitor user login activity, but they cannot monitor when someone has changed data. There is a certain level of monitoring that can occur, they do check some changes on a weekly basis (they can monitor if something has changed, but not exactly what changed). Project to upgrade EDIS to 16.2 has commenced. User access management is governed by policy - existing and on the ACT Health portal. There are policies in place for who can change the data. The Compromise Data Integrity Escalation Procedure has also been developed and is published in the policy register on the ACT Health portal.
63	15	MR15	Principles and conditions of data access: that general rules and specific rules for particular data holdings be: a. readily available to users and b. linked to the system access points c. acknowledged by users at the point of use as part of the access procedure. (In the same way as conditions of issue of airline tickets – or acknowledgement of license conditions before loading software.)	This is part of the initial login procedure, also as part of code of conduct etc.
66	31	MR31	Data systems security management: that system access profiles be developed for each staff category and clinical role where use of records systems is required. That system logons be refined to facilitate access for authorised personnel and restrict access to unauthorized personnel.	DSD have been progressing role based access for most systems and managing access to these systems through the new IAM solution. Not all systems are using IAM due to legacy system issues. But all new systems will use IAM and role based profiles. There are over 400 systems and not all of these will be technically capable to use the IAM solution. To get access to a system, the manager needs to approve that access. DSD still use IAM for access to most systems, but not all are automated. DSD is also doing regular 6-monthly reviews of staff that have left the Directorate - staff clearance form - sent to HR then SSICT for removal from system. In EDIS and ACTPAS there are profiles for different clinical areas and administrators, there are roles and groups in the new IAM. This is an ongoing activity DSD is working through the digital health strategy with a view to removing legacy systems. In effect, this recommendation has been completed as the IAM has been implemented.



Rec UID #	Report Rec #	Identifier	Recommendation	Audit comments as at 31 March 2018
67	32	MR32	Data system security management: that a register of [people] authorised to access data holdings in the systems be established for each operational system and level of access for each authorised person be specified – role, data entry – data correction –and data deletion.	Data audit trail - SSPs have these. Some of this has been actioned esp. around generic logons. Further to this, the development of the data warehouse, as part of the SWR, people who are authorised to access the data holdings will be identified. IAM system now controls access to most of the data holdings / systems. This constantly logs data access and reports on that access for remediation if access is not valid. The data warehouse data access is something that will occur once the requirements and design of the data warehouse have been developed.
69	35	MR35	Data system security management: that for data entry and system management staff similar logon authorization management and data access logs be maintained as for other system users be maintained.	Data audit trail - SSPs have these. Some of this has been actioned esp. around generic logons. DSD have implemented access audit processes for our government critical systems. Each system has different capabilities but there are documented processes for auditing access logs for these systems and the intention was to perform these random audits 1-2 times per year. Where concerning behaviour in relation to access to systems occurs, audits are able to be run by the system administrators of those systems. In effect, this recommendation has been completed as the IAM has been implemented. For all data entry and SA staff have the same process to get access to systems through the IAM solution. Data access management processes have been implemented for all govt critical systems.
70	3	SCPAR3	The Committee recommends that the Government of the day review the security of information which identifies individual patients at the Canberra Hospital and report on the outcomes of this review to the ACT Legislative Assembly on the first sitting day of 2013.	System Security Plans have been developed for all ACT Health systems. These include information (and security requirements of that information) stored in the system. SSPs are being reviewed and the template updated. ACPTPAS SSP does contain information classification. In addition, an 'audit' by system administrators of targeted IT systems was conducted in Sept 16 (including EDIS and ACTPAS) with a range of users removed with no need for access. Ongoing work to review this access occurs.
71	8	SCPAR8	The Committee recommends that all ACT Government directorates and agencies should prioritise as a matter of urgency an assessment of the adequacy of controls over their respective IT systems and applications. This should include consideration of the controls that affect the reliability of all IT systems and applications (general controls) and controls that are specific to each application (application controls).	Based on the Government Response to the SCPA Report No. 29, this recommendation was completed. On 4/7/12, the Chief Minister wrote to all Ministerial colleagues, and subsequently, the DG of ACT Health write to all ACT Govt Directorates to draw their attention to this issue.
73	17	MR17	Principles and conditions of data access: that a program of review of data access arrangements be developed so	Systems administrators do regular reviews and if not accessed the account is disabled. IAM system is reviewed regularly. Just starting to link to HR data.

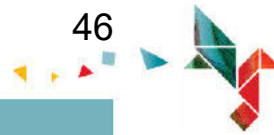


Rec UID #	Report Rec #	Identifier	Recommendation	Audit comments as at 31 March 2018
			that each data holding is covered at least once each year or according to risk rating.	The data warehouse - data access is something that will occur once the requirements and design of the data warehouse have been developed.
74	11	PWCR11	Review and update access controls to Shared Network Drive for PI (Report Template) and DSS (Report Proof).	This is managed through PRD management approving access to these drives through the IAM system. RACI chart exists, but this specific recommendation is part of the IAM system.
80	40	MR40	Data access management: that access registers be analysed on a regular basis to identify systematic patterns of access to data records for change or update.	Every system has different capabilities to determine what data elements will be changed. As part of the system administration activities for the systems that can pull medical records out, there are audit logs that are reviewed 1-2 times each year. Evidence of this was sighted (an audit done in September 2016) allowed for users to be removed from the systems who no longer had a need to access them.

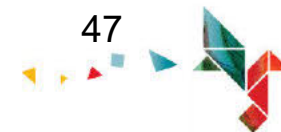
5.2.5 Workforce

Seven (7) recommendations have been mapped to the Workforce domain, see table below for details:

Rec UID #	Report Rec #	Identifier	Recommendation	Audit comments as at 31 March 2018
28	6	AG15R6	Training Materials: Canberra Hospital should finalise its draft EDIS training documents and implement a mandatory requirement for staff to complete EDIS training before receiving access to the system.	System Administrators control all the access. They do the training on the spot as well as having the eLearning package. Training is available as an eLearning course, face to face if eLearning is not suitable and via group sessions for staff rotations. As evidence, reports were obtained from the Capability team on who has completed the eLearning modules for EDIS; this is an ongoing activity. EDIS System Admins conduct 'at the desk training' for new staff who require access to EDIS, before they are granted access.
83	37	MR37	Training in values and best practice in data security: that data entry and data review staff are provided on a regular basis with feedback for their checking and confirmation on: <ol style="list-style-type: none"> Patterns of data access with reasons. Results of data validation and QA on the data that they have entered or accessed for further action. [The purposes for this include ensuring that all staff can be held responsible for their own logons and that possible false logons are identified quickly.]	There is an eLearning package that all new staff need to do that talks about data security. Clinical records do a check on all access on a monthly basis, they check what people have been looking at and if it does not relate to what people are doing. The outcome of the new data warehouse and new technologies will also assist in terms of using data analytics tools for these purposes. EDIS System Administrators do their own management of access. All system e-learning packages have content that includes data security and privacy. The new IAM system, together with IMPRIVATA and Rapid Single Sign on all contribute to controlling access to data in the systems.



Rec UID #	Report Rec #	Identifier	Recommendation	Audit comments as at 31 March 2018
84	38	MR38	Training in values and best practice in data security: that staff with discrepant levels of validation or edit queries be provided with further training or guidance.	Training in all systems now occurs through the e-learning packages.
119	4	SCPAR4	The Committee recommends that the Health Directorate in conjunction with Shared Services ICT ensure that appropriate training on every IT related hospital system, with a particular focus on the Emergency Department Information System (EDIS), is provided to all staff at the Canberra Hospital and Calvary Public Hospital.	DSD has been moving to role based e-Learning training packages for all IT solutions underpinned with support from the Digital Solutions System Support Help Desk. IAM and the Elearning modules process addresses this recommendation.
121	22	MR22	Training and support in use and interpretation of data: that a user-friendly on-line library of training materials for data system users be developed or linked to the systems access register.	Elearning modules have been developed for all systems that hold medical records (ACTPAS, Clinical Portal, Electronic Medication Mgt, Alerts System etc). DSD are consulting with the business units to understand the data in the systems. Staff cannot access the system unless they complete the Elearning training.
123	20	MR20	Training and support in use and interpretation of data: that an index of training material be prepared – ideally web-based and linked to training material for online learning and reference.	DSD will be working with the PRD Division to incorporate proper use and interpretation of data in the ACT Health systems training during 17-18. All training is in the online Capability System (Learning Management System) which lists all Elearning and booking face-face training.
124	21	MR21	Training and support in use and interpretation of data: that a training protocol be developed for each information system component and a register of expert users.	DSD have been working on the transition from project to support – this includes information on training to support desk as well as registers of super users. This will be part of the Transition to Support processes documented by the DSD ICT PMO. For each new system, a training plan is developed and determines what model of training is required. DSD has developed templates for transitioning to support and pass on to Support Desk.



5.2.6 Communication

One (1) recommendation has been mapped to the Communication domain, see table below for details:

Rec UID #	Report Rec #	Identifier	Recommendation	Audit comments as at 31 March 2018
61	24	MR24	<p>Help desks: that within CIOs Branch, a help desk be set up for ICT systems operation queries – locii of responsibility and SME should be differentiated and clarified. In particular the functions of the SSICT help desk should be reviewed in relation to the IM help desk to ensure there are no gaps. The core functions of the system help desk should include.</p> <ul style="list-style-type: none"> a. system components operation <ul style="list-style-type: none"> i. system performance review ii. system development and integration iii. system provider management – including shared services b. system access registration and c. system login tracking security monitoring and d. system access audits. 	<p>A DSD Systems Support number that is specific to support the multiple Health applications is now in place. All of the core functions listed in this recommendation will be provided as part of that Service Desk number. Stickers have been given to all Health assets to communicate the number to call. They receive level 1 support for Health systems. The functions of the help desk come under the responsibilities of the CIOs Branch.</p>

5.2.7 Change Management

Two (2) recommendations have been mapped to the Change Management domain, see table below for details:

Rec UID #	Report Rec #	Identifier	Recommendation	Audit comments as at 31 March 2018
18	1	AG15R1	<p>Change Management: As the Health Directorate implements its Information Management Strategy 2015-2016, change management activities should include:</p> <ul style="list-style-type: none"> a) training Health Directorate and hospital staff to ensure they have an adequate understanding of the Strategy and specifically data integrity activities; and b) documenting and allocating responsibility for data integrity activities for the key systems, including ACTPAS, EDIS and the Health Directorate data warehouse. 	<p>Part a) of the recommendation references a Strategy and the PRD Branch now has a new <i>ACT Health Performance Reporting and Data Strategy</i>. Some data integrity activities are being undertaken. Training plans concentrate on the learning outcomes. DSD System Support team does the training. The tools that allow audit and data entry restrictions is managed by System Administrators. PRD has developed an internal orientation guide. DSD component is training in the new systems. Collaboration between DSD and PRD is occurring about the strategy and policies etc.</p>

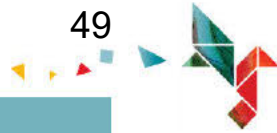


Rec UID #	Report Rec #	Identifier	Recommendation	Audit comments as at 31 March 2018
20	10	SCPAR10	The Committee recommends that clear guidelines be established concerning internal communication between the ACT Health Directorate, the Canberra Hospital and Calvary Public Hospital.	The Annual Report of 2012-13 assessed this recommendation as complete. The response to this recommendation was made in the 2012-13 Annual Report "A response is provided in the government's submission to the assembly. The response noted the work undertaken to assess organisational culture and systems in place to address issues raised from that assessment."

5.2.8 Information and Insights

Fifteen (15) recommendations have been mapped to the Information and Insights domain, see table below for details:

Rec UID #	Report Rec #	Identifier	Recommendation	Audit comments as at 31 March 2018
29	14	AG15R14	Reporting of ABF Costing Data: The Health Directorate should develop and publish a costing framework which: <ul style="list-style-type: none"> a) allocates roles and responsibilities between the Health Directorate and hospitals; b) specifies a firm schedule for hospitals to submit costings; c) incorporates a costing data specification; d) outlines a costing review and validation process; and e) includes an urgent issue escalation process. 	In 2015, an ACT Health - Patient Level Costing Framework document was developed and has been in circulation and both hospitals have approved it. It is updated annually, though it has not been updated since 2015. The costing data in the document has been endorsed by the hospitals before it is loaded into the software. This document was evidenced.
95	4	MR4	A record of reports issued and data sources: that each six months, a regular stock of data holdings take be conducted by web portal with data analysts/data managers. By area of data system operation/function and also a sample of key data users/dataset holders who create reports and secondary datasets. The surveys would ask four sets of questions outlined in the box below. SIX-MONTHLY UPDATES FOR REGISTER OF DATA REPORTS AND DATA HOLDINGS <ul style="list-style-type: none"> · What reports and data release provision are you responsible for? To whom? For what purpose? · Who/what is the official point/authority for release of the reports/datasets? Date of releases in past six months – Date of next scheduled/expected release. 	The RCU has a record of all reports issued. The development of the new d/w will link reports to data sources. RCU can do 6-monthly updates, but the stock take of data holdings and datasets falls into the new data warehouse team's responsibilities and will fall part of the new governance arrangements (metadata, lineage) for the data warehouse. In essence, this recommendation has been addressed by the introduction of the RCU which keeps a register of the reports, the data release provisions, data sources etc. The design and development of the new data warehouse will complement this recommendation.



Rec UID #	Report Rec #	Identifier	Recommendation	Audit comments as at 31 March 2018
			<ul style="list-style-type: none"> · What are the data sources for the reports/data releases? Source records? Compiled datasets? Working datasets? – Date of releases in past six months – Date of next scheduled/expected release. · What data holdings do you maintain? How are they stored? Who has access? Under what conditions? What records are there of data release? What is the audit trail from final reports to source records for the data used? – <ul style="list-style-type: none"> a. Standards and protocols? – b. Compliance assurance/audits? – c. Date of next scheduled audit or review? <p>To minimize repetition, the survey forms can be prepopulated with answers from the previous returns and only require confirmation updating that ideally would be done dynamically as reports and datasets are authorised for release. The survey that would then function as a follow up check and periodic stock take mechanism.</p> <ul style="list-style-type: none"> a. Reporting obligation under which report was prepared b. Purpose of the report c. Key users of the report d. Data sources and working datasets from which report compiled. 	
97	3	MR3	<p>A record of reports issued and data sources: that for each of the reports issued, archive copies of the report be stored in PDF or similar protected document form in an archive repository with folders numbered in a logical order based on the Register of Reports’ indexing arrangement.</p>	<p>RCU - this may be superseded by a new d/w, depending on the requirements agreed. The reports are filed as hard copies and held in the team work area and also stored as PDF versions in the Q: network drive. Once the reports have been pdf'd, the hard copies are destroyed.</p>
98	5	MR5	<p>A record of reports issued and data sources: that data holdings required for replication of key registered reports be indexed and archived in retrievable data storage arrangements as at the date used.</p>	<p>RCU has instigated a process for doing this. In addition, once the new data warehouse capability is in place, the ability to replicate reports will be inherent in the solution.</p>



Rec UID #	Report Rec #	Identifier	Recommendation	Audit comments as at 31 March 2018
99	52	MR52	Identification of report authorship and underpinning data status: that reports for Minister, Assembly or Public release have a registration point that documents source data and clearance point and data and version of databases used in their production.	The new QA Sign-Off Sheet identifies report authorship, the data source, clearance points. However, the database version is not included as this will be managed as part of the implementation of an agreed new d/w. In essence, this recommendation has been completed as the new RCU keep track of all reports, their source data, version and the clearance point is now the new DDG PRD. Automation of this will occur in the new data warehouse, when implemented.
100	53	MR53	Identification of report authorship and underpinning data status: that information analysis reports should have footnote reports metadata that allows identification of source data and reference data and definitions used that match what would be recorded in the register for more formal analysis reports.	Metadata dictionary linked in to the Reporting register should address most of this. The Register of Reports includes a data request number, a file is added to the n/w drive, then the location (path) to the project file is included as a footnote in the report. The RCU manages this process. A standard footnote is used.
111	4	PWCR4	Review and make determination on the inclusion of 'publications' (such as the Report) to be subjected to the formal 'Ministerial Process' for publishing on the Government website.	Advised to AG Dec 2016 per COR16/16228. The Annual report is subject to the standard Ministerial Process.
117	39	PWCR39	Operational reporting requirements are outstanding and will require consideration once available.	Operational reporting requirements are being considered now with all areas of the Directorate, this will inform what reports are required. Currently have an RFQ to look at performance metrics for performance reporting. Finalising selection by end of April 2018. This will inform new operational scorecard reports by identifying 'good to have' and 'must have' metrics.
118	15	SCPAR15	The Committee recommends that the Government of the day should inform the ACT Legislative Assembly, at the earliest possible opportunity, if the emergency access targets under the National Partnership Agreement on Improving Public Hospital Services, will not be reached by the Canberra Hospital for the 2012 calendar year.	Based on the ACT Health's response to the SCPA report, this recommendation has been actioned.
126	47	MR47	Data falsification risk management: that data and analytical staff be encouraged to quickly and collaboratively report early indications of variations from normal trends to business areas both for the purpose of checking data integrity and also for early management	Clinical coding staff identify and report variations and trends and check data integrity. Variation from data standards is reported, but the updated version of the data standards was delayed which made this difficult. For TCH and Calvary: refer to previous comments on recommendation MR45. Further awareness and training has occurred in relation to this. A Policy has been developed about EDIS data management. Calvary has an EDIS Data



Rec UID #	Report Rec #	Identifier	Recommendation	Audit comments as at 31 March 2018
			information feedback, and responds variance from data standards.	Management (who is also the Sys Admin), a suite of reports has been written to look at trends, examine data on a daily and weekly basis. These are available on the intranet for ED staff (evidence of this was sighted). These reports can be used by the clinicians to assess whether they are identifying trends.
128	17	RR17	The ED P&I Branch should work with each Division to improve data analytics.	ED, PRD meets with the EDs monthly and are developing new scorecards. There is a tender process to acquire an analytical tool. They have spoken with Finance about a new product group - categories of who they provide data to each month.
131	16	RR16	The ongoing improvements to Divisional scorecards, together with the introduction of the data repository and better data linkages provide opportunities to move from process measures to output and outcome measures and these should be exploited.	The Directorate continues to review and improve its performance indicators and is ensuring these exploit the new data warehousing capability.
132	18	RR18	Each Division should be provided with a monthly whole-of-hospital scorecard to better contextualize their Divisional performance.	Scorecards are in place. Monthly Divisional Scorecard sighted as part of review of evidence for Milestone One Report (18/9/17).
133	19	RR19	A workshop should be held across the Directorate and with relevant external stakeholders to review current priorities for data linkage initiatives within the ACT.	This was a suggestion made by Michael Reid in Dec 2012. It relates to linking data sets maintained by the Health Directorate and other ACT government agencies. By linking data, there could be a potential to improve output/outcome measures, that underpin management capacity. The new data warehouse has considered these linkages in its development. By using the WhoG OCDO platform this has addressed this recommendation to ensure linkages across directorates.
146	55	MR55	External data audit: that an external audit be commissioned to follow the coding audit of the costing data and conformance of the costing data to the NHCDC reporting standards. This audit should also be asked to report on fitness of costing data and system functionality for use of the costing reports for hospital operational management and feedback to clinical units on utilization benchmarking.	The whole costing process is reviewed and validated by ACT Health Directorate using software consultants. They look at what has been done, what has been loaded, comparison to previous years, and other jurisdictions before the data is released to IHPA. At the time of this report (and recommendation), this was in the early days of the costing data, now they have progressed significantly. They also have clinicians to assist.

Appendix A – Full list of recommendations and status as at March 2018

Rec UID #	Report Rec #	Identifier	Recommendation	Internal Audit Final assessment of progress (March 2018)
1	1	PWCR1	Design, develop and implement Data Governance and Data Management Framework for ACT Health.	Ongoing
2	32	PWCR32	Embed a data management and governance framework, that should include at least: <ul style="list-style-type: none"> • defining the ownership and accountabilities for data and reporting. This should include appointing an individual with the key accountability for the definition and oversight for data and information governance; • building and implementing the data management and governance model supporting the data owner(s); • defining the data quality requirements of all stakeholders reliant on BPIDS reporting; and • performing ongoing quality assurance and testing of the data warehouse. This should include ensuring that changes to business processes can be identified to understand the impact on data holdings and underlying calculations. 	Ongoing
3	5	SCPAR5	The Committee recommends that robust data validation processes be established for the Canberra Hospital and that the Government of the day report to the ACT Legislative Assembly on the first sitting day of 2013 on their implementation.	Ongoing
4	9	AG15R9	Validation Processes: The Health Directorate should develop and implement overarching policies and procedures related to data validation processes and activities. These should provide a consistent framework that is flexible and adaptable when needed to reflect local processes and organisation structure.	Ongoing
5	14	MR14	Principles and conditions of data access: that the governance arrangements for Health Directorate data holdings should include a statement of high level principles and general rules that apply to all data holdings.	Underway
6	5	RR5	There should be a Directorate wide suite of Standards, Standard Operating Procedures and Training modules required to be adopted for all data management.	Underway
7	6	RR6	The ED P&I Branch should be included in the list of data custodians within various legislative and data policy documents.	Underway
8	7	RR7	Information management issues should be a regular agenda item for discussions by the ICT Management Committee. The terms of reference and membership of this committee will need to be reviewed in light of this broadened scope.	Completed
9	8	RR8	As a general rule, Data Managers and Business Information Managers should be employed as out-posted officers of the P&I Branch.	No longer relevant
10	9	RR9	There should be a regular newsletter from P&I Branch to interested people within the Directorate on initiatives in information management with a particular focus on implementation of Activity Based Funding.	Underway



ACT Health Internal Audit Interim Report: Effectiveness of ACT Health's Implementation of Recommendations Relating to Data Integrity – Phase 4 Review

11	12	PWCR12	Develop and implement a formal Change Control Process for amendments to the Report (Annual and Quarterly Performance Reports), including: <ul style="list-style-type: none"> Change Request Template to capture changes requested; and Change Request Register to capture date and origin of change requested. 	Underway
12	13	PWCR13	Develop Governance Assurance Framework for BPIDS Reporting Function.	Underway
13	14	PWCR14	Develop Implementation Plan for the Governance Assurance Framework for BPI&DS Reporting Function. (This will incorporate the 'Reporting Program of Work' mapping activity)	Underway
14	17	PWCR17	Reporting Program of Work – mapping of the reporting environment (source to reports to stakeholders) and development of a 'risk heat map' based on current known issues with report processes (including SQL and ETL errors).	Underway
15	21	PWCR21	Develop procedural documentation for the end-to-end report creation process, including clear roles and responsibilities in alignment to the requirements definitions. Develop a formal approvals process for provisioning access to subscription reporting, in particular for those which report sensitive data. Develop a periodic review process for automated routine reporting, which re-assesses design appropriateness against requirements definitions, identifies any updates to content required due to organisational changes or similar, and considers reports that are no longer required and can be decommissioned.	Underway
16	26	PWCR26	Develop and implement a formal Change Control Process applicable to the provisioned reports and associated SQL/business logic.	Underway
17	16	PWCR16	Undertake full review of BPIDS response to Auditor-General Recommendations.	Completed
18	1	AG15R1	Change Management: As the Health Directorate implements its Information Management Strategy 2015-2016, change management activities should include: a) training Health Directorate and hospital staff to ensure they have an adequate understanding of the Strategy and specifically data integrity activities; and b) documenting and allocating responsibility for data integrity activities for the key systems, including ACTPAS, EDIS and the Health Directorate data warehouse.	Completed
19	12	SCPAR12	The Committee recommends that the Government of the day detail to the ACT Legislative Assembly, at the earliest possible opportunity, what action the Health Directorate has taken to assess whether a prevailing organisational culture at the Canberra Hospital contributed to the circumstances surrounding the alteration and misreporting of performance information.	Completed
20	10	SCPAR10	The Committee recommends that clear guidelines be established concerning internal communication between the ACT Health Directorate, the Canberra Hospital and Calvary Public Hospital.	Completed
21	11	SCPAR11	The Committee recommends that clear guidelines be established concerning external communication regarding matters concerning the ACT Health Directorate, the Canberra Hospital and Calvary Public Hospital.	Completed



22	2	AG12R2	<p>The Health Directorate and Calvary Public Hospital should develop essential EDIS governance documentation, including:</p> <ul style="list-style-type: none"> a) an overarching governance statement that describes: <ul style="list-style-type: none"> i. the purpose and use of the system; ii. its business owner, system administrator and all roles and responsibilities associated with the system and its support (including third party stakeholders such as Shared Services ICT); iii. the security classification of the system and its data; iv. applicable policy and administrative guidance; v. record-keeping obligations; vi. training requirements; and vii. what is monitored and audited to ensure compliance with policy and supporting system documentation. b) standard operating procedures for all roles and responsibilities associated with the system and its use; c) training material that covers all dimensions of EDIS including user roles and responsibilities, processes described in standard operating procedures and specific policy that is applicable to the system; and d) a System Security Plan, which is informed by a risk assessment and risk management plan. 	Completed
23	4	AG12R4	<p>The Health Directorate and Calvary Public Hospital should:</p> <ul style="list-style-type: none"> a) review the current distribution of access to EDIS throughout the hospital and remove any users who do not have a specific and documented requirement for access to the system; and b) develop policies, administrative procedures and system controls (if possible) that restrict the use of generic user accounts outside the Emergency Department work environment. 	Completed
24	5	AG12R5	<p>The Health Directorate and Calvary Public Hospital should:</p> <ul style="list-style-type: none"> a) identify and document responsibilities for user access management and log monitoring for EDIS; and b) develop a process to monitor user activity within EDIS and how to report and escalate unusual activity to the appropriate authorities. 	Completed
25	7	AG12R7	<p>The Health Directorate should develop policy and administrative guidance for EDIS data validation activities for the two Canberra hospitals. The policy and administrative guidance should identify and document: a) agreed Emergency Department actions which constitute 'clock starting' and 'clock stopping' moments for the purpose of EDIS timeliness records; and b) protocols for data validation activities in the day(s) following a patient's presentation to the Emergency Department.</p>	Completed
26	8	AG12R8	<p>The Health Directorate should implement additional review and assurance controls over the preparation and reporting of Emergency Department timeliness performance information. These review and assurance controls should address both Canberra Hospital and Calvary Public Hospital performance information. The Health Directorate should consider whether the additional review and assurance controls should be applied to other performance information.</p>	Completed
27	5	AG15R5	<p>Patient Record Close Period:</p> <ul style="list-style-type: none"> a) Calvary Public Hospital should align its EDIS record close period (i.e. the period after which records are locked) with that of Canberra Hospital. b) The Health Directorate should undertake a monthly assessment to monitor changes to patient records after the close period. 	Completed
28	6	AG15R6	<p>Training Materials: Canberra Hospital should finalise its draft EDIS training documents and implement a mandatory requirement for staff to complete EDIS training before receiving access to the system.</p>	Completed



29	14	AG15R14	Reporting of ABF Costing Data: The Health Directorate should develop and publish a costing framework which: a) allocates roles and responsibilities between the Health Directorate and hospitals; b) specifies a firm schedule for hospitals to submit costings; c) incorporates a costing data specification; d) outlines a costing review and validation process; and e) includes an urgent issue escalation process.	Completed
30	18	AG15R18	Clinical Coding: Canberra Hospital and Calvary Public Hospital should improve their clinical coding with the following process changes. a. Where coding is completed before the availability of the discharge summary, the medical record should be flagged, to facilitate subsequent identification of potentially incorrectly coded episodes. b. Where the discharge summary directly conflicts with information in the record, a query should be forwarded to the treating clinician for clarification. These queries should be followed-up and documented for future reference.	Completed
31	1	MPR1	Registers be established and maintained of reports issued and data holdings maintained and that these registers be developed as the key control mechanism for the report release authorization and recording process.	Completed
32	20	PWCR20	Develop and agree requirements definitions for automated routine reports. This is to include identification of a relevant business report owner.	Underway
33	1	MR1	A record of reports issued and data sources: that a register of statistical and management reports (Register of Reporting – RoR) be prepared and maintained by P&I Branch from monthly returns from each of the areas using and analysing data.	Completed
34	7	MR7	Operational information systems that generate data and reports: that the example list of source systems and data holdings in Table 1 above be replaced by a systematically maintained Register of Operational Data Stores. This should be then used as a standard reference point to identify source data used in reports and data extract cover sheets.	Underway
35	10	MR10	Data custodians and recording of data releases: that a responsible custodian is identified for each data holding – and levels of delegation for release specified in the Register of Reporting.	Underway
36	11	MR11	Data custodians and recording of data releases: that a specified subject matter expert is identified for each data holding who has a defined role in its management.	Underway
37	12	MR12	Data custodians and recording of data releases: that an auditable register be maintained of standards applicable to each data holding – dates of implementation and updates to the standards. These standards and policies should include metadata specifications, release policies and procedures, access policies and register, security arrangements and audit documentation.	Underway
38	13	MR13	Data custodians and recording of data releases: that each data holding is classified according to its level of access and level and category of risk.	Underway
39	27	MR27	Report credentialing and conditions of release: that the Register of Reports also identify the responsible data custodian by position for each of the datasets and link to standard documentation of standard conditions of release of the dataset, subsets or reports.	Underway



40	28	MR28	Data audit status and metadata standards: that for each of the systems in the Register of Reports, the audit status of system access and the security of record change history system functions and supervision be identified and updated when audit actions are scheduled and completed.	Underway
41	51	MR51	Identification of report authorship and underpinning data status: that the register record responsible management points from source to analytical output for each periodic report.	Underway
42	1	RR1	A register of all Directorate external data provision should be developed and maintained.	Completed
43	5	MPR5	Office of Data Integrity be established and supported by direct report senior executive on progress with implementation of the recommended building blocks and provide a focal point for receiving and follow up of data integrity concerns.	No longer relevant
44	61	MR61	The Office of Data Integrity: that the Data Integrity Adviser position be staffed as soon as possible and the Office of Data Integrity be tasked with the priority function of delivering a three year external audit program as well as ongoing responsibility for risk assessment and support for professionalism in health information management and data recording in particular.	No longer relevant
45	62	MR62	The Office of Data Integrity: that the Data Integrity Adviser be asked to report annually on progress with implementation of those elements of this Data Integrity Strategy that are agreed by the Health Directorate Executive.	No longer relevant
46	25	MR25	Health information professionalism: that on recruitment to data management and analysis positions, qualifications and/or practical experience should be sought according to role in skills areas such as:- a. health informatics b. health information system analysis c. health information management d. epidemiology e. health econometrics f. health statistics g. Casemix/ABF. h. health classifications i. clinical costing.	Ongoing
47	26	MR26	Health information professionalism: that current staff should be encouraged and facilitated in attending continuing professional education forums – extension courses symposia and conferences in the above fields.	Ongoing
48	21	RR21	An assessment of the skills and competencies of people involved in data management and dissemination should be undertaken. Targeted education and training should be provided to accommodate identified skills deficiencies.	Ongoing



49	60	MR60	Data qualifications and disclaimers: that the data qualification categories listed in IHPA's Data Integrity Framework be incorporated by the ACT Health Directorate into the RoR notations at least in the early stages of IHPA reporting routines. Once these thresholds become historic, finer thresholds for qualification and disclaimers that identify confidence levels in data precision and rigor would and should almost certainly be introduced.	No longer relevant
50	31	PWCR31	Create a data management strategy and roadmap. This document should define responsibilities for data management, information management and reporting . It should reflect the current state and desired state architectures and provide a roadmap (and a budget) to facilitate the required improvement in maturity. The strategy should define the role of source systems, reporting databases and the data warehouse , and should define the high level business requirements and metrics proposed to assess the strategy's implementation.	Underway
51	30	PWCR30	Define the architecture to support development of a roadmap that can prioritise what reporting is performed and the systems required. This will require maturing any existing enterprise architecture (EA) documentation, which should include the business architecture, technical architecture, data architecture and application architecture. This will also require management agreement of the desired end state for data management and reporting (that should consider both benefits and costs).	Underway
52	17b	AG15R17b	Non-Admitted Patient Data and Systems: The Health Directorate should implement a single patient management system, and standardise data management policies and procedures, across all public outpatient clinics.	Underway
53	6	AG12R6	The Health Directorate should: a) review the current EDIS upgrade project and link it with current Health Directorate Identity and Access Management and Rapid Sign-On initiatives that are currently underway, to allow staff to be individually accountable for their actions; and b) review all available Emergency Department software to evaluate whether or not the current EDIS should be replaced with one that has strong confidentiality and integrity controls as well as appropriate process linkages.	Underway
54	6	SCPAR6	The Committee recommends that, consistent with the recommendation of the Auditor-General, the rapid sign-on system be implemented as soon as practicable and that the Government of the day report to the ACT Legislative Assembly at the earliest opportunity on its implementation.	Completed



55	6	MR6	<p>Data repositories: that the concept of a 'one source of truth' data repository for management data access be clarified in terms of</p> <ul style="list-style-type: none"> a. data holdings design: particularly extraction and transformation points and points at which automated and manual coding, ETL, storage, processing and aggregation occur. b. data provenance: particularly the level of detail summarisation at each stage of case or unit of activity bundling and classification – (see section 4.5 below for further detail); c. development of reporting requirements and level of data abstraction; d. capacity and data quality assurance protocols for reconciling and replicating important counts and measures with original source records in operational and business systems; e. audit requirements and audit plans for reports and data extracts against source records or other evidence. f. mapping of historical data to current dataset versions to permit longitudinal comparative analysis. 	Underway
56	12	RR12	The timeframe and scope of data inputs to the data repository needs urgent clarification.	Underway
57	40	PWCR40	Develop new data warehouse	Underway



58	34	PWCR34	<p>Design and build the data warehouse, which should include:</p> <ul style="list-style-type: none"> • understanding the range of existing source information systems (and supporting source databases) and agreed sources of truth for each data type; • defining the detailed business reporting requirements of each branch, including the level of business intelligence and analytics required; • defining the detailed business reporting requirements of each branch, including the level of business intelligence and analytics required; • designing a data model aligned to the data architecture and agreed naming conventions; • creating a technical design that incorporates the platform, capacity and performance requirements, indexation, user access, change management etc.; • defining the required data transformation services, including ETL from source systems; • testing the build to ensure business logic is correctly applied when reporting from the warehouse. This will require the design and test teams having access to key business process documentation for source systems (including EDIS and ACTPAS) to define and review business logic in place. Ensure changes to business processes can be identified to understand the impact on data holdings and underlying calculations; and • decommissioning of existing data warehouse databases that will no longer be required. 	Underway
59	41	PWCR41	Consider introducing new technologies	Completed
60	35	PWCR35	<p>Undertake an assessment of the application of emerging data technologies for ACT Health. For example, data virtualisation tools would allow dynamic usage of data from multiple source systems for ad-hoc reporting. This would allow limiting the data warehouse to key required fields, and additional fields only used occasionally would not need to be stored in the data warehouse.</p> <p>A separate category of data management tool covers data visualisation. ACT Health are not currently leveraging these tools for most reports, which could improve the efficiency of report generation and the impact that reports have on different stakeholders.</p>	Ongoing



61	24	MR24	<p>Help desks: that within CIOs Branch, a help desk be set up for ICT systems operation queries – locii of responsibility and SME should be differentiated and clarified. In particular the functions of the SSICT help desk should be reviewed in relation to the IM help desk to ensure there are no gaps. The core functions of the system help desk should include.</p> <ol style="list-style-type: none"> a. system components operation <ol style="list-style-type: none"> i. system performance review ii. system development and integration iii. system provider management – including shared services b. system access registration and c. system login tracking security monitoring and d. system access audits. 	Completed
62	7	AG15R7	<p>Audit Logs: Both Canberra Hospital and Calvary Public Hospital should establish useable audit logs for EDIS to allow monitoring activities after the close off period. The audit logs should be reviewed regularly, with results presented to the accountable hospital executives and to the Health Directorate.</p>	Underway
63	15	MR15	<p>Principles and conditions of data access: that general rules and specific rules for particular data holdings be:</p> <ol style="list-style-type: none"> a. readily available to users and b. linked to the system access points c. acknowledged by users at the point of use as part of the access procedure. (In the same way as conditions of issue of airline tickets – or acknowledgement of license conditions before loading software.) 	Completed
64	16	MR16	<p>Principles and conditions of data access: that the eHealth strategy provisions for data holdings management be expanded and promulgated to staff both as</p> <ol style="list-style-type: none"> a. general topic manuals with rules applicable across all data holdings and b. specific purpose documents associated with each data holding. 	Underway



65	18	MR18	<p>Principles and conditions of data access: that changes in the specification, standards or provisions of access to any data holding be:</p> <ol style="list-style-type: none"> promulgated to registered users; listed in a running bulletin at a central web location; maintained in documentation associated with the data holding. 	Underway
66	31	MR31	<p>Data systems security management: that system access profiles be developed for each staff category and clinical role where use of records systems is required. That system logons be refined to facilitate access for authorised personnel and restrict access to unauthorized personnel.</p>	Completed
67	32	MR32	<p>Data system security management: that a register of [people] authorised to access data holdings in the systems be established for each operational system and level of access for each authorised person be specified – role, data entry – data correction –and data deletion.</p>	Completed
68	33	MR33	<p>Data system security management: that for all databases, a system be enabled to log and register:-</p> <ol style="list-style-type: none"> history of database access, history of <ol style="list-style-type: none"> record search, record extraction, record entry, record completion, record change action and reasons for change. 	Underway



69	35	MR35	Data system security management: that for data entry and system management staff similar logon authorization management and data access logs be maintained as for other system users be maintained.	Completed
70	3	SCPAR3	The Committee recommends that the Government of the day review the security of information which identifies individual patients at the Canberra Hospital and report on the outcomes of this review to the ACT Legislative Assembly on the first sitting day of 2013.	Completed
71	8	SCPAR8	The Committee recommends that all ACT Government directorates and agencies should prioritise as a matter of urgency an assessment of the adequacy of controls over their respective IT systems and applications. This should include consideration of the controls that affect the reliability of all IT systems and applications (general controls) and controls that are specific to each application (application controls).	Completed
72	14	SCPAR14	The Committee recommends that the Commissioner for Public Administration, in consultation with ACT Government directorates and agencies, develop a whole-of-government policy for the management of private information relating to ACT Public Service employees and recipients of ACT Government services.	No longer relevant
73	17	MR17	Principles and conditions of data access: that a program of review of data access arrangements be developed so that each data holding is covered at least once each year or according to risk rating.	Completed
74	11	PWCR11	Review and update access controls to Shared Network Drive for PI (Report Template) and DSS (Report Proof).	Completed
75	23	PWCR23	Apply access controls to the SQL query and the Excel file used to populate the Surgeon Wait Times public report.	No longer relevant
76	24	PWCR24	Reduce levels of 'write' access to report files (.rdl files), to include only the data team who actively manage the reports.	Underway



77	38	PWCR38	Apply PwC's SQL fixes to MORBID and continue to use MORBID.	No longer relevant
78	36	PWCR36	Apply PwC's SQL fixes to MORBID and continue to use MORBID in the short term for external reporting.	No longer relevant
79	34	MR34	Data system security management: that regular audits of access be conducted and unusual patterns of access – particularly systematic record change be reviewed and/or investigated.	Ongoing
80	40	MR40	Data access management: that access registers be analysed on a regular basis to identify systematic patterns of access to data records for change or update.	Completed
81	41	MR41	Data access management: that annual audit programs include a review of access registers and investigation of atypical systematic access patterns.	Ongoing
82	36	MR36	Training in values and best practice in data security: that data entry and data review staff be trained in the ethics of data security.	Ongoing
83	37	MR37	Training in values and best practice in data security: that data entry and data review staff are provided on a regular basis with feedback for their checking and confirmation on: a. Patterns of data access with reasons. b. Results of data validation and QA on the data that they have entered or accessed for further action. [The purposes for this include ensuring that all staff can be held responsible for their own logons and that possible false logons are identified quickly.]	Completed
84	38	MR38	Training in values and best practice in data security: that staff with discrepant levels of validation or edit queries be provided with further training or guidance.	Completed
85	9	AG12R9	The Director-General of the Health Directorate and the ACTPS Head of Service note the findings of this report with respect to the executive who has admitted to manipulating hospital records, and consider whether this executive has engaged in misconduct in breach of section 9 of the Public Sector Management Act 1994 and their executive contract.	Completed
86	10	AG12R10	The Health Directorate reinforce to Health Directorate employees, especially executive staff, the need to act with integrity with respect to the maintenance of health records and associated data.	Completed



87	13	SCPAR13	The Committee recommends that, given the Health Directorate's failure to protect the privacy of the Executive who admitted to altering data—prior to any civil, criminal or administrative proceedings—the Health Directorate should: (i) issue a public apology to the individual concerned; and (ii) take appropriate steps to acknowledge the individual's contributions to the operation and administration of the Canberra Hospital.	Completed
88	42	MR42	Data access management: that as staff leave positions or move from role to role, access authorisations be automatically removed and reinstated as appropriate.	No longer relevant
89	2	PWCR2	Undertake a full Data Warehouse reconciliation and integrity validation check against source systems. This will include business and technical confirmation of data alignment.	Underway
90	19	PWCR19	Identify appropriate additional resource/s who will require 'run' access to support current single resource for CHARM.	Completed
91	8	MR8	Operational information systems that generate data and reports: that system development plans for any business system component include a comprehensive schedule of interfaces and tabulation of the interface metadata references and particulars.	Completed
92	4	AG15R4	Define ABF-Related Data Mapping: Health Directorate should develop an Emergency Department Data Dictionary to standardise the definition of ABF-related data and define ABF-related data mapping from EDIS in both hospitals to the data warehouse.	No longer relevant
93	15b	AG15R15b	Risk Based Approach to Investigations: As a priority, the Health Directorate should review the mapping processes used to extract data from EDIS to the data warehouse, and ensure that Admitted Patient principal diagnosis and Emergency Department type of visit are mapped appropriately.	Underway
94	9	MR9	Operational information systems that generate data and reports: that mapping tables used at each interface between business system components be maintained in a register that links to the metadata data registry standards for each end of the map so that each time the standards are revised the interfaces to be updated will be identified and flagged.	Underway