AIRPORT, WATER AND WASTE COMMITTEE MEETING

AGENDA

15 AUGUST 2017

Your attendance is required at a meeting of the Airport, Water and Waste Committee to be held in the Council Chambers, 232 Bolsover Street, Rockhampton on 15 August 2017 commencing at 3.00pm for transaction of the enclosed business.

R Cheesman

ACTING CHIEF EXECUTIVE OFFICER
9 August 2017

Next Meeting Date: 19.09.17

Please note:

In accordance with the *Local Government Regulation 2012*, please be advised that all discussion held during the meeting is recorded for the purpose of verifying the minutes. This will include any discussion involving a Councillor, staff member or a member of the public.

TABLE OF CONTENTS

1 OPENING

2 PRESENT

Members Present:

Councillor N K Fisher (Chairperson)
The Mayor, Councillor M F Strelow
Councillor R A Swadling
Councillor A P Williams
Councillor C E Smith
Councillor C R Rutherford
Councillor M D Wickerson

In Attendance:

Mr P Kofod – General Manager Regional Services (Executive Officer)
Mr E Pardon – Chief Executive Officer

3 APOLOGIES AND LEAVE OF ABSENCE

4 CONFIRMATION OF MINUTES

Minutes of the Airport, Water and Waste Committee held 18 July 2017

5 DECLARATIONS OF INTEREST IN MATTERS ON THE AGENDA

6 BUSINESS OUTSTANDING

Nil

7 PUBLIC FORUMS/DEPUTATIONS

Nil

8 OFFICERS' REPORTS

8.1 ROCKHAMPTON AIRPORT - MONTHLY OPERATIONS REPORT - PERIOD ENDING JULY 2017

File No:	**7927**
Attachments:	**1. Rockhampton Airport July 2017 Monthly Operations Report**
Authorising Officer:	**Scott Waters - General Manager Regional Development and Aviation**
Author:	**Tracey Baxter - Acting Manager Airport**

SUMMARY

The monthly operations and annual performance plan report for the Rockhampton Airport for July 2017 is presented for Councillors information.

OFFICER'S RECOMMENDATION

THAT the Rockhampton Airport Operations and Annual Performance Plan Report for July 2017 be 'received'.

COMMENTARY

The monthly operations and annual performance plan report for the Rockhampton Airport of the Regional Development and Aviation Department is attached for Council's consideration.

CONCLUSION

It is recommended that the monthly operations and annual performance plan report for the Rockhampton Airport for July 2017 be received.

ROCKHAMPTON AIRPORT - MONTHLY OPERATIONS REPORT – PERIOD ENDING JULY 2017

Rockhampton Airport July 2017 Monthly Operations Report

Meeting Date: 15 August 2017

Attachment No: 1

Monthly Operations Report

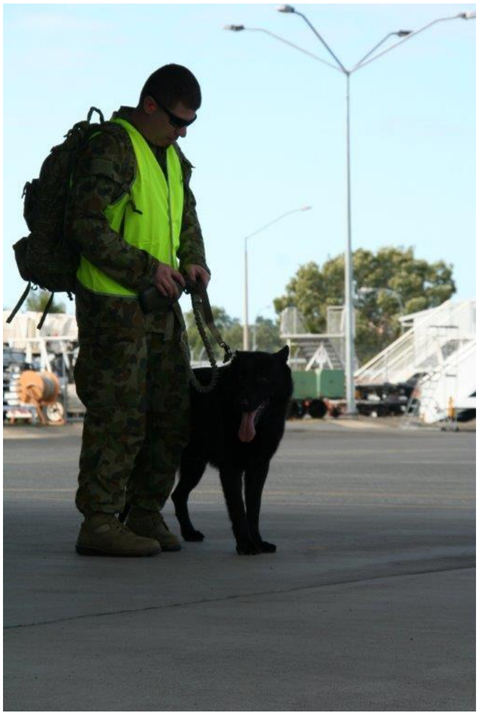
Rockhampton Airport

July 2017

1. Highlights

The Department of Defence commenced operations at Rockhampton Airport for military Exercise Talisman Saber 2017. The Exercise is a biennial military training activity conducted between Australian and United States air, land and maritime forces and is the largest combined military exercise undertaken by the Australian Defence Force (ADF). This will be the seventh time the exercise has been conducted, involving over 30,000 Australian and US participants.

This year the airport supported a variety of charter aircraft, wide bodied military and numerous Australian and American Defence Force helicopters.



2. Innovations, Improvements and Variations

(Operational Plan Ref:

5.3.2.1 Identify at least one operational saving per section of responsibility

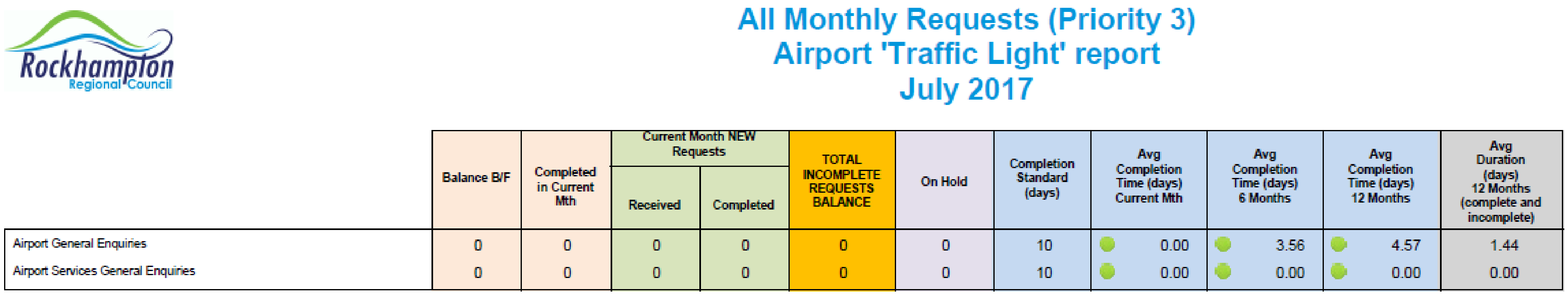
5.4.2.6 Identify at least two improved processes per section of responsibility)

Nil Innovations, Improvements or Variations recorded for the reporting period.

3. Customer Service Requests

(Operational Plan Ref: 4.1.1.1 Provide timely and accurate responses to requests)

Response times for completing customer requests in this reporting period for July 2017 are within set timeframes.



Rockhampton Regional Council

All Monthly Requests (Priority 3)
Airport 'Traffic Light' report
July 2017

	Balance B/F	Completed in Current Mth	Current Month NEW Requests		TOTAL INCOMPLETE REQUESTS BALANCE	On Hold	Completion Standard (days)	Avg Completion Time (days) Current Mth	Avg Completion Time (days) 6 Months	Avg Completion Time (days) 12 Months	Avg Duration (days) 12 Months (complete and incomplete)
			Received	Completed							
Airport General Enquiries	0	0	0	0	0	0	10	🟢 0.00	🟢 3.56	🟢 4.57	1.44
Airport Services General Enquiries	0	0	0	0	0	0	10	🟢 0.00	🟢 0.00	🟢 0.00	0.00

4. Service Delivery

(Operational Plan Ref: 4.1.1.2 Provide effective delivery of Council services)

Non-Financial Performance Targets & Required Outcomes
Required Outcomes compared for the same period in 2016/2017:

	Monthly Target	**Result** **Monthly / YTD**	
Passenger Numbers**	0%	2.44%	/ 2.44%
Aircraft Movements*	0%	-9.89%	/ -9.95%
Bird Strikes	3 per month	2	/ 2
Lost Time Days – workplace injuries	0	0	/ 0
Reported Public Injuries on Airport Precinct	0	0	/ 0
Customer Requests Actioned	100%	100%	/ 100%
Airline Engagement Meetings	Every 3 months	100%	/ 100%
Military Exercise Briefings Attended	100%	100%	/ 100%

*Aircraft Movements – July 2017 figures were not available on Airservices Australia website at the time of lodging the report. May 2017 figures were utilised for statistical data and therefore year to date **(YTD) Aircraft Movement data is only up until May 2017.**

5. Legislative Compliance and Standards (including Risk and Safety)

(Operational Plan Ref: 5.2.1.1 Comply with legislative requirements)

Legislative Compliance & Standards

Legislative Compliance Matter	Due Date	% Completed	Comments
Biannual Review of Airport Security Risk Register	September 2017	20%	Review assesses security measures and procedures to consider if they are adequate to meet the requirements of the local security risk context statement.
Annual Review of Airport SMS Risk Register	October 2017	0%	Review is conducted at least annually to determine whether the nominated risk treatments/controls remain valid for the risks identified. The RRC Risk Calculator is used to quantify the current risk rating.
Annual Airport Electrical Inspection	November 2017	0%	Aerodrome Operation Support Pty Ltd conduct an annual inspection of the key aviation related electrical components at the aerodrome.
Annual Airport Technical Inspection	November 2017	0%	Aerodrome Operation Support Pty Ltd conduct an annual inspection of the aerodrome facilities, equipment, procedures and OLS.
Emergency Exercise (Field Top Exercise)	May 2018	0%	An onsite emergency exercise is required to be conducted at least every second year. The 2017 exercise scenario will be the basis for the 2018 on site exercise.
Annual Runway Friction Testing	March 2018	0%	An external contractor is engaged to undertake this specialised testing.

Safety Statistics

The safety statistics for the reporting period are:

	FIRST QUARTER 2017/2018		
	July	August	September
Number of Lost Time Injuries	0	N/A	N/A
Number of Days Lost Due to Injury	0	N/A	N/A
Total Number of Injuries	0	N/A	N/A
Number of Completed Hazard Inspections	N/A	N/A	N/A

Risk Management Summary

Potential Risk	Current Risk Rating	Future Control & Risk Treatment Plans	Due Date	% Completed	Comments
Security breach or threat at the airport resulting in possible death or injury, reputation damage to the airport, additional costs, disruption to airline services due to airport closure, infrastructure damage, fines in relation to a regulatory breach	Moderate 6	Replace hard key system on all gates and access points with proximity card electronic card system so lost cards can have access withdrawn.	30/06/2018	90%	Final stages of the design of an automatic emergency access gate for emergency services. The Airport system requires a software update which is expected to occur in late August 2017.
Airport revenue decreases over a sustained period resulting in the airport performance KPI's not being met, budgetary impacts, reduced availability of funds for capital programs.	Moderate 5	Redevelop the airport terminal to increase retail revenue.	Terminal 1/07/2020	80%	The options for Terminal redevelopment will be further considered as part of the Airport Master Planning process.
Airport assets not maintained, upgraded, inspected or monitored effectively in accordance with regulatory requirements resulting in possible death or injury, reputational damage,	Moderate 6	Facility maintenance and condition assessment inspection schedules are in the process of being completed and detailed in conquest. Upgrade of	Stage 1: 30/6/2015	80%	Main Runway condition re-assessment by AECOM completed and recommendations included in 10 yr Capex program. Chilled water system capacity improved with better control system and new heat exchange units High Risk Fire Hydrant Systems now completed Air-conditioning condition

Potential Risk	Current Risk Rating	Future Control & Risk Treatment Plans	Due Date	% Completed	Comments
compliance failure, reduced service delivery, WH&S fine		RPT and GA Apron flood lighting to meet LUX standards. Review of Asset Management Plan	30/06/2018		report completed. HV Transformers condition evaluation completed. Roads pavement condition assessment completed Airport Council owned buildings condition assessment completed and priority 1 defects being addressed. FRW has undertaken condition report on mains water and replacement of priority section completed final section in Capex program.

6. Operational Plan Targets by Section

Operational Plan Targets for the Rockhampton Airport are encapsulated within the whole of Regional Development and Aviation departmental monthly report.

7. Capital Projects

As at period ended **July** – **8.3%** of year elapsed

Project	Planned Start Date	Planned End Date	Status	Budget Estimate	YTD actual (incl committals)
ROCKHAMPTON AIRPORT CAPITAL WORKS PROGRAM					
959133 – RPT Apron Lighting	29/08/13	June 2018	**WIP** Installation of six new switchboards at each apron light pole, four complete, two remaining. Operations to review aircraft parking requirements prior to conducting design review to consider LED Lighting and installation.	$600,000	$0
Commentary: To obtain regulatory compliance a condition assessment was conducted in 2014 with upgrade recommendations identified one area remaining non-compliant. Engineering assessment confirmed additional lights could be installed on existing poles. Original concept design under review to investigate options of LED installation and review parking layout. Testing of electrical supply cables identified that they were close to failure. Project to be delivered in two stages, Stage 1 16/17 – Replace and upgrade electrical supply cables, Lighting Design Review and Project Concept, Stage 2 17/18 – Implement compliant system.					
959135 – GA Apron Lighting	17/02/12	June 2018	**WIP** Remainder of project postponed to allow reconfiguration of cross runway. Operations to review of aircraft parking requirements prior to conducting design review to consider LED Lighting and installation.	$0	$0
Commentary: To obtain regulatory compliance a condition assessment was conducted in 2014 with upgrade recommendation. Original concept design under review to investigate					

Project	Planned Start Date	Planned End Date	Status	Budget Estimate	YTD actual (incl committals)
options of an LED installation and review aircraft parking layout. System remains non-compliant due to inability to infringe the airspace of Runway 04/22; this will be rectified in Stage 3 following Runway 04/22 displacement. Project to be delivered in three stages, Stage 1 15/16 – Install three lights for RFDS Operations, Stage 2 16/17 – Lighting Design Review and Project Concept, Stage 3 18/19 – Implement compliant system.					
987694 – Refurbish Terminal Concourse Toilets	Early 2015	Phase 1 – September 2017	**WIP** Contractor engaged of Stage 1 – Removal of entry doors from all four main toilets. Materials have been procured, planning for works has commenced.	$0	$39,947
Commentary: It has been identified that the terminal toilets are not meeting the current passenger needs and impede passenger flow through the terminal. Toilets need to be refurbished and reconfigured to improve customer service levels. Project to be delivered in three stages, Phase 1 – Removal of toilet entry doors, Phase 2 – Reconfigure Southern toilet facilities, Phase 3 – Reconfigure Northern toilet facilities.					
987712 – Replace General Aviation Power Switchboards	Early 2015	Phase 2 - October 2017	**WIP** Contractor to supply and replace Area 3 (Aeroworx) Switchboard has been engaged and waiting delivery.	$60,000	$14,863
Commentary: A condition assessment conducted in 2015 has identified that several General Aviation switchboards are in various stages of deterioration and will require replacement. Project Concept Design has been developed to accommodate future potential business growth and system upgrade requirements. Replacement of Area 3 (Aeroworx) Switchboard identified as a priority due to age and non-compliance, Phase 1 – Design Are 3 Switchboard 16/17 ($17,250), Phase 2 – Implement Area 3 Switchboard 17/18 ($60,000). Remaining switchboards replacements have been postponed until to 2026/27.					
1047109 – Replace existing storage-workshop-office-lunchroom (site BD)	Sept 15	June 2018	**WIP** Proposed building works have been presented to the RRC Duty Planner who advised: • A Development Application will be required including	$100,000	$857

Project	Planned Start Date	Planned End Date	Status	Budget Estimate	YTD actual (incl committals)
			a Flood Hazard Assessment – in progress. • Sewer connection infrastructure - completed		
Commentary: Several issues with the buildings within the Aeroworx complex were identified in the RRC Asset Building Inspection in 2014. Electrical switchboard issues were identified in condition assessment conducted in 2015. Office building and electrical switchboards are beyond repair therefore requiring replacement. The project scope is to extend hanger, renew electrical connection and replace office and lunchroom.					
987926 – Upgrade terminal standby power generator	Sept 15	September 2017	**WIP** Construction works are progressing to plan. New system now operational. Terminal BMS being connected for monitoring. Additional works required to remove the in-ground fuel tank is being planned.	$100,000	$41,610
Commentary: Current generator only supplies a portion of the Terminal, it failed during cyclone Marcia and failed again not long after and replaced with a hire generator. The replacement generators are an essential component of the Airport Business Continuity Plan.					
987723 – Replace Air Conditioning Chilled Water Unit	Jan 17	June 2018	**WIP** Engineering consultancy services have been engaged to assist in Developing a Project Concept Plan & Scope of Works for the complete Terminal Air Conditioning System, for approval.	$300,000	$6,500
Commentary: The Chiller unit has reached the end its expected life. This has been quantified by several component failures over recent years. With the current load on the chiller it is required to operate at 100% capacity to cool the Airport Terminal during the hottest portion of the year.					

Project	Planned Start Date	Planned End Date	Status	Budget Estimate	YTD actual (incl committals)
The project will consist of a concept (scope of works), design, construction and commissioning stages. While this project continues over several years the initial concept and design will be for the entire project.					
987704 – Improve Airside Stormwater Management	July 2017	June 2018	**WIP** Management framework for project to be finalised	$520,200	$0
Commentary: The Rockhampton Airport has recently experienced several cases of subsidence within flight area of the airport. The drainage of the Airport is a key factor in the continued aeronautical operation during extreme weather. The intention of this project is to evaluate the causes of this subsidence and the effectiveness of current drainage systems. This will include implementing strategies to improve drainage and remedial work on existing drainage systems.					
989183 – Terminal Refurbishment – Auto Doors	July 2017	June 2018	**WIP** Technical Specification being developed	$135,000	$0
Commentary: Terminal automatic entry doors are approaching the end of their useful life. Currently there are safety concerns with these doors, with small children able to be impacted by the door mechanisms. Project scope has been revised to initially upgrade the control system and drive mechanisms on the nine oldest doors.					
987727 –Master planning and reconfiguration	Late 2015	July 17	**WIP** Completion of Airport Masterplan	$0	$2,440
Commentary: Ongoing engagement with LEAPP.					
987685 – Renewal of aviation security infrastructure	Ongoing	Ongoing	**WIP** Finalising design requirements to install automatic vehicle gate at Airside Security Gate 1.	$0	$68,422

Project	Planned Start Date	Planned End Date	Status	Budget Estimate	YTD actual (incl committals)
Commentary: Operational need identified to replace Airside Security Gate 1 due to emergency access requirements and high usage during military exercises.					
959150 – Runway Lighting System Replacement	18/12/11	31/11/17	**WIP** • Stage 1 – Practical completion issued 24 April 2014. List of final defects repaired. • Stage 2 – Practical completion has been issued. Issues with initial Contractor being available to repair defects. Current on-site contractor have commenced defect rectification. • Stage 3 – Currently working through the commissioning and regulatory process. Decommissioning of current system to commence pending regulatory approval.	$0	$232,380
Commentary: Major Projects are managing this project; please refer to the Major Projects Monthly Report for more detail. The Airport Lighting System was commissioned on the 5th June, ongoing rectification works to be undertaken in the coming months.					
1076549 - Smart business hub business lounge	**TBA**	**TBA**	**TBA**	$60,000	$0.00

8. Operational Projects

Nil Operational Projects to report at Rockhampton Airport during the month of July 2017.

9. Budget

Financial performance as expected for the reporting period

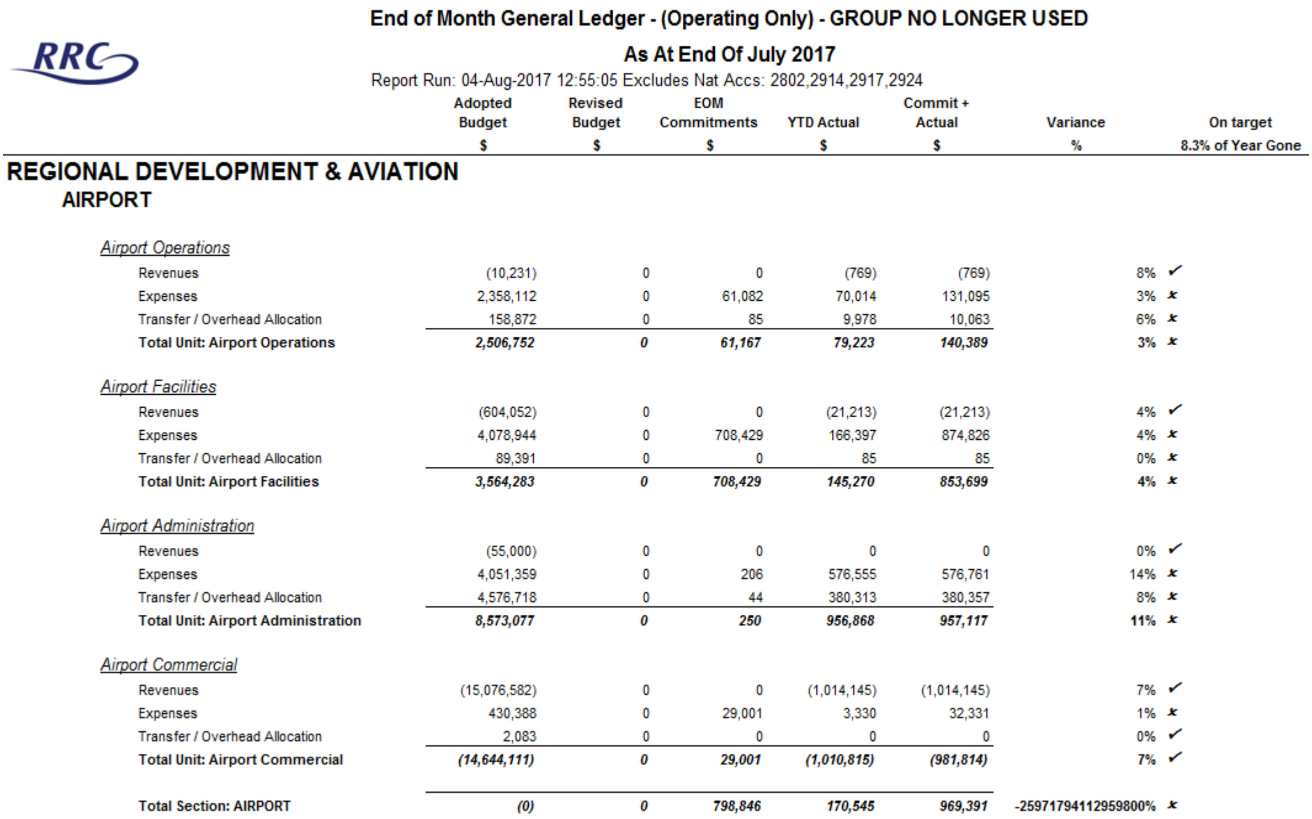
AIRPORT FINANCIAL

Summary

Total revenue is below the percentage of year elapsed at 6.58% due to Tax Invoice timing delays. Operating expenditure is also lower than the percentage of year elapsed at 7.66% resulting in a current surplus position for the Airport.

Capital

Overall Airport's capital expenditure is below the percentage of year elapsed at 0.24% of budget with expenditure expected to be brought closer to budget as the year progresses.



RRC

End of Month General Ledger - (Operating Only) - GROUP NO LONGER USED

As At End Of July 2017

Report Run: 04-Aug-2017 12:55:05 Excludes Nat Accs: 2802,2914,2917,2924

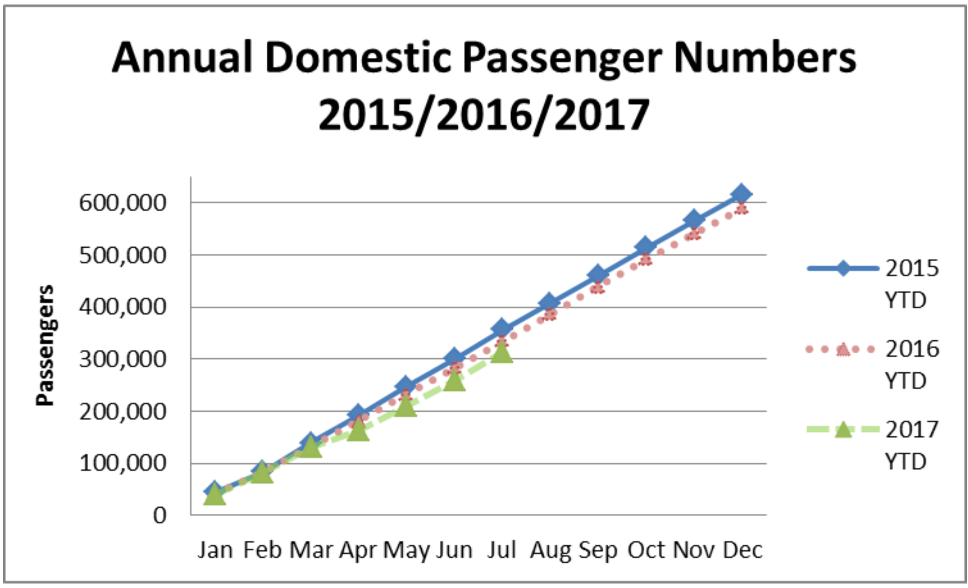
	Adopted Budget	Revised Budget	EOM Commitments	YTD Actual	Commit + Actual	Variance	On target
	$	$	$	$	$	%	8.3% of Year Gone
REGIONAL DEVELOPMENT & AVIATION							
AIRPORT							
Airport Operations							
Revenues	(10,231)	0	0	(769)	(769)	8%	✓
Expenses	2,358,112	0	61,082	70,014	131,095	3%	✗
Transfer / Overhead Allocation	158,872	0	85	9,978	10,063	6%	✗
Total Unit: Airport Operations	***2,506,752***	***0***	***61,167***	***79,223***	***140,389***	**3%**	✗
Airport Facilities							
Revenues	(604,052)	0	0	(21,213)	(21,213)	4%	✓
Expenses	4,078,944	0	708,429	166,397	874,826	4%	✗
Transfer / Overhead Allocation	89,391	0	0	85	85	0%	✗
Total Unit: Airport Facilities	***3,564,283***	***0***	***708,429***	***145,270***	***853,699***	**4%**	✗
Airport Administration							
Revenues	(55,000)	0	0	0	0	0%	✓
Expenses	4,051,359	0	206	576,555	576,761	14%	✗
Transfer / Overhead Allocation	4,576,718	0	44	380,313	380,357	8%	✗
Total Unit: Airport Administration	***8,573,077***	***0***	***250***	***956,868***	***957,117***	**11%**	✗
Airport Commercial							
Revenues	(15,076,582)	0	0	(1,014,145)	(1,014,145)	7%	✓
Expenses	430,388	0	29,001	3,330	32,331	1%	✗
Transfer / Overhead Allocation	2,083	0	0	0	0	0%	✓
Total Unit: Airport Commercial	***(14,644,111)***	***0***	***29,001***	***(1,010,815)***	***(981,814)***	**7%**	✓
Total Section: AIRPORT	***(0)***	***0***	***798,846***	***170,545***	***969,391***	**-25971794112959800%**	✗

10. Section Statistics

AIRPORT COMMERCIAL

Passenger Numbers

Domestic passenger numbers for July 2017 were: 52,834 compared to July 2016: 51,578.



Patient Travel Subsidy Scheme Car Park Waiver

During July 2017, 169 vehicles had $8,696.00 in car park fees waived. The total period of time these vehicles were in the Airport car parks was an average of 2.25 days stay per passenger.

AIRPORT OPERATIONS

Audit and Compliance

There are no outstanding audit or compliance matters to report.

Military Exercises

Australian, New Zealand and U.S. Defence forces commenced operations for Exercise Talisman Sabre 2017 out of Rockhampton Airport.

The Airport Operation Coordinator attended the final planning conference for the upcoming military Exercise Wallaby 2017.

General

Capricorn Helicopter Rescue Service continued construction of their new hangar facility on Canoona Road.

AIRPORT FACILITIES

Terminal Standby Power System

The new system is operational. During routine testing, a fault was identified in the initial set-up of the Automatic Transfer Switch; this has since been rectified resulting in a timeframe for loss of power of less than 30 seconds before the generators take the load. Reliability testing for the revised set-up is being planned. To further improve the reliability of the system it has been decided to investigate the introduction of a load shedding function to reduce the start-up load when changing over to the generators, this will also cater for situations when one generator fails to start. A detailed commissioning testing plan is being developed to ensure these changes will improve the overall reliability of the system.

The redundant generator has been removed and planning for removal of the in-ground fuel tank in progressing, which has a current target date of late August early September.

Terminal Concourse Toilets Refurbishment

The contractor to remove the existing entry doors to all four main Terminal toilets has been engaged and materials have been procured. On-site works are planned to commence early August, with a current target completion of early September.

Terminal Air Conditioning System

A consultant engineer is developing a strategy to manage the replacement of Terminal Air Conditioning Assets through the Capital Replacement program over the next ten years.

Replacement of Aeroworx Storage/Workshop/Office/Lunchroom Building (Lease Site BD)

Development Application is in the process of being developed.

FRW have installed the sewer connection infrastructure.

8.2 ROCKHAMPTON REGIONAL WASTE AND RECYCLING MONTHLY OPERATIONS REPORT

File No:	**7927**
Attachments:	**1. Rockhampton Regional Waste and Recycling Operational Report July 2017**
Authorising Officer:	**Peter Kofod - General Manager Regional Services**
Author:	**Craig Dunglison - Manager RRWR**

SUMMARY

The purpose of this report is to provide an overview of Rockhampton Regional Waste and Recycling (RRWR) Operations for the month of July 2017.

OFFICER'S RECOMMENDATION

THAT the RRWR Operations Report for the period July 2017 be received.

ROCKHAMPTON REGIONAL WASTE AND RECYCLING MONTHLY OPERATIONS REPORT

Rockhampton Regional Waste and Recycling Operational Report July 2017

Meeting Date: 15 August 2017

Attachment No: 1

Monthly Operations Report

Rockhampton Regional Waste and Recycling

July 2017

1. Highlights

River Festival 14-16 July

Rockhampton Regional Waste and Recycling (RRWR) involvement in the 2017 River Festival was the supply of a waste and recycling collection and removal service.

A new approach was trialled at this event with the provision of 10 – 1000L industrial bins throughout the site during the set up period by the stalls at the site. The bins were removed prior to the official opening of the event. These bins were provided to capture the cardboard and other recyclables generated by the stall owners as they set up their stalls. This process captured an estimated 40 cubic meters of cardboard.

Through the event there were 40 waste and 40 recycling - 240L wheelie bins positioned throughout the site with another 40 bins positioned in three bin corrals positioned at either end and the middle of the site; but off the site. In association with the event management, persons were charged with the regular inspection of the bins on the site. If a full bin was noticed it would be removed to the closest corral and an empty bin returned to its original position on the site.

RRWR waste collection vehicles and staff serviced the corrals 3 times a day.

The recycling bins were all heavily contaminated and were all disposed of to landfill. More effort will have to be put into the promotion of the recycling aspect of the waste service, prior to and during the event. Also some bins were overfull at times and this will be worked upon with the event management for next year.

Department of Environment Heritage Protection (EHP) – Compliance Inspection Lakes Creek Road Landfill – 5 July

Department of Environment and Heritage Protection is now conducting regular pre-notified inspections of Council's waste facilities with Lakes Creek Road Landfill.

The EHP officers conducting the inspection were extremely satisfied with the condition of the facility; stating that "the site was a tidy, well run site."

The Coordinator Waste Services, and his staff have worked hard to improve and maintain the standard of the site and I would like to compliment them on their efforts.

Rocky Swap – 5 August

RRWR is working with the event organisers to provide the waste management services for the event. RRWR provided this service to last year's event and will follow a similar process this year. As at the River Festival though, 20 – 1000L bins will be provided to the site prior to the event's commencement for the stall owners to place recyclable products like cardboard into.

At the event there will be 203 waste and 57 recycling 240L bins provided. The recycling bins are centred on the food outlets only as this was found to be the area where most recyclables are generated. RRWR will have a stall at the event to promote recycling. Officers will also walk around the site through the day offering small gifts to persons correctly utilising the recycling bins. Councillors are invited to visit the stall if they attend the event.

As last year, an audit of the recycling bins will be undertaken to determine the type and level of contaminants so they can be targeted next year.

2. Innovations, Improvements and Variations

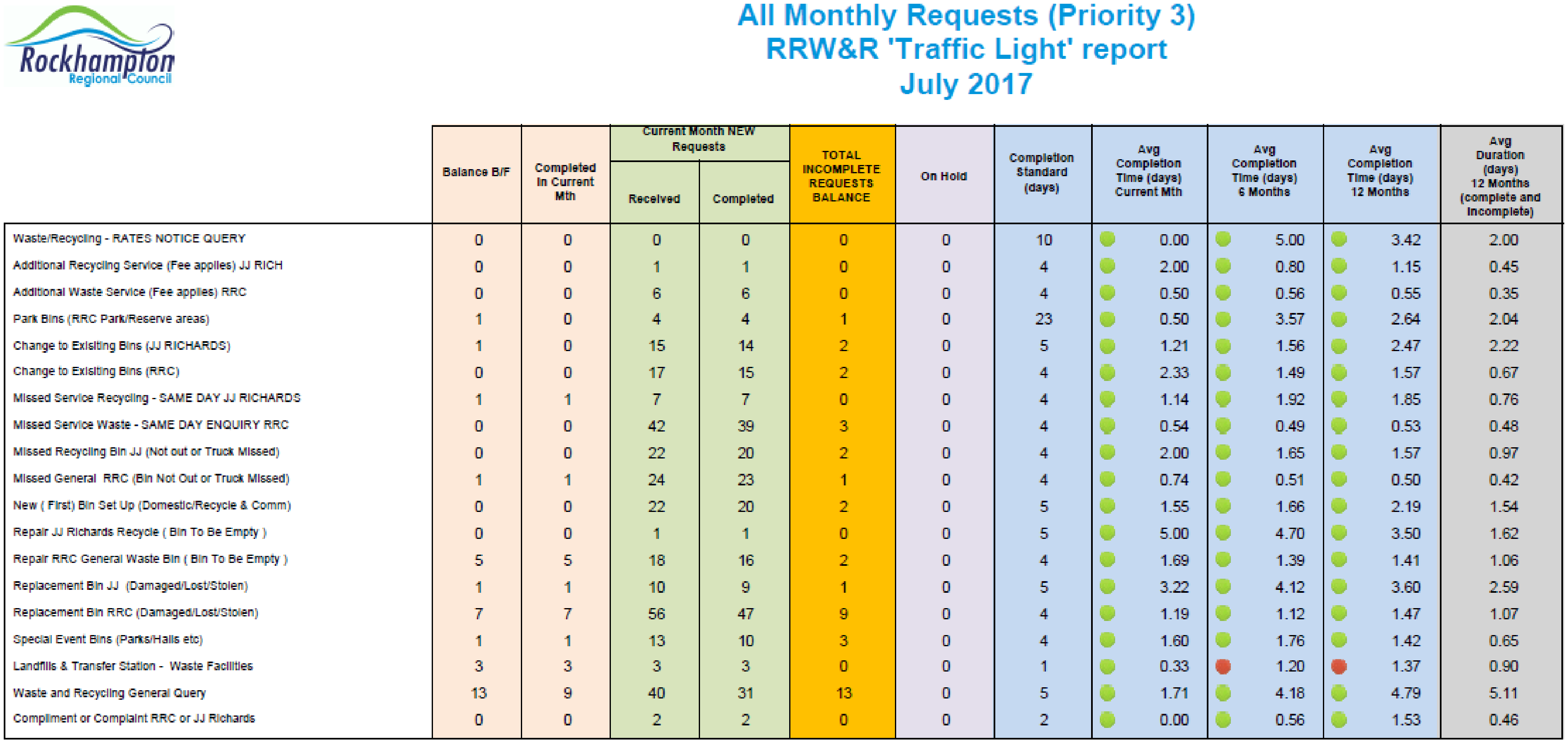
Lakes Creek Road – Waste Transfer Station, Mattress Stripping / Recycling Trial
RRWR are currently performing trials with Trendy Trash to test the ease and viability to strip inner spring mattresses for the purpose of recycling the inner spring as scrap metal and reducing the volume of waste disposed at landfill.

Should the trial prove to be successful, RRWR intend to commence the stripping / recycling of mattresses as soon as possible.

Lakes Creek Road – Waste Transfer Station, Manual Wheelie Bin Lifter
RRWR have just taken possession of a manually operated wheelie bin lifter. This wheelie bin lifter will be located within the transfer station to assist residents to empty the contents of any wheelie bins safely into the transfer station pit. Training of staff will be undertaken in the coming days.

3. Customer Service Requests

Response times for completing customer requests in this reporting period for July are within the set timeframes.



Rockhampton Regional Council

All Monthly Requests (Priority 3) RRW&R 'Traffic Light' report July 2017

	Balance B/F	Completed in Current Mth	Current Month NEW Requests		TOTAL INCOMPLETE REQUESTS BALANCE	On Hold	Completion Standard (days)	Avg Completion Time (days) Current Mth	Avg Completion Time (days) 6 Months	Avg Completion Time (days) 12 Months	Avg Duration (days) 12 Months (complete and incomplete)
			Received	Completed							
Waste/Recycling - RATES NOTICE QUERY	0	0	0	0	0	0	10	🟢 0.00	🟢 5.00	🟢 3.42	2.00
Additional Recycling Service (Fee applies) JJ RICH	0	0	1	1	0	0	4	🟢 2.00	🟢 0.80	🟢 1.15	0.45
Additional Waste Service (Fee applies) RRC	0	0	6	6	0	0	4	🟢 0.50	🟢 0.56	🟢 0.55	0.35
Park Bins (RRC Park/Reserve areas)	1	0	4	4	1	0	23	🟢 0.50	🟢 3.57	🟢 2.64	2.04
Change to Existing Bins (JJ RICHARDS)	1	0	15	14	2	0	5	🟢 1.21	🟢 1.56	🟢 2.47	2.22
Change to Existing Bins (RRC)	0	0	17	15	2	0	4	🟢 2.33	🟢 1.49	🟢 1.57	0.67
Missed Service Recycling - SAME DAY JJ RICHARDS	1	1	7	7	0	0	4	🟢 1.14	🟢 1.92	🟢 1.85	0.76
Missed Service Waste - SAME DAY ENQUIRY RRC	0	0	42	39	3	0	4	🟢 0.54	🟢 0.49	🟢 0.53	0.48
Missed Recycling Bin JJ (Not out or Truck Missed)	0	0	22	20	2	0	4	🟢 2.00	🟢 1.65	🟢 1.57	0.97
Missed General RRC (Bin Not Out or Truck Missed)	1	1	24	23	1	0	4	🟢 0.74	🟢 0.51	🟢 0.50	0.42
New (First) Bin Set Up (Domestic/Recycle & Comm)	0	0	22	20	2	0	5	🟢 1.55	🟢 1.66	🟢 2.19	1.54
Repair JJ Richards Recycle (Bin To Be Empty)	0	0	1	1	0	0	5	🟢 5.00	🟢 4.70	🟢 3.50	1.62
Repair RRC General Waste Bin (Bin To Be Empty)	5	5	18	16	2	0	4	🟢 1.69	🟢 1.39	🟢 1.41	1.06
Replacement Bin JJ (Damaged/Lost/Stolen)	1	1	10	9	1	0	5	🟢 3.22	🟢 4.12	🟢 3.60	2.59
Replacement Bin RRC (Damaged/Lost/Stolen)	7	7	56	47	9	0	4	🟢 1.19	🟢 1.12	🟢 1.47	1.07
Special Event Bins (Parks/Halls etc)	1	1	13	10	3	0	4	🟢 1.60	🟢 1.76	🟢 1.42	0.65
Landfills & Transfer Station - Waste Facilities	3	3	3	3	0	0	1	🟢 0.33	🔴 1.20	🔴 1.37	0.90
Waste and Recycling General Query	13	9	40	31	13	0	5	🟢 1.71	🟢 4.18	🟢 4.79	5.11
Compliment or Complaint RRC or JJ Richards	0	0	2	2	0	0	2	🟢 0.00	🟢 0.56	🟢 1.53	0.46

4. Service Delivery

ADOPTED OPERATIONAL SERVICE DELIVERY STANDARD	Target	Current Performance
Weekly collection of domestic waste on same day every week	98%	99.98%
Weekly collection of commercial waste	95%	99.98%
Fortnightly Collection of domestic recyclable waste	98%	99.95%
Fortnightly Collection of commercial recyclable waste	98%	99.95%
Missed service collection provided within two working days from notification when notification is within one working day of scheduled collection	95%	93.68%
Collection services will be made available within four working days upon application by owner	98%	94.68%
Provision of assisted services within ten working days from application by owner	100%	95.68%
Repair or replacement of stolen, removed, damaged, vandalised mobile bins within four working days from notification	100%	96.68%

5. Legislative Compliance and Standards

Legislative timeframes

6. Operational Plan Targets by Section

The following Operational Plan actions and targets are required to be reported to Council on a monthly basis. This data will also form part of the Operational Plan quarterly report to Council:

Operational Plan Ref	Action	Target	Status
1.1.1.1	Operate, maintain and repair infrastructure as detailed in the annual maintenance program	Delivery of the annual operating budget to 95%	5.5% expended
1.1.1.2	Deliver the annual capital works program	Budget expenditure greater than 95%	2% expended
1.3.5.2	Develop a plan for the effective safe management of waste during a disaster	Plan developed by 31 December and adopted by Council by 30 June 2018	Development of plan has commenced.
3.1.6.1	Develop and deliver an effective educational program to the community promoting kerbside recycling and general resource conservation	Achieve targets in line with the Waste Reduction and Recycling Plan (WRRP)	Draft education has been developed.

7. Capital Projects

As at period ended July – 8.3% of year elapsed

Project	Planned Start Date	Planned End Date	Status	Budget Estimate	YTD actual (incl committals)
CAPITAL WORKS PROGRAM					
Approved FY17/18 Capital Budget					
Lakes Creek Road Landfill - Remediation	**01/07/17**	**30/06/18**	**0%**	**$844,778**	**$977**
Comment: Capping and remediation of LCR landfill is ongoing with majority of funding allocated to finalising Stage 1. Commenced with capping of legacy waste areas as well.					
LCRL Augmentation	**01/07/17**	**30/06/18**	**7%**	**$4,500,000**	**$338,370**
Comment: Consultants have finalised the concept design and RRWR are reviewing the documents. Consultant completed design of Cell A with the detail design drawings / technical specifications received by RRWR. Construction of cell A is expected to be complete in October 2018. Site possession and construction of Cell A is expected to commence early 2018.					
Capping and Closure of Stage 1 and 2 – Gracemere landfill	**01/07/17**	**30/06/18**	**0%**	**$200,000**	**$43,581**
Comment: Completion of stage 1 capping works and commencement stage 2 landfill capping as per approved Closure plan. Part of project to commence for WTF construction stage. Engaged consultant to finalise the capping design. The proposed design is to consider phytocapping.					
RRC Rubbish Bin Renewal Program	**1/7/17**	**30/6/18**	**0%**	**$140,000**	**$44,067**
Comment: Ongoing replacements					

8. Operational Projects

Project	Planned Start Date	Planned End Date	Status	Budget Estimate	YTD actual (incl committals)
Biomax Project	01/05/17	31/12/17	Initial investigation undertaken and report to Council. Detailed assessment is underway. Budget for project being developed	Being Prepared	$0

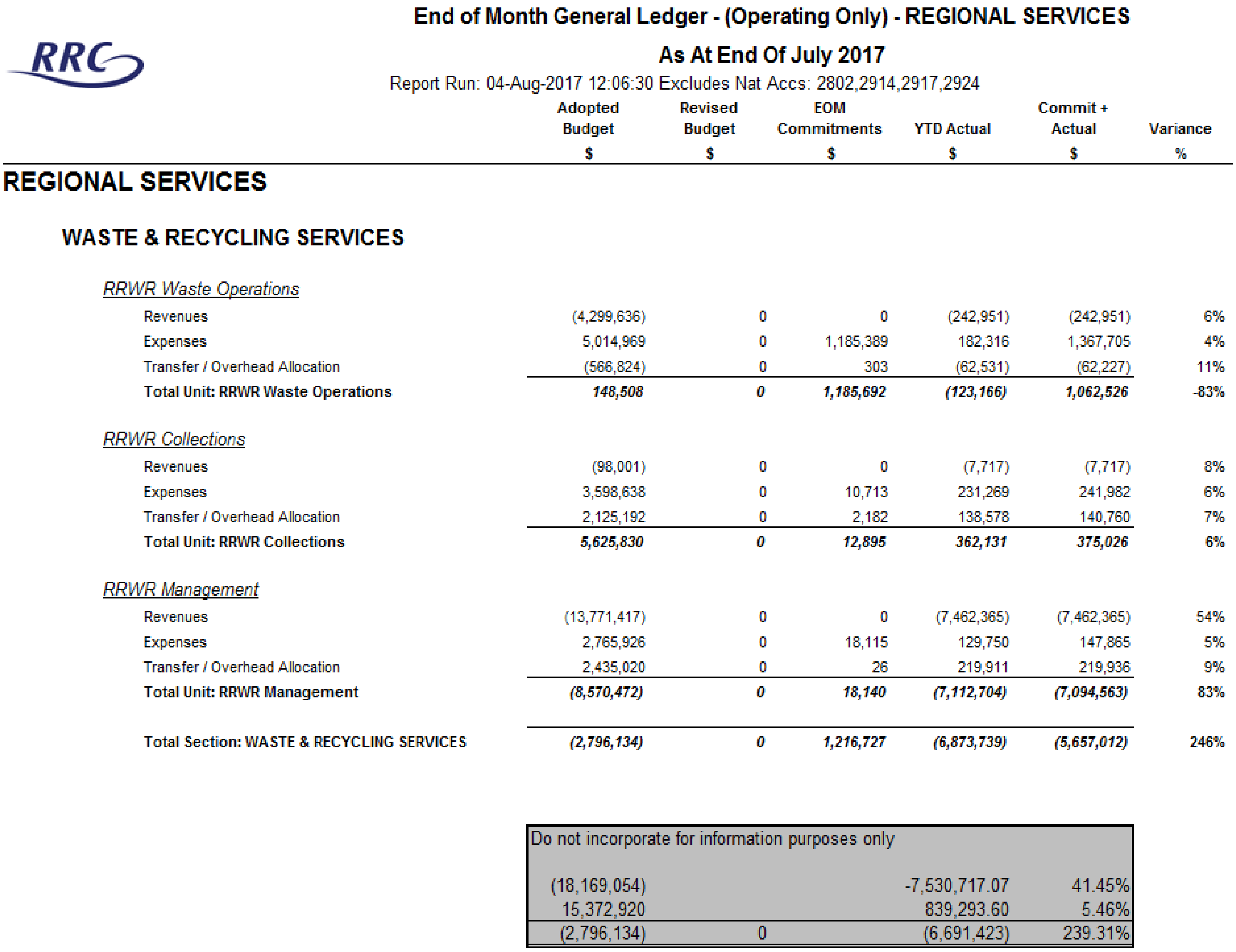
9. Budget

Operational Summary

Total revenue is significantly above the percentage of year elapsed at 41.45% due to the first half of the years rating cycle now having been issued. Expenditure is lower than the percentage of year elapsed at 5.46% resulting in an overall surplus position.

Capital Summary

RRWR capital project expenditure is significantly below the percentage of year elapsed at 2% of budget. The majority of RRWR's capital expenditure to date relates to the, LCR capping project and LCR carpark upgrade front office area. It's anticipated that expenditure will be brought closer to budget as the year progresses.



End of Month General Ledger - (Operating Only) - REGIONAL SERVICES

As At End Of July 2017

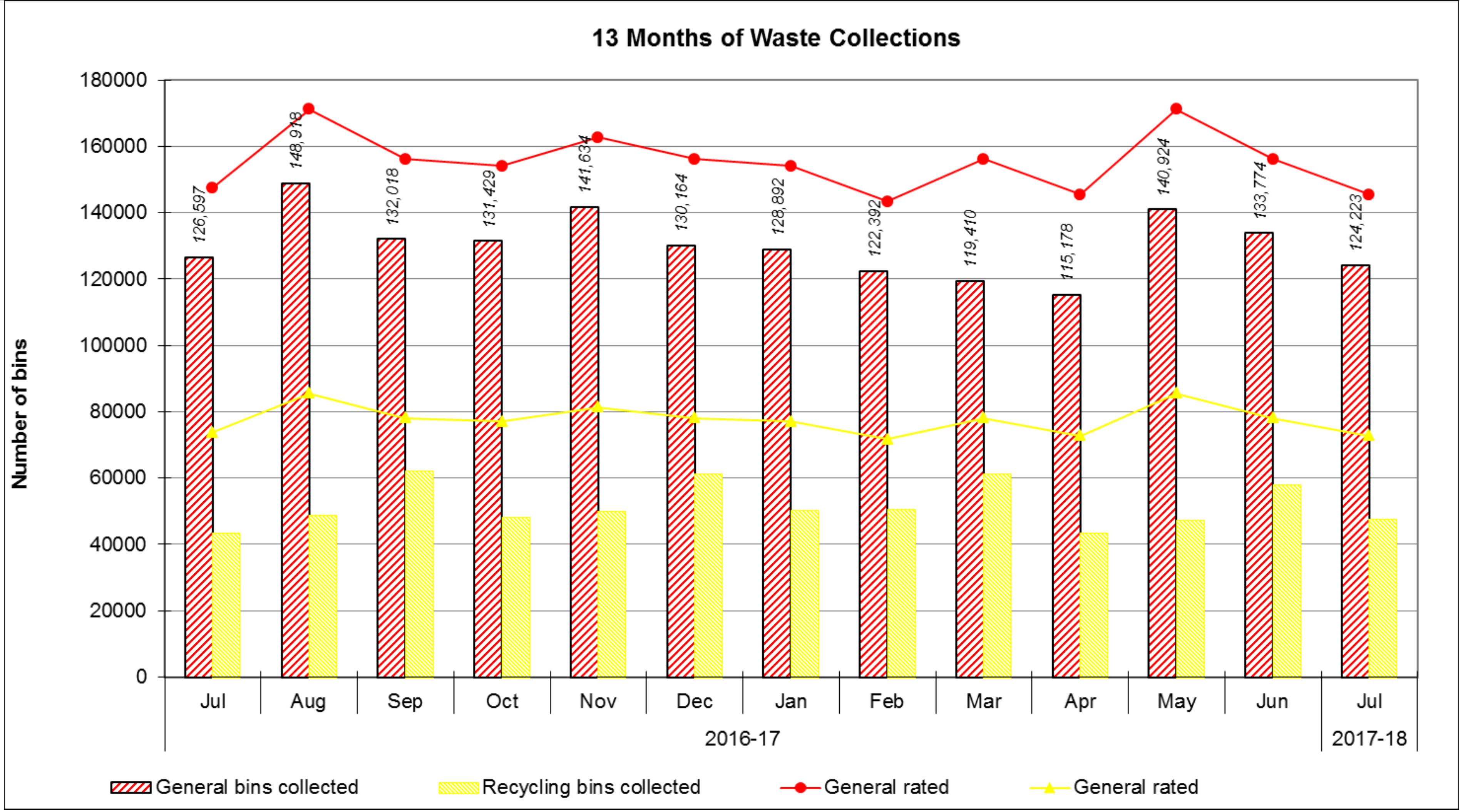
Report Run: 04-Aug-2017 12:06:30 Excludes Nat Accs: 2802,2914,2917,2924

	Adopted Budget	Revised Budget	EOM Commitments	YTD Actual	Commit + Actual	Variance
	$	$	$	$	$	%
REGIONAL SERVICES						
WASTE & RECYCLING SERVICES						
RRWR Waste Operations						
Revenues	(4,299,636)	0	0	(242,951)	(242,951)	6%
Expenses	5,014,969	0	1,185,389	182,316	1,367,705	4%
Transfer / Overhead Allocation	(566,824)	0	303	(62,531)	(62,227)	11%
Total Unit: RRWR Waste Operations	***148,508***	***0***	***1,185,692***	***(123,166)***	***1,062,526***	**-83%**
RRWR Collections						
Revenues	(98,001)	0	0	(7,717)	(7,717)	8%
Expenses	3,598,638	0	10,713	231,269	241,982	6%
Transfer / Overhead Allocation	2,125,192	0	2,182	138,578	140,760	7%
Total Unit: RRWR Collections	***5,625,830***	***0***	***12,895***	***362,131***	***375,026***	**6%**
RRWR Management						
Revenues	(13,771,417)	0	0	(7,462,365)	(7,462,365)	54%
Expenses	2,765,926	0	18,115	129,750	147,865	5%
Transfer / Overhead Allocation	2,435,020	0	26	219,911	219,936	9%
Total Unit: RRWR Management	***(8,570,472)***	***0***	***18,140***	***(7,112,704)***	***(7,094,563)***	**83%**
Total Section: WASTE & RECYCLING SERVICES	***(2,796,134)***	***0***	***1,216,727***	***(6,873,739)***	***(5,657,012)***	**246%**

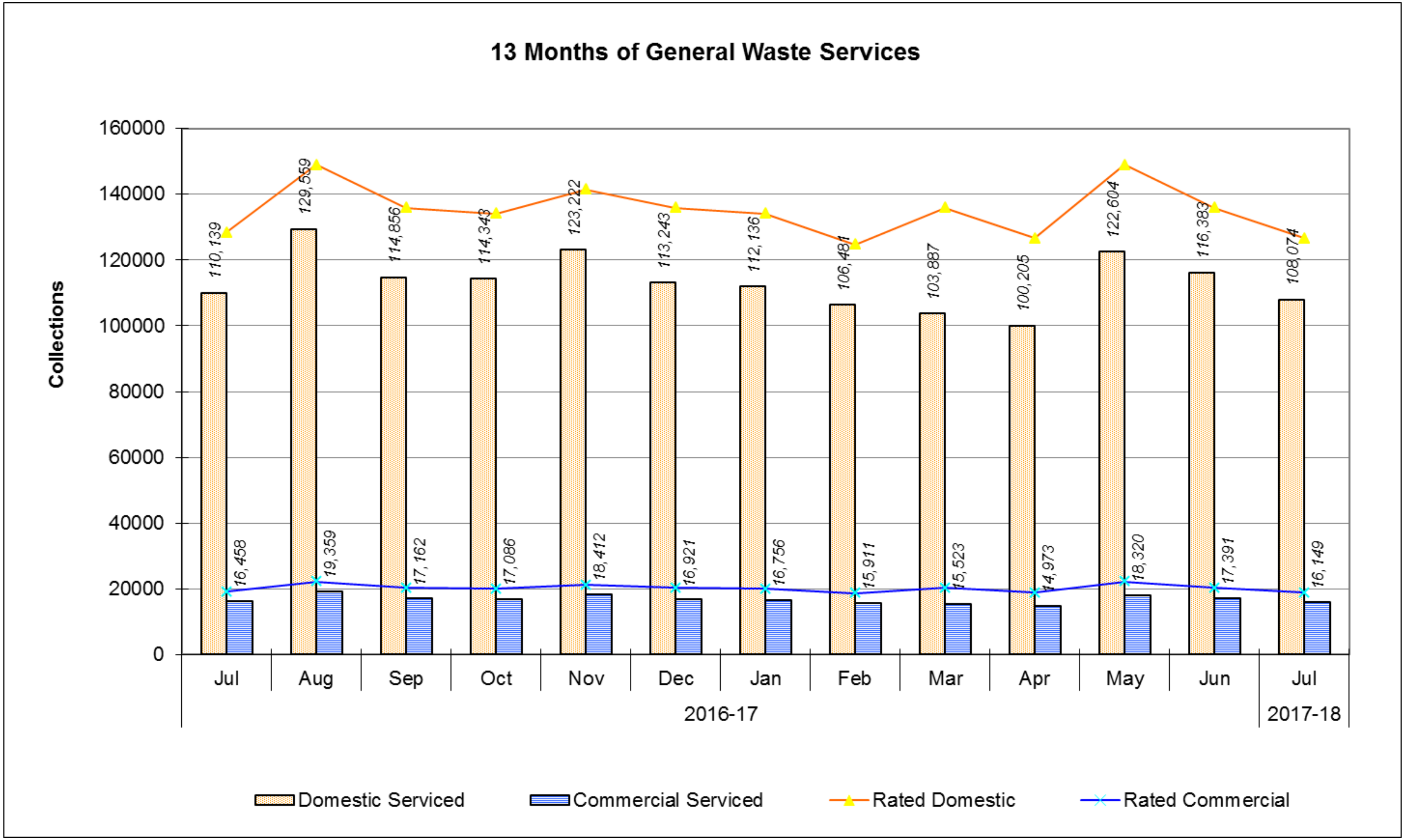
Do not incorporate for information purposes only

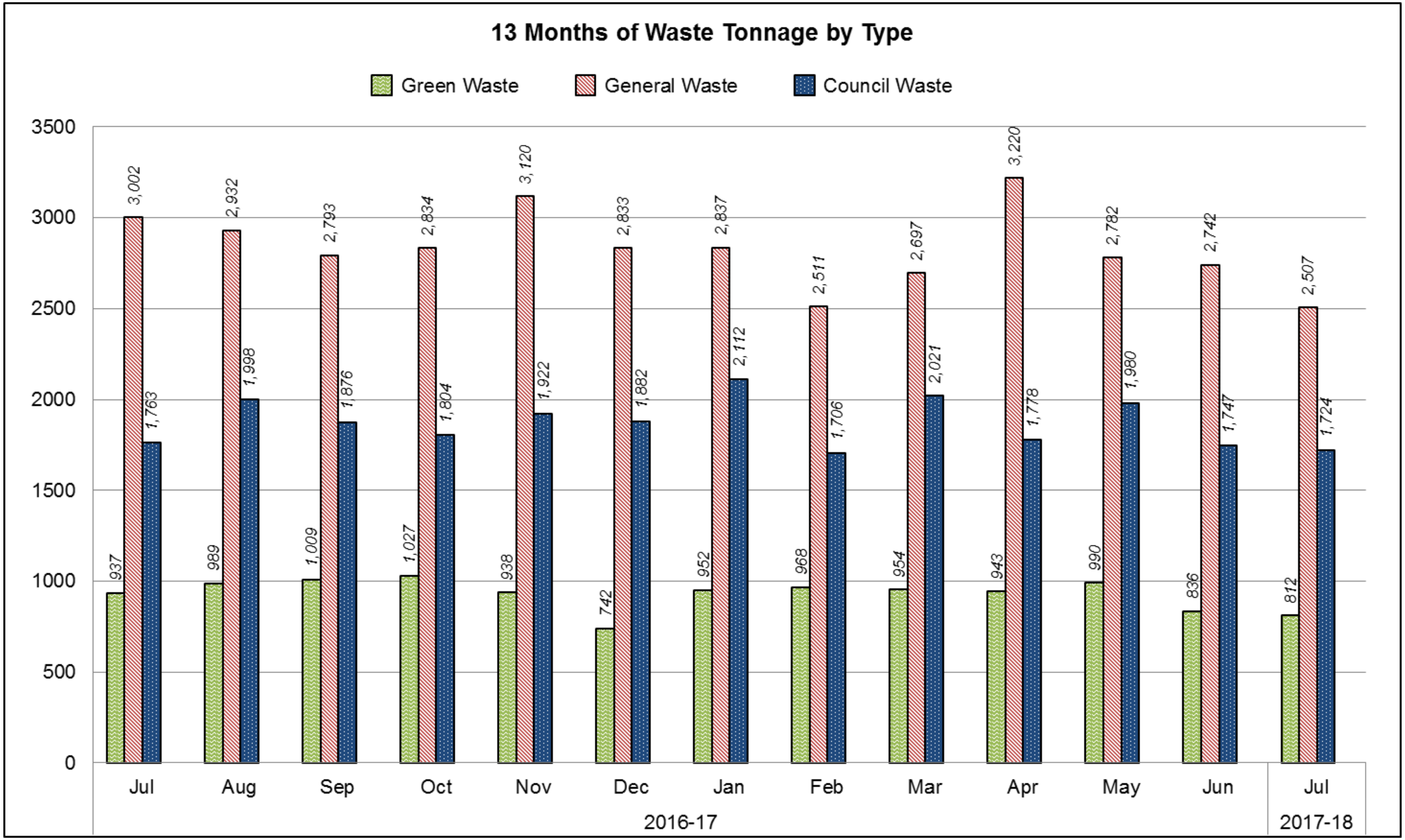
(18,169,054)			-7,530,717.07	41.45%
15,372,920			839,293.60	5.46%
(2,796,134)	0		(6,691,423)	239.31%

10. Section Statistics

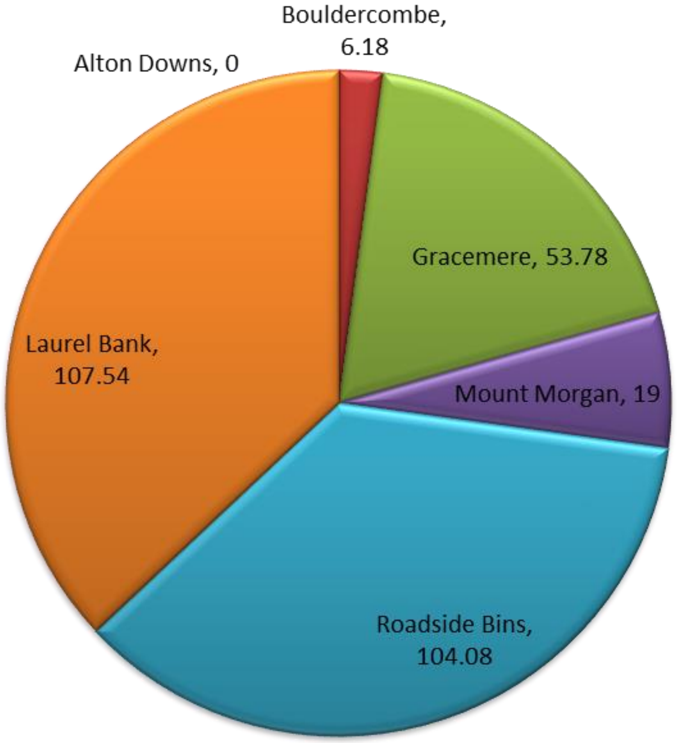


The above graph depicts the number of general waste and recycling bins serviced monthly over a 13 month period

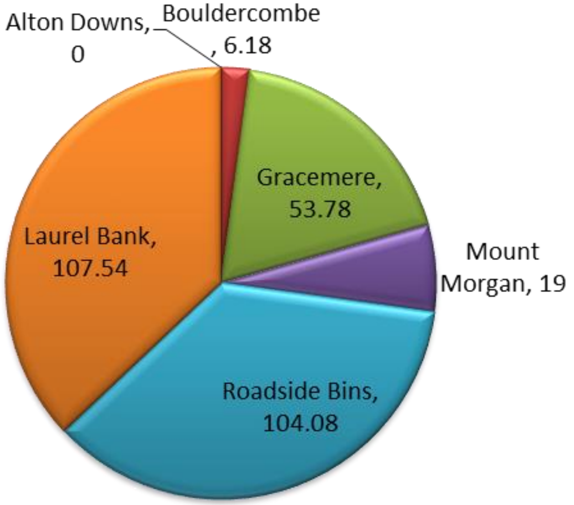

13 Months of General Waste Services
Collections
160000
140000
120000
100000
80000
60000
40000
20000
0
110,139
129,559
114,856
114,343
123,222
113,243
112,136
106,481
103,887
100,205
122,604
116,383
108,074
16,458
19,359
17,162
17,086
18,412
16,921
16,756
15,911
15,523
14,973
18,320
17,391
16,149
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
2016-17
2017-18
Domestic Serviced
Commercial Serviced
Rated Domestic
Rated Commercial

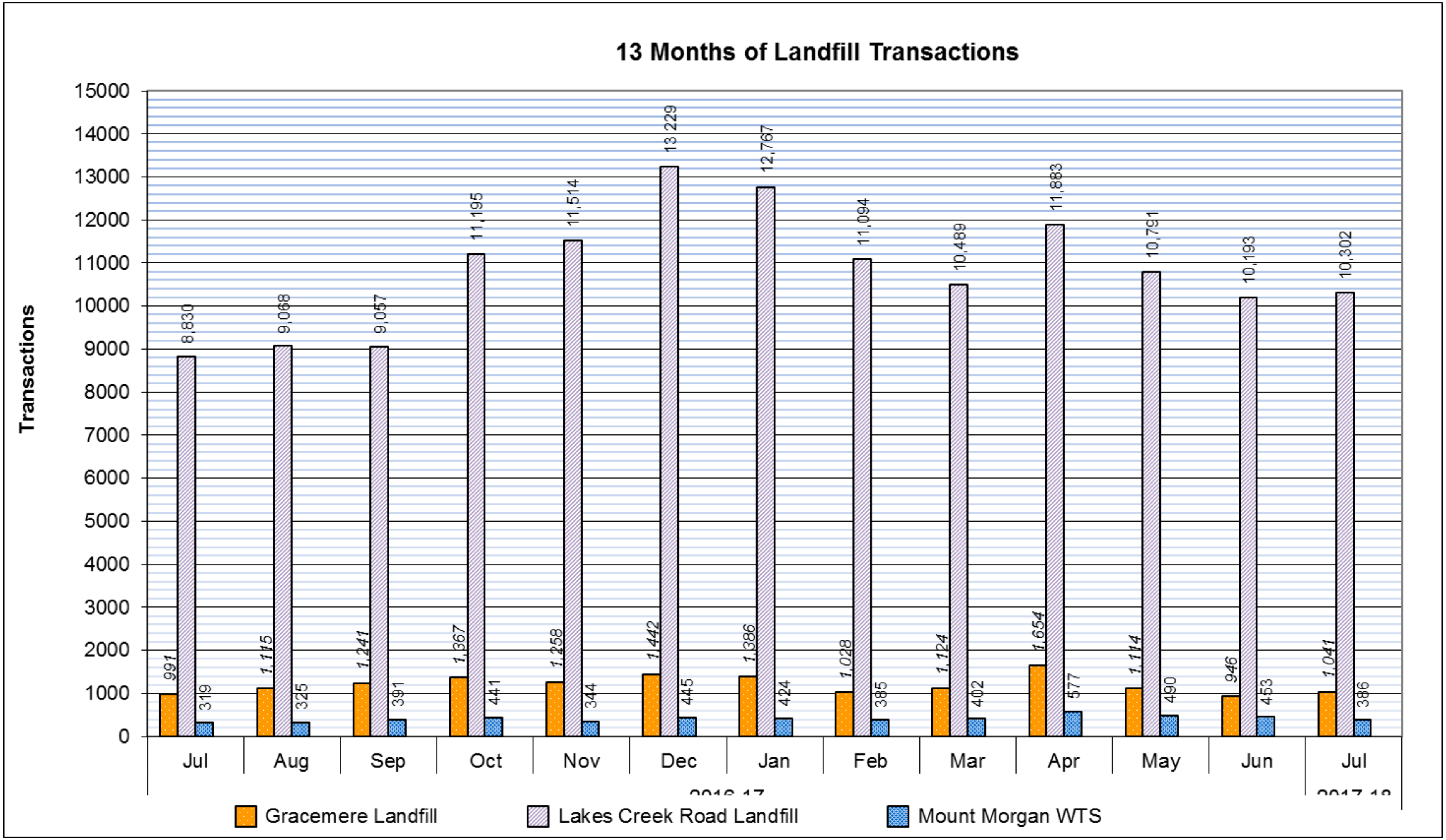

13 Months of Waste Tonnage by Type
Green Waste
General Waste
Council Waste
3500
3000
2500
2000
1500
1000
500
0
Jul 937 3,002 1,763
Aug 989 2,932 1,998
Sep 1,009 2,793 1,876
Oct 1,027 2,834 1,804
Nov 938 3,120 1,922
Dec 742 2,833 1,882
Jan 952 2,837 2,112
Feb 968 2,511 1,706
Mar 954 2,697 2,021
Apr 943 3,220 1,778
May 990 2,782 1,980
Jun 836 2,742 1,747
Jul 812 2,507 1,724
2016-17
2017-18

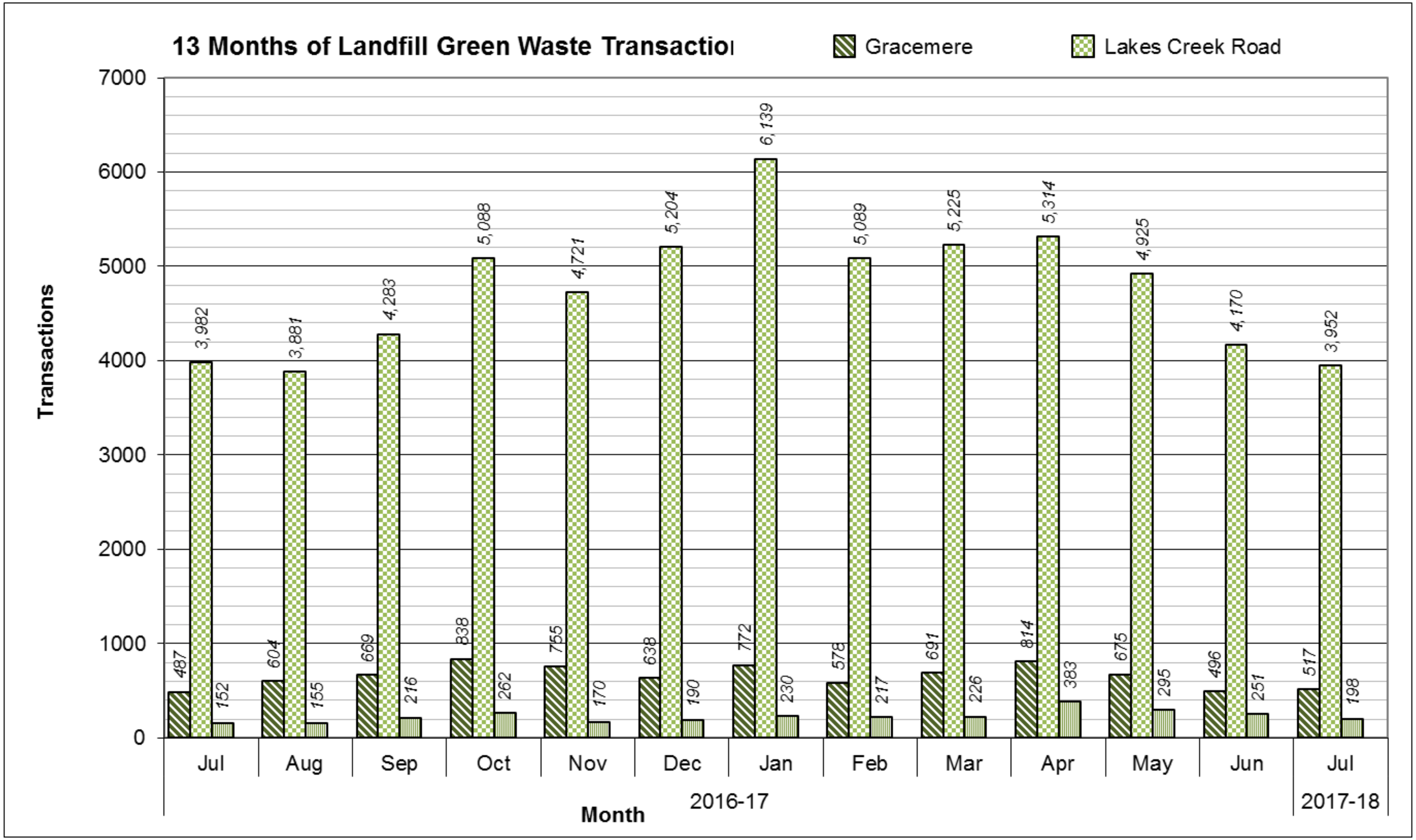
WASTE TRANSFER STATIONS
Tonnes Transferred to Landfill
July 2017



YTD 2017-18




13 Months of Landfill Transactions


13 Months of Landfill Green Waste Transactio
Gracemere
Lakes Creek Road
Transactions
7000
6000
5000
4000
3000
2000
1000
0
Jul 487 3,982 152
Aug 604 3,881 155
Sep 669 4,283 216
Oct 838 5,088 262
Nov 755 4,721 170
Dec 638 5,204 190
Jan 772 6,139 230
Feb 578 5,089 217
Mar 691 5,225 226
Apr 814 5,314 383
May 675 4,925 295
Jun 496 4,170 251
Jul 517 3,952 198
2016-17
2017-18
Month

8.3 FRW MONTHLY OPERATIONS REPORT - JULY 2017

File No:	**1466**
Attachments:	**1. FRW Monthly Operations Report - July 2017**
Authorising Officer:	**Peter Kofod - General Manager Regional Services**
Author:	**Jason Plumb - Manager Fitzroy River Water**

SUMMARY

This report details Fitzroy River Water's financial position and other operational matters for the Council's information as at 31 July 2017.

OFFICER'S RECOMMENDATION

THAT the FRW Monthly Operations Report for July 2017 be received.

FRW MONTHLY OPERATIONS REPORT - JULY 2017

FRW Monthly Operations Report - July 2017

Meeting Date: 15 August 2017

Attachment No: 1

Monthly Operations Report

Fitzroy River Water

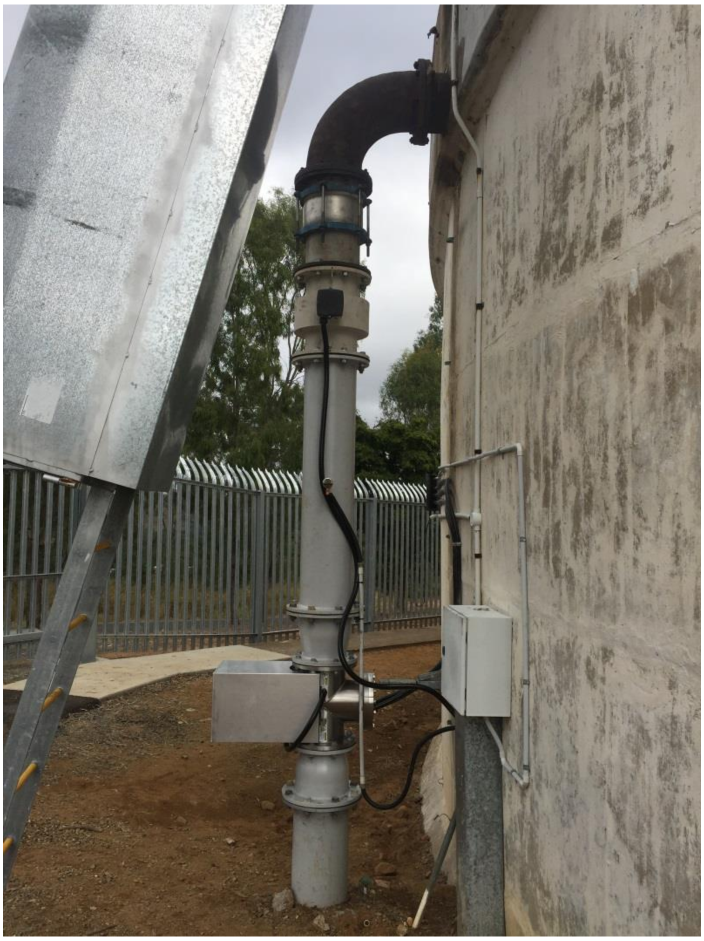
***July* 2017**

1. Highlights

The FRW Barrage Open Day was held on 29 July 2017 and was a great success! This event which is held only once every three years provides an opportunity for members of the community to take a brief tour on the top of the Barrage and also find out more about what FRW does for the community. The event this year was again very well supported by the community with more than 1200 people taking the Barrage tour and many others visiting the site to see the various displays and information stalls. FRW was well supported also by the range of other Council and non-Council organisations who gathered for the day to promote the Fitzroy River and its importance for the community both as a water resource and for its significant environmental value. Once again Fitz the bottom-breathing turtle made an appearance to the delight of all those present. The holding of the event in July helped to provide a slightly cooler day but also enabled members of the public to see directly the flow through one of the partially opened Barrage gates.

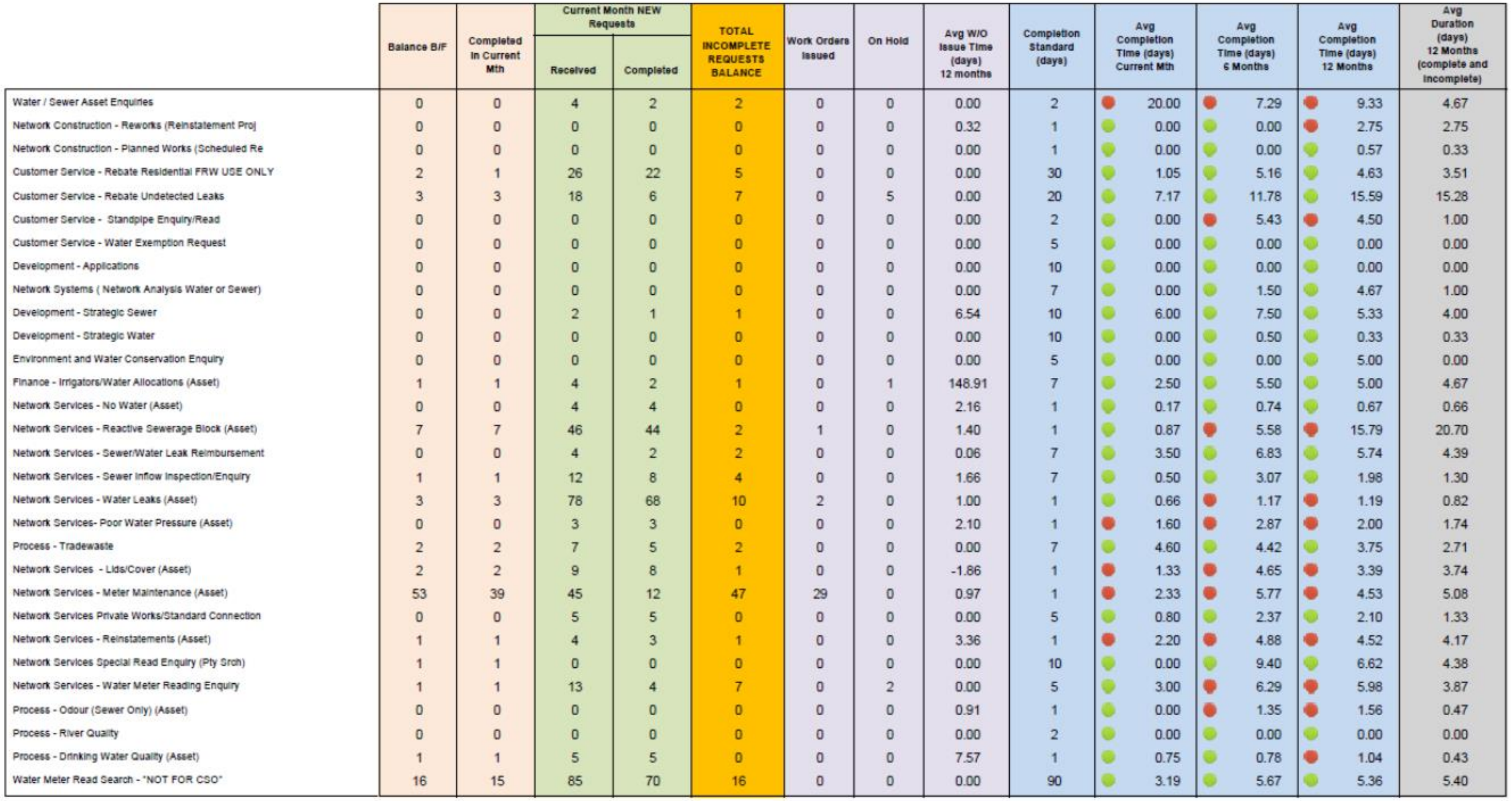
2. Innovations, Improvements and Variations

Recently, some improvements to the Mount Morgan WTP and STP have been completed with the installation of a new UV Disinfection system at the WTP and renewal of the old UV Disinfection system at the STP. These projects are important parts of delivering against Operational Plan Actions Reference No. 1.1.1.2, 1.1.1.4 and 1.1.1.5, and completion of these capital works providing significant improvements to the treatment process at each of these treatment plants. UV Disinfection is a very powerful and cost-effective means of ensuring that all potentially harmful disease causing microorganisms are destroyed. These improvements provide an increased level of confidence that the Mount Morgan WTP will consistently produce safe drinking water for the community, and that Mount Morgan STP will consistently produce recycled water that is safe for irrigation on sporting fields and public open spaces. These two projects were completed by a company called WestWater with a combined total project cost of approximately $110,000. The photo below shows the UV Disinfection system installed on the clear water reservoir inlet pipe at the Mount Morgan WTP.



3. Customer Service Requests

Response times for completing customer requests in this reporting period for July are below. FRW uses Pathway escalations to monitor service performance compliance to the Customer Service Standards.



	Balance B/F	Completed In Current Mth	Current Month NEW Requests		TOTAL INCOMPLETE REQUESTS BALANCE	Work Orders Issued	On Hold	Avg W/O Issue Time (days) 12 months	Completion Standard (days)	Avg Completion Time (days) Current Mth	Avg Completion Time (days) 6 Months	Avg Completion Time (days) 12 Months	Avg Duration (days) 12 Months (complete and incomplete)
			Received	Completed									
Water / Sewer Asset Enquiries	0	0	4	2	2	0	0	0.00	2	🔴 20.00	🔴 7.29	🔴 9.33	4.67
Network Construction - Reworks (Reinstatement Proj	0	0	0	0	0	0	0	0.32	1	🟢 0.00	🟢 0.00	🔴 2.75	2.75
Network Construction - Planned Works (Scheduled Re	0	0	0	0	0	0	0	0.00	1	🟢 0.00	🟢 0.00	🟢 0.57	0.33
Customer Service - Rebate Residential FRW USE ONLY	2	1	26	22	5	0	0	0.00	30	🟢 1.05	🟢 5.16	🟢 4.63	3.51
Customer Service - Rebate Undetected Leaks	3	3	18	6	7	0	5	0.00	20	🟢 7.17	🟢 11.78	🟢 15.59	15.28
Customer Service - Standpipe Enquiry/Read	0	0	0	0	0	0	0	0.00	2	🟢 0.00	🔴 5.43	🔴 4.50	1.00
Customer Service - Water Exemption Request	0	0	0	0	0	0	0	0.00	5	🟢 0.00	🟢 0.00	🟢 0.00	0.00
Development - Applications	0	0	0	0	0	0	0	0.00	10	🟢 0.00	🟢 0.00	🟢 0.00	0.00
Network Systems (Network Analysis Water or Sewer)	0	0	0	0	0	0	0	0.00	7	🟢 0.00	🟢 1.50	🟢 4.67	1.00
Development - Strategic Sewer	0	0	2	1	1	0	0	6.54	10	🟢 6.00	🟢 7.50	🟢 5.33	4.00
Development - Strategic Water	0	0	0	0	0	0	0	0.00	10	🟢 0.00	🟢 0.50	🟢 0.33	0.33
Environment and Water Conservation Enquiry	0	0	0	0	0	0	0	0.00	5	🟢 0.00	🟢 0.00	🟢 5.00	0.00
Finance - Irrigators/Water Allocations (Asset)	1	1	4	2	1	0	1	148.91	7	🟢 2.50	🟢 5.50	🟢 5.00	4.67
Network Services - No Water (Asset)	0	0	4	4	0	0	0	2.16	1	🟢 0.17	🟢 0.74	🟢 0.67	0.66
Network Services - Reactive Sewerage Block (Asset)	7	7	46	44	2	1	0	1.40	1	🟢 0.87	🔴 5.58	🔴 15.79	20.70
Network Services - Sewer/Water Leak Reimbursement	0	0	4	2	2	0	0	0.06	7	🟢 3.50	🟢 6.83	🟢 5.74	4.39
Network Services - Sewer Inflow Inspection/Enquiry	1	1	12	8	4	0	0	1.66	7	🟢 0.50	🟢 3.07	🟢 1.98	1.30
Network Services - Water Leaks (Asset)	3	3	78	68	10	2	0	1.00	1	🟢 0.66	🔴 1.17	🔴 1.19	0.82
Network Services- Poor Water Pressure (Asset)	0	0	3	3	0	0	0	2.10	1	🔴 1.60	🔴 2.87	🔴 2.00	1.74
Process - Tradewaste	2	2	7	5	2	0	0	0.00	7	🟢 4.60	🟢 4.42	🟢 3.75	2.71
Network Services - Lids/Cover (Asset)	2	2	9	8	1	0	0	-1.86	1	🔴 1.33	🔴 4.65	🔴 3.39	3.74
Network Services - Meter Maintenance (Asset)	53	39	45	12	47	29	0	0.97	1	🔴 2.33	🔴 5.77	🔴 4.53	5.08
Network Services Private Works/Standard Connection	0	0	5	5	0	0	0	0.00	5	🟢 0.80	🟢 2.37	🟢 2.10	1.33
Network Services - Reinstatements (Asset)	1	1	4	3	1	0	0	3.36	1	🔴 2.20	🔴 4.88	🔴 4.52	4.17
Network Services Special Read Enquiry (Pty Srch)	1	1	0	0	0	0	0	0.00	10	🟢 0.00	🟢 9.40	🟢 6.62	4.38
Network Services - Water Meter Reading Enquiry	1	1	13	4	7	0	2	0.00	5	🟢 3.00	🔴 6.29	🔴 5.98	3.87
Process - Odour (Sewer Only) (Asset)	0	0	0	0	0	0	0	0.91	1	🟢 0.00	🔴 1.35	🔴 1.56	0.47
Process - River Quality	0	0	0	0	0	0	0	0.00	2	🟢 0.00	🟢 0.00	🟢 0.00	0.00
Process - Drinking Water Quality (Asset)	1	1	5	5	0	0	0	7.57	1	🟢 0.75	🟢 0.78	🔴 1.04	0.43
Water Meter Read Search - "NOT FOR CSO"	16	15	85	70	16	0	0	0.00	90	🟢 3.19	🟢 5.67	🟢 5.36	5.40

4. Service Delivery

Service Delivery Standard	Target	Current Performance	Service Level Type (Operational or Adopted)
Drinking Water Samples Compliant with ADWG	>99%	100%	Adopted
Drinking water quality complaints	<5 per 1000 connections	0.16	Adopted
Total water and sewerage complaints	N/A	172	N/A
Glenmore WTP drinking water E.C Content	<500 µS/cm	430 µS/cm	Operational
Glenmore WTP drinking water sodium content	<50 mg/L	39 mg/L	Operational
Average daily water consumption – Rockhampton	N/A	43.1 ML	N/A
Average daily water consumption – Gracemere	N/A	5.0 ML	N/A
Average daily water consumption – Mount Morgan	N/A	0.95 ML	N/A
Average daily bulk supply to LSC	N/A	7.56 ML	N/A
Drinking water quality incidents	0	0	Adopted
Sewer odour complaints	<1 per 1000 connections	0	Adopted
Total service leaks and breaks	80	58	Adopted
Total water main breaks	15	5	Adopted
Total sewerage main breaks and chokes	32	7	Adopted
Total unplanned interruptions – water	N/A	19	N/A
Average response time for water incidents (burst and leaks)	N/A	105 min	N/A
Average response time for sewerage incidents (including main breaks and chokes)	N/A	56 min	N/A
Rockhampton regional sewer connection blockages	42	28	Adopted

5. Legislative Compliance and Standards (including Risk and Safety)

Safety Statistics

The safety statistics for the reporting period are:

	FIRST QUARTER 2017/18		
	July	**August**	**September**
Number of Lost Time Injuries	0		
Number of Days Lost Due to Injury	38		
Total Number of Incidents Reported	6		
Number of Incomplete Hazard Inspections	0		

Hazard inspections are being completed however FRW processing of any rectification actions can delay meeting the end of month cut-off date for HR reporting.

Treatment and Supply

- No lost time injuries for the month.
- No employees on long term lost time injuries.
- One incident reported for the month. An employee sustained a minor cut to their hand due to the sharp end of a cut cable tie.

Network Operations

- No lost time injuries for the month.
- One employee currently on a long term lost time injury.
- Five safety incidents were reported for the month.

Three of the above incidents involved asset damage, while two incidents involved incidents regarding underground services. Presence of unmarked underground services continues to be a significant risk during excavation.

Business and Project Services

- No lost time injuries for the month
- No employees on long term lost time injuries
- No incidents reported for the month.

Legislative timeframes

Item	Due Date	Compliant? (Yes/No)	Status
Annual Review of Mount Morgan No. 7 Dam Emergency Action Plan	30/09/2017	Yes	Review currently underway
DEWS Mandatory Annual Water Reporting	01/10/2017	Yes	Reporting currently being compiled

6. Operational Plan Targets by Section

The following Operational Plan actions and targets are required to be reported to Council on a monthly basis. This data will also form part of the Operational Plan quarterly report to Council:

Operational Plan Ref	Action	Target	Status
1.1.1.1	Operate, maintain and repair infrastructure as detailed in the annual maintenance programs	Delivery of the annual operating budget to 95%	On-track after July
1.1.1.2	Deliver the annual capital works program	Budget expenditure greater than 95%	Capital projects well underway
1.1.1.3	Ensure safe and reliable operation of raw water storages	Compliance with state legislation and national guidelines	All water storages compliant with normal operational and maintenance work ongoing.
1.1.1.4	Ensure safe and reliable treatment and supply of drinking water	Compliance with Customer Service Standards, state legislation and national guidelines	100% compliance with state legislation and national guidelines. Performance against Customer Service Standards reported quarterly.
1.1.1.5	Ensure safe and reliable transport and treatment of sewage	Compliance with Customer Service Standards, state legislation and national guidelines	>99% compliant with state legislation and national guidelines. Some minor exceedances reported for WRSTP. Performance against Customer Service Standards reported quarterly.
1.1.1.6	Ensure safe and reliable supply of non-potable water	Compliance with state legislation and national guidelines	100% compliance with state legislation and national guidelines.

Operational Plan Ref	Action	Target	Status
1.3.6.1	Ensure the safe and reliable operation of raw water storages	Compliance with legislative requirements for dam safety management	Annual updating of Mount Morgan No. 7 Dam Emergency Action Plan underway. Barrage Failure Impact Assessment underway.
2.2.3.1	Support programs that encourage residents to transition away from social support options	Consider options in budget planning to support employment programs in 2018/19	Continued focus on developing and managing projects that can be procured from and delivered by local contractors to boost local employment.
3.1.2.1	Promote water wise behaviours and practices	Achievement of annual marketing communications plan activities in accordance with agreed timeframes	FRW MarComms Plan currently being delivered with planning in advance of National Water Week.
3.1.2.1	Promote water wise behaviours and practices	Provide water rebates for residential water efficient products and process all rebate applications within 10 business days	Residential water efficient products rebates processed according to policy.
3.1.5.1	Minimise nutrient and sediment discharges to local waterways	Demonstrate compliance with Environmental Authority release limits and continuous improvement initiatives	Minor suspended solids exceedance at WRSTP. Capital upgrades for improved STP performance underway. Environmental Management Plans used to manage impacts of relevant construction activities.
3.2.1.1	Develop a renewable energy program for Fitzroy River Water	Program completed by 30 June 2018	Solar Farm opportunity being developed along with other program opportunities.
4.1.1.1	Provide timely and accurate responses to requests	In accordance with unit's customer service standards or adopted service levels	Performance against Customer Service Standards reported quarterly.
4.1.1.2	Provide effective delivery of Council services	In accordance with unit's customer service standards and service levels	All services delivered accordingly. See specific Operational Plan references above.
5.2.1.1	Comply with legislative requirements	Updates to be presented to Council in sectional monthly reports	See specific Operational Plan references above.

Operational Plan Ref	Action	Target	Status
5.2.1.4	Operational risks are monitored and managed in accordance with legislative requirements	Risk registers are presented to Council on a quarterly basis	Risk Register updated accordingly by FRW. New Risk Category and reporting format currently being developed.
5.2.1.8	Monitor and review non-compliance of legislative requirements	Report on legislative non-compliance included in sectional reports presented to Council on a monthly basis	See specific Operational Plan references above and the remainder of the report.
5.3.1.1	Workforce planning is reviewed to ensure that resourcing levels meet business needs in accordance with budget allocations	Review workforce requirements in accordance with budget schedule	Workforce requirements reviewed continuously and adjusted as required or following employee turnover.
5.3.2.1	Continually review operational expenditure	Identify at least one operational saving per section of responsibility	Operation and maintenance cost savings associated with electricity and chemical use constantly reviewed. Employee overtime monitored closely.
5.4.2.6	Pursue improved processes through all levels of Council	Identify at least two improved processes per section of responsibility	Review of preventative maintenance program underway. Review of water meter reading roster completed.

7. Capital Projects

As at period ended 31 July 2017 – 8.3% of year elapsed. Information is provided for projects for which significant progress has been made during this reporting period.

The following abbreviations have been used within the table below:

R	*Rockhampton*
G	*Gracemere*
M	*Mount Morgan*
WPS	*Water Pump Station*
SPS	*Sewage Pump Station*
STP	*Sewage Treatment Plant*
S	*Sewerage*
W	*Water*

Project	Planned Start Date	Planned End Date	Status	Budget Estimate	YTD actual (incl committals)
CAPITAL WORKS PROGRAM					
NETWORK OPERATIONS CAPITAL WORKS PROGRAM					
Rockhampton/Gracemere Water					
Yaamba Road Trunk Water Main Relocation Project 600mm water main replacement	February 2017	June 2018	15%	$7,655,007	$2,523,976
Comments: 600mm DICL main replacement project. Water main construction as part of Department of Transport and Main Roads RNAU Project. Stage 2 water main construction in progress with major scope/alignment changes to within the Norman Road corridor between Yeppoon Road and Olive Streets.					
Lion Creek Road (Morgan – Curtis) 150mm water main replacement	May 2017	July 2017	100%	$255,768	$211,855

Project	Planned Start Date	Planned End Date	Status	Budget Estimate	YTD actual (incl committals)
Comments: 100mm AC main replacement project.					
Main Street (Haynes – Bertram) 150mm water main replacement	July 2017	October 2017	5%	$225,060	$28,460
Comments: 150mm CI main replacement project.					
William Street (Alma – Canning) 200mm water main replacement	March 2017	December 2017	5%	$772,914	$261,149
Comments: 200mm CI main replacement project.					
Mount Morgan Water					
Byrnes Parade (Ganter – Possum) 150mm water main replacement	July 2017	October 2017	5%	$194,445	$13,389
Comments: 100mm AC main replacement project.					
Hall Street (Black – Hall Street WPS) 100mm water main replacement.	July 2017	July 2017	100%	$63,809	$64,511
Comments: 100mm AC main replacement project.					
Rockhampton/Gracemere Sewer					
West Rockhampton Sewage Catchment Diversion Project Jardine Park 300mm SRM construction	April 2017	June 2018	43%	$3,000,000	$1,347,851
Comments: Stage 2 construction in progress, preliminary design works for Stage 3 progressing.					

Project	Planned Start Date	Planned End Date	Status	Budget Estimate	YTD actual (incl committals)
Sewer rehabilitation program (including Building over Sewer)	July 2017	June 2018	8%	$408,000	$22,403
Comments: Rehabilitation and renewals annual program of works.					
Mount Morgan Sewer					
Railway Ave New 225mm Gravity Sewer Construction (Stages 2 & 3 incl. SPS)	July 2015	June 2018	75%	$4,200,000 (15/16 – 17/18) Including $1m BOR	$2,305,517
Comments: On Schedule. Significant increase in cost due to stabilised backfill requirements specified within TMR reserve. Scope of project increased to service additional properties. Construction of Stage 3 in progress, with some extensions to this stage being designed. Design work also progressing on both the SPS and SRM designs.					
TREATMENT AND SUPPLY CAPITAL WORKS PROGRAM					
Pipeline from West to South STP – Design Phase	July 2014	June 2019	40%	$2,900,000	$1,021,000
Comments: Stage 1 construction work now underway along Murray St. Stage 2 design works currently underway.					
GSTP Augmentation	July 2016	June 2019	40%	$543,644	$358,640
Comments: Stage 2. Mechanical dewatering contract awarded to contractor with design work underway and site works commencing.					
M W Dam No 7 CCTV Installation	July 2014	Sep 2017	50%	$30,000	$12,000
Comments: Procurement of CCTV and communications equipment underway and an agreement signed with Qld Government for access to a communications tower. Site works to commence in late August.					
M WTP CCTV Installation	July 2014	Sep 2017	50%	$15,000	$5,000
Comments: Procurement of CCTV and communications equipment underway and an agreement signed with Qld Government for access to a communications tower. Site works to commence in late August.					

Project	Planned Start Date	Planned End Date	Status	Budget Estimate	YTD actual (incl committals)
M W Dam No 7 Raw Lift Pump Upgrade	July 2016	July 2017	99%	$25,000	$6,500
Comments: Work to be finalized after commissioning of the new UV Disinfection system at the WTP in early August. This project has been delayed slightly due to the late completion of the UV disinfection project.					
R GWTP Chemical Oxidation dosing system	September 2016	July 2017	70%	$350,000	$316,263
Comments: Project well underway with equipment delivered from Germany after some supply and delivery delays. Installation to commence in mid-August following some minor delays due to design issues.					
M WTP UV Disinfection Installation	December 2016	July 2017	99%	$150,000	$77,222
Comments: Complete, with some minor defects being addressed.					
M STP UV Disinfection Renewal	December 2016	July 2017	100%	$25,000	$38,913
Comments: Complete.					
R – S NRSTP Aerator Replacement	July 2017	June 2018	30%	$50,000	$0
Comments: New works commencing to renew aerators No. 6 and No. 1, with this project part of a rolling renewal program.					
GWTP Highlift Pump Station Upgrade (Stage 2)	August 2014	August 2016	100%	$3,510,000	$3,260,898
Comments: Practical Completion issued in late August. Dispute over application of Liquidated Damages currently being discussed.					
MMWTP Coagulant Dosing Upgrade	January 2016	Sep 2017	70%	$70,000	$49,968
Comments: Project delayed slightly by heavy rainfall events causing changes to the raw water quality. Work to recommence again during a period of lower consumption as part of externally contracted work.					
R – North Rockhampton SPS No. 1 and 2 electrical upgrade	July 2016	July 2017	99%	$929,000	$938,052
Comments: All installation works complete with Practical Completion to be issued later this month.					

Project	Planned Start Date	Planned End Date	Status	Budget Estimate	YTD actual (incl committals)
R – NRSTP RAS pump renewal	July 2016	July 2017	100%	$25,000	$27,301
Comments: Complete					
R – SCADA Upgrade	July 2016	August 2017	80%	$250,000	$268,049
Comments: Project work well underway with site installation works to commence in May. Some slight delays to project progress following the completion of a cyber security risk assessment workshop. Some further delays experienced to incorporate the findings of the risk assessment.					
R – WPS Thozet Rd Generator Installation	October 2016	August 2017	60%	$300,000	$112,099
Comments: Generator now being delivered to FRW following a slight delay. Project delayed due to heavy rainfall and flood event. Installation to be completed as part of externally contracted works awarded in early August to local contractor.					
R – SRSTP Anoxic Mixers Renewal	December 2016	September 2017	70%	$40,000	$22,000
Comments: Project awarded to contractor with design work underway and equipment ordered. Awaiting delivery of equipment from overseas in late August.					
R – SRSTP New Inlet Screen	December 2016	September 2017	60%	$80,000	$55,281
Comments: Project awarded to contractor with design work underway and equipment ordered. Delivery expected in late August.					

8. Operational Projects

As at period ended July 2017 – 8.3% of year elapsed.

Project	Planned Start Date	Planned End Date	Status	Budget Estimate	YTD actual (incl committals)
Inflow and Infiltration Inspection Program	3 July 2017	30 September 2017	Inspection program well underway. Further information provided in the report.	$20,000	Not yet available

9. Budget

Operational

Revenue is currently 34.8% of the 2017/2018 Adopted Budget. Revenue streams are below target with the exception of utility charges due the advanced impact of water and sewerage access charges. No trends are evident at this early stage of the year.

Gross water consumption revenue is 23.7% of the adopted budget. One sector of Rockhampton has been billed. Average water consumption during July is higher than that for the same period last year. Gross water and sewerage access charges are on target. Bulk water sales are on below target due to timing of billing July consumption. No Private Works revenue has been recognised during July. Fees and charges are below target at 1.3%, attributed to the timing of trade waste and metered standpipe invoicing. Interest revenue is yet to be processed.

Expenditure year to date is 6.1% of the 2017/2018 Adopted Budget. Most expenditure streams are on target and as previously mentioned it is a little early to establish any trends. No units areas showing stress at this early stage.

No other material exceptions to be reported.

Capital

Capital expenditure is below the percentage of year elapsed at 4.1% in comparison to the 2017/2018 Adopted Budget. Expenditure during July has decreased compared to June by $1,982k. This is attributed to final end of year accruals being processed into June 2017 and finalisation of some contracted projects.

Water YTD 4.4% and Sewer YTD 3.9%.

Networks YTD 4.0% and Treatment YTD 4.4%.

The areas of prominent activity are the Yaamba Rd 600mm water main replacement, GWTP electrical and control renewal, Sewer pipeline from WRSTP to SRSTP, Sewer main refurbishment and Water Main Replacement programs.

There are no material exceptions to report.

Sundry Debtors

Below is a summary of aged sundry debtor balances at the end of July 2017. The 90+ day balances are either on payment plans, the business is in administration or the debt is with Collection House.

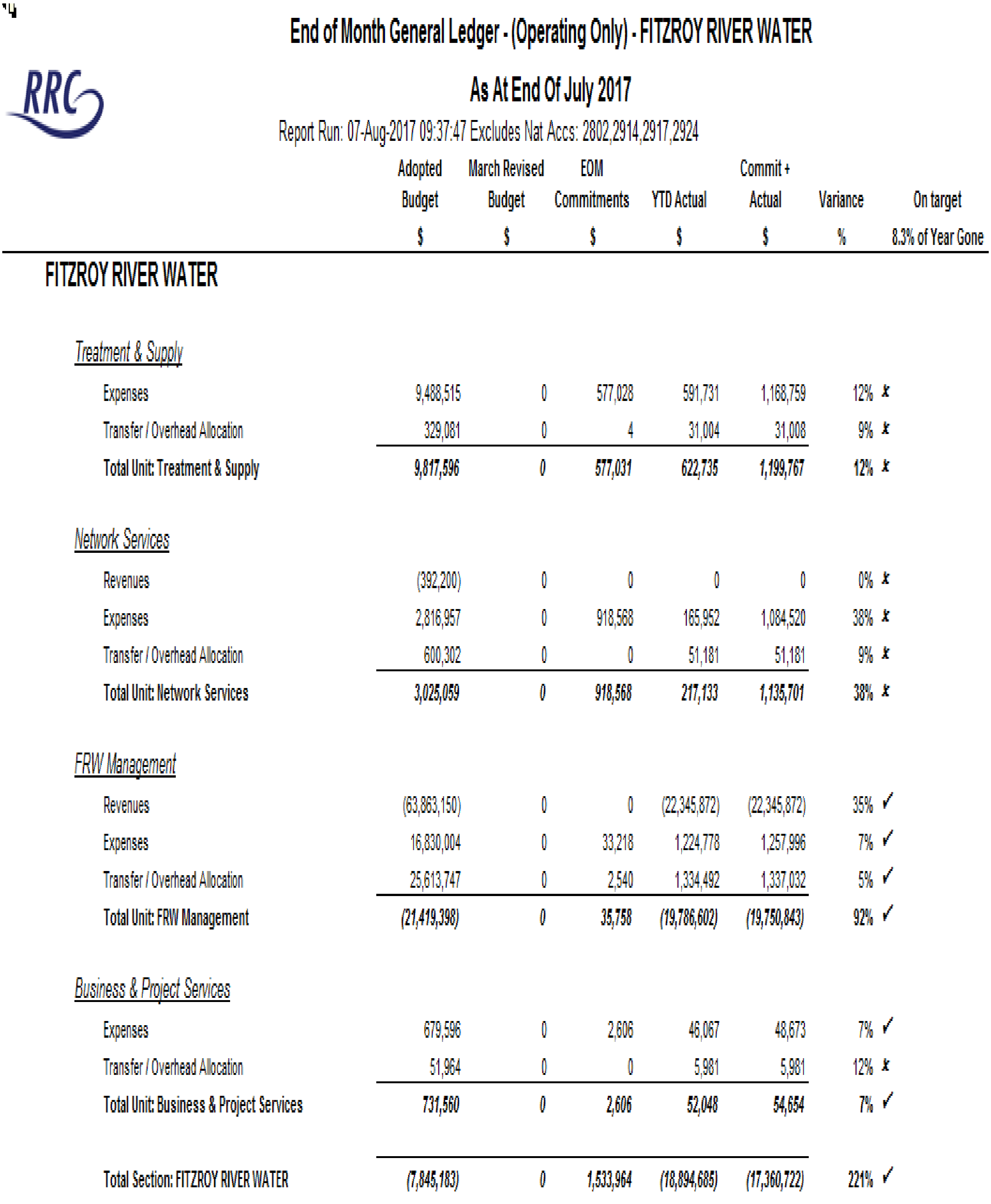
	Balance	0-30 Days	30-60 Days	60-90 Days	90+ Days
No. of Customers	86	50	14	10	40
Total Value	$420,083.73	$296,703.12	$2,482.38	$24,468.25	$96,429.98

Below is an explanation of the debtor types, being a mixture of standpipes, irrigators, emergency works and effluent usage.

90+ days	Comments
$82,407.58	Trade Waste
$8,315.45	Standpipes
$5,706.95	Irrigators
60-90 Days	**Comments**
$1,426.04	Standpipes (includes $717.06 from 3 debtors that have 90+ days)

$23,042.21	Trade Waste (includes $22,318.53 from 3 debtors that have 90+days)
30-60 Days	**Comments**
$2,482.38	Standpipes (includes $1,195.74 from 3 debtors that have 90+ days)

A summary of financial performance against budget is presented below:



End of Month General Ledger - (Operating Only) - FITZROY RIVER WATER

As At End Of July 2017

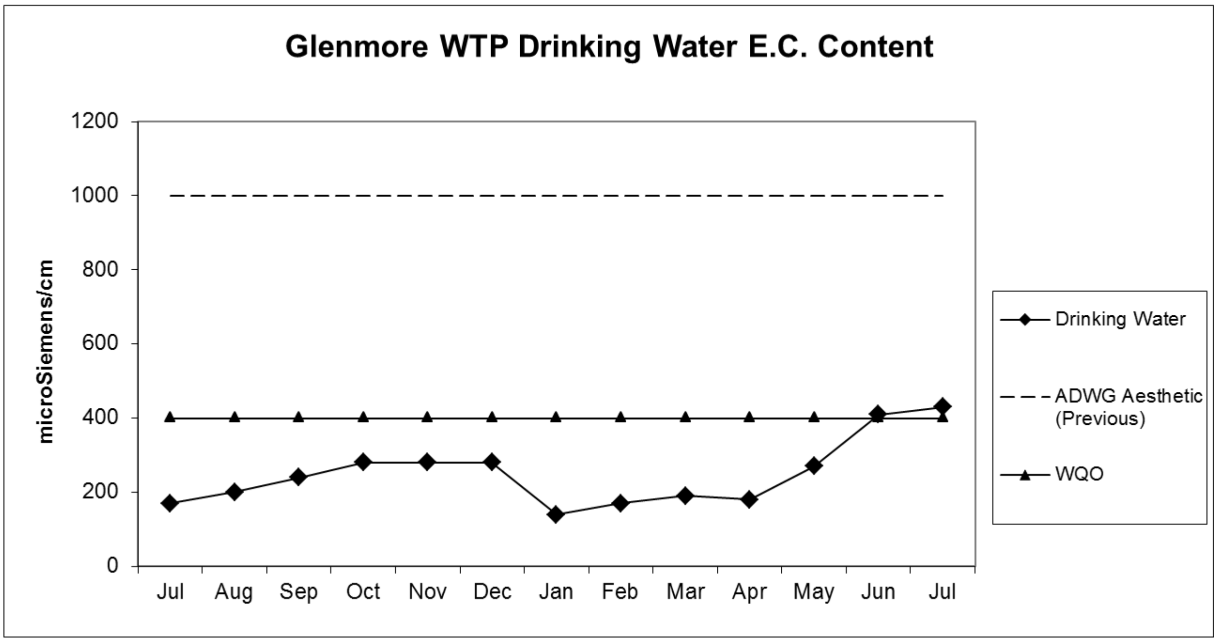
Report Run: 07-Aug-2017 09:37:47 Excludes Nat Accs: 2802,2914,2917,2924

	Adopted	March Revised	EOM		Commit +		
	Budget	Budget	Commitments	YTD Actual	Actual	Variance	On target
	$	$	$	$	$	%	8.3% of Year Gone
FITZROY RIVER WATER							
Treatment & Supply							
Expenses	9,488,515	0	577,028	591,731	1,168,759	12%	✗
Transfer / Overhead Allocation	329,081	0	4	31,004	31,008	9%	✗
Total Unit: Treatment & Supply	***9,817,596***	***0***	***577,031***	***622,735***	***1,199,767***	**12%**	✗
Network Services							
Revenues	(392,200)	0	0	0	0	0%	✗
Expenses	2,816,957	0	918,568	165,952	1,084,520	38%	✗
Transfer / Overhead Allocation	600,302	0	0	51,181	51,181	9%	✗
Total Unit: Network Services	***3,025,059***	***0***	***918,568***	***217,133***	***1,135,701***	**38%**	✗
FRW Management							
Revenues	(63,863,150)	0	0	(22,345,872)	(22,345,872)	35%	✓
Expenses	16,830,004	0	33,218	1,224,778	1,257,996	7%	✓
Transfer / Overhead Allocation	25,613,747	0	2,540	1,334,492	1,337,032	5%	✓
Total Unit: FRW Management	***(21,419,398)***	***0***	***35,758***	***(19,786,602)***	***(19,750,843)***	**92%**	✓
Business & Project Services							
Expenses	679,596	0	2,606	46,067	48,673	7%	✓
Transfer / Overhead Allocation	51,964	0	0	5,981	5,981	12%	✗
Total Unit: Business & Project Services	***731,560***	***0***	***2,606***	***52,048***	***54,654***	**7%**	✓
Total Section: FITZROY RIVER WATER	***(7,845,183)***	***0***	***1,533,964***	***(18,894,685)***	***(17,360,722)***	**221%**	✓

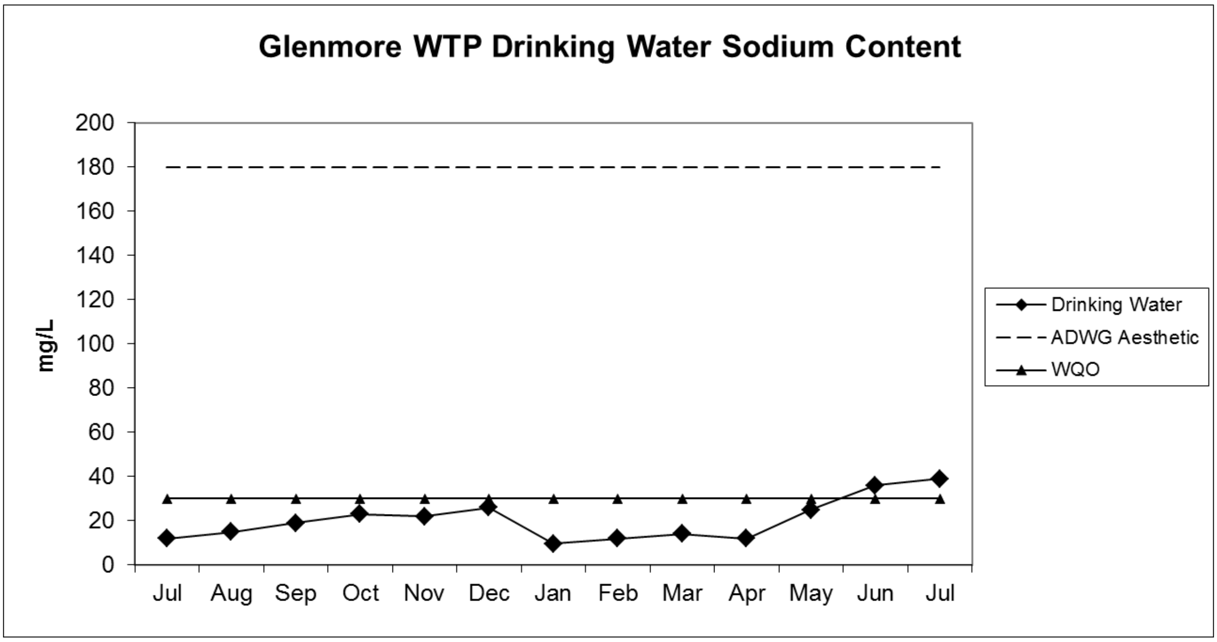
10. Section Statistics

TREATMENT AND SUPPLY

Drinking Water E.C. and Sodium Content



The level of E.C. in drinking water supplied from the Glenmore Water Treatment Plant (GWTP) during July increased slightly to be 430 µS/cm. The level of E.C. is slightly above the Water Quality Objective of 400 µS/cm but well beneath the previously used aesthetic guideline value of 1000 µS/cm. The E.C. reading is expected to remain relatively unchanged for the next few months.



The concentration of sodium in drinking water supplied from the GWTP during July increased slightly to be 39 mg/L. The current level of sodium is above the Water Quality Objective value of 30 mg/L but is well beneath the aesthetic guideline of 180 mg/L for sodium in the Australian Drinking Water Guidelines. The sodium concentration is expected to remain relatively unchanged for the next few months.

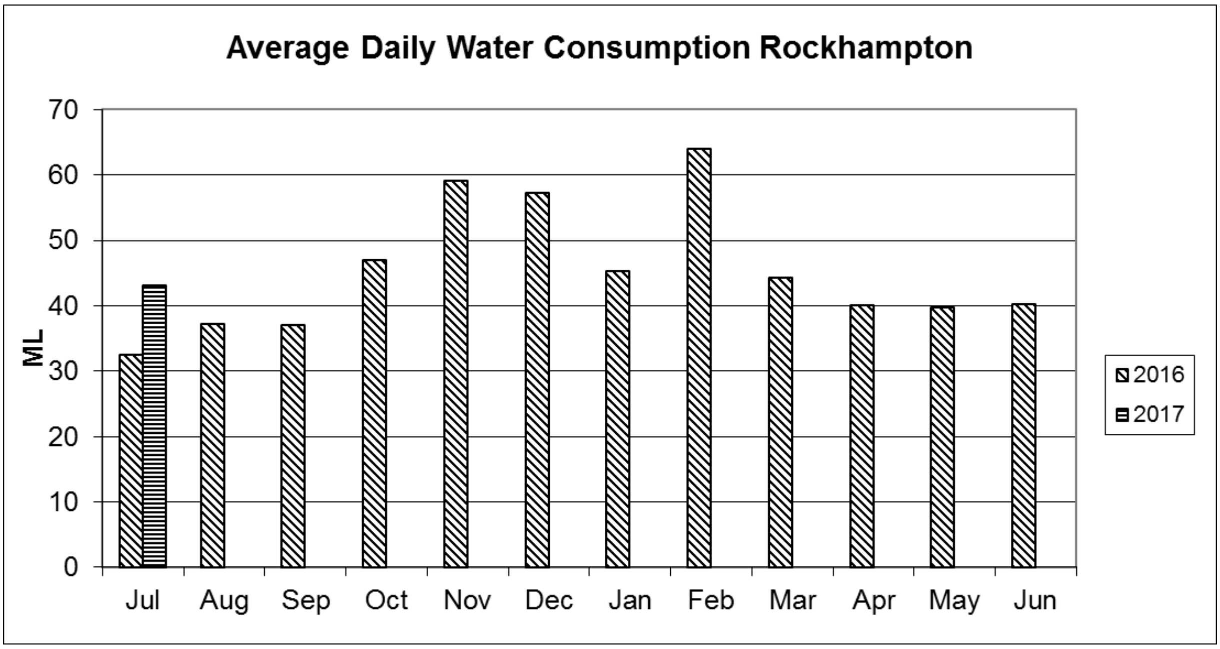
Drinking Water Quality as at 12 July 2017		
Parameter	Rockhampton	Mount Morgan
Total Dissolved Solids (mg/L)	240	190
Sodium (mg/L)	39	42
Electrical Conductivity (µS/cm)	430	280
Hardness (mg/L)	120	40
pH	7.73	7.61

The table above shows the results of drinking water testing in Rockhampton and Mount Morgan for selected water quality parameters.

Drinking Water Supplied

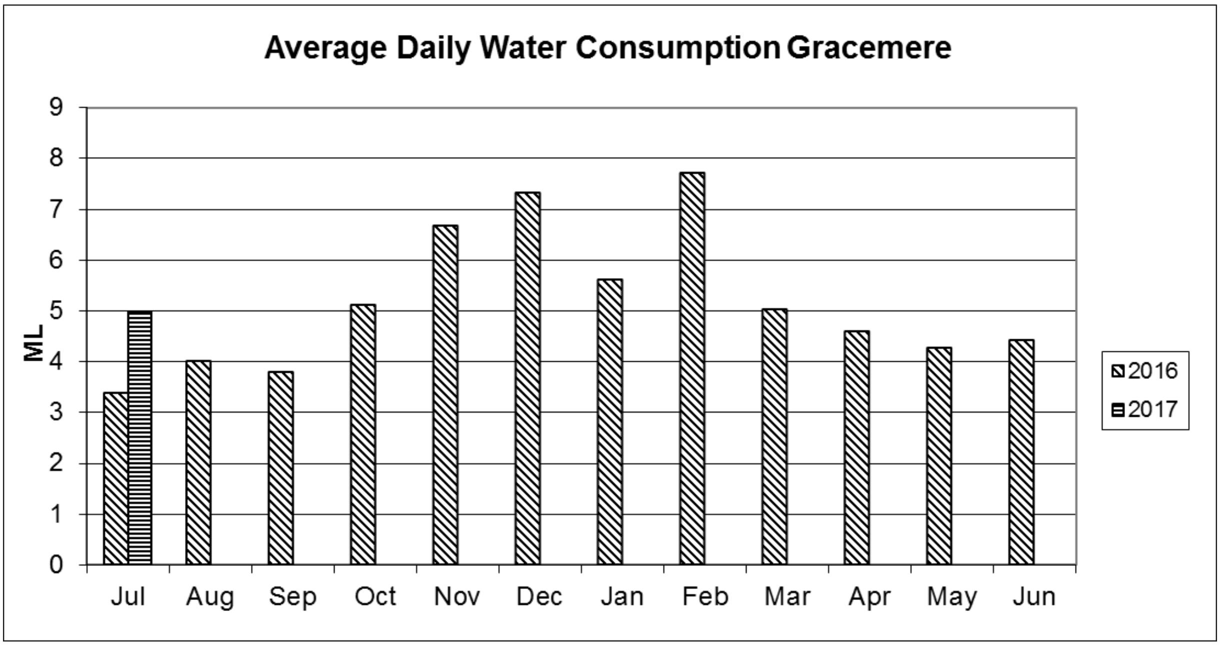
Data is presented in graphs for each water year (e.g. 2016 is the period from July 2016 to June 2017).

Rockhampton



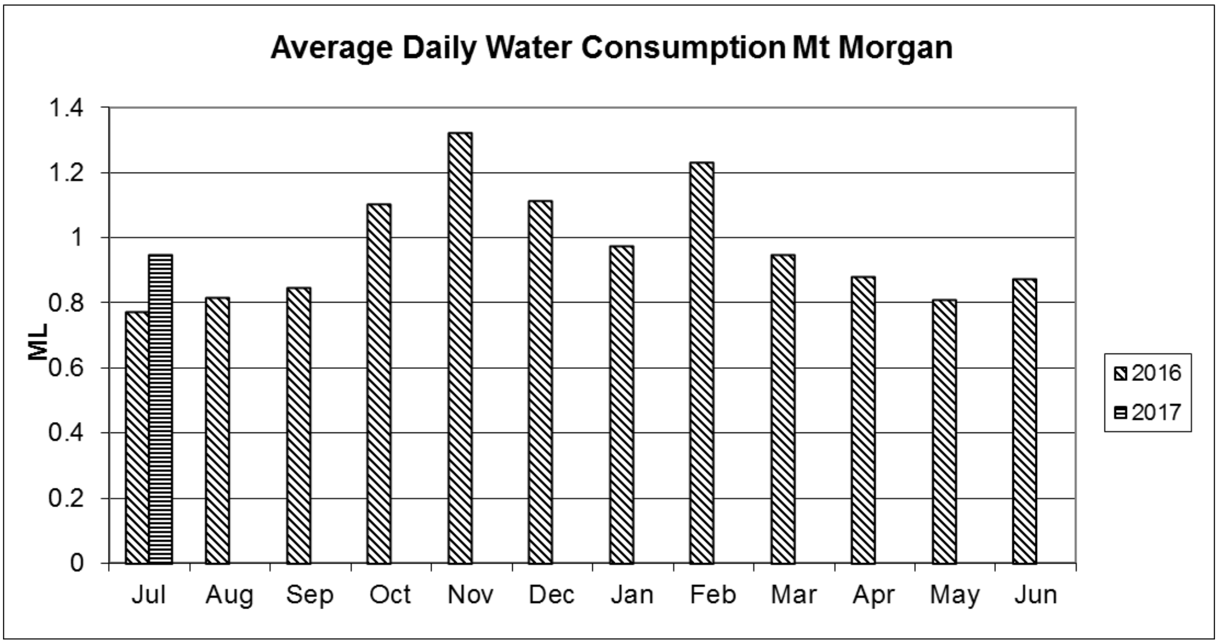
Average daily water consumption in Rockhampton during July (43.1 ML/d) increased slightly from that recorded in June and was much greater than that reported in the same period last year. The higher consumption was due to the relatively low rainfall during the month. The Fitzroy Barrage Storage is currently at 100% of accessible storage volume and is therefore well above the threshold in the Drought Management Plan used to trigger the implementation of water restrictions.

Gracemere



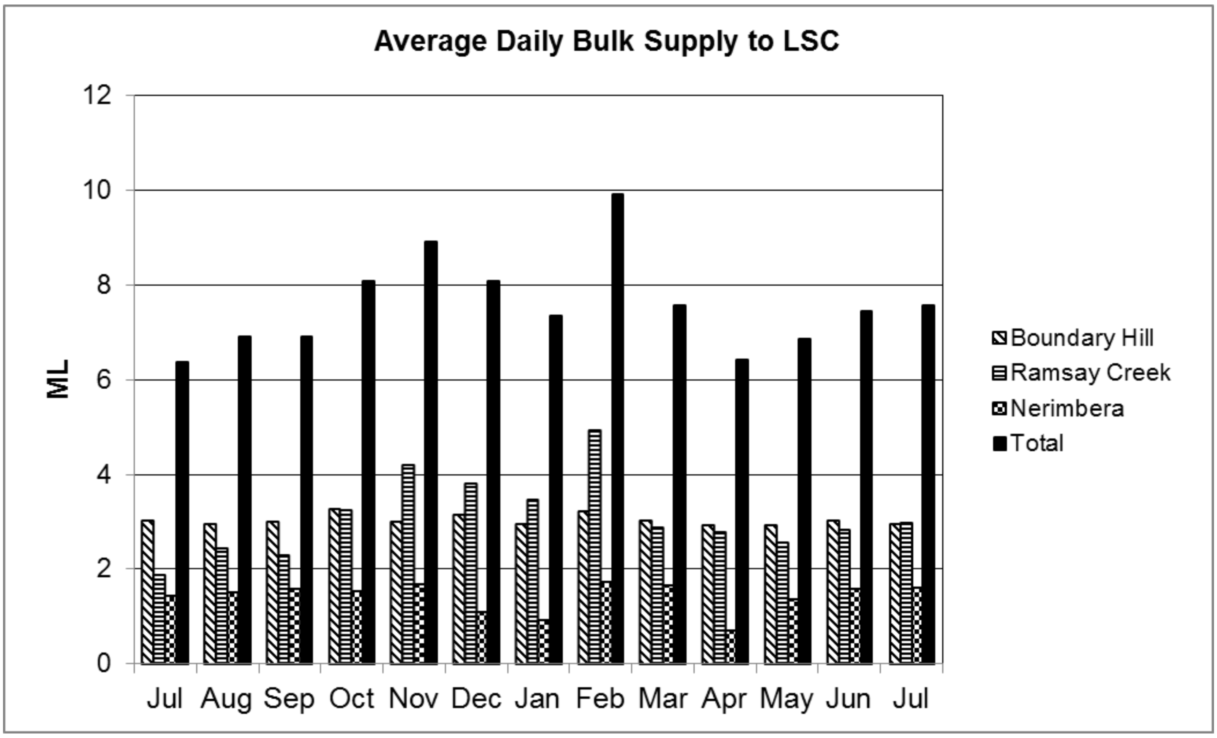
Average daily water consumption in Gracemere during July (5.0 ML/d) increased slightly compared to that recorded in June and was much greater than that reported in the same period last year. The higher consumption was due to the relatively low rainfall during the month. The Fitzroy Barrage Storage is currently at 100% of accessible storage volume and is therefore well above the threshold in the Drought Management Plan used to trigger the implementation of water restrictions.

Mount Morgan



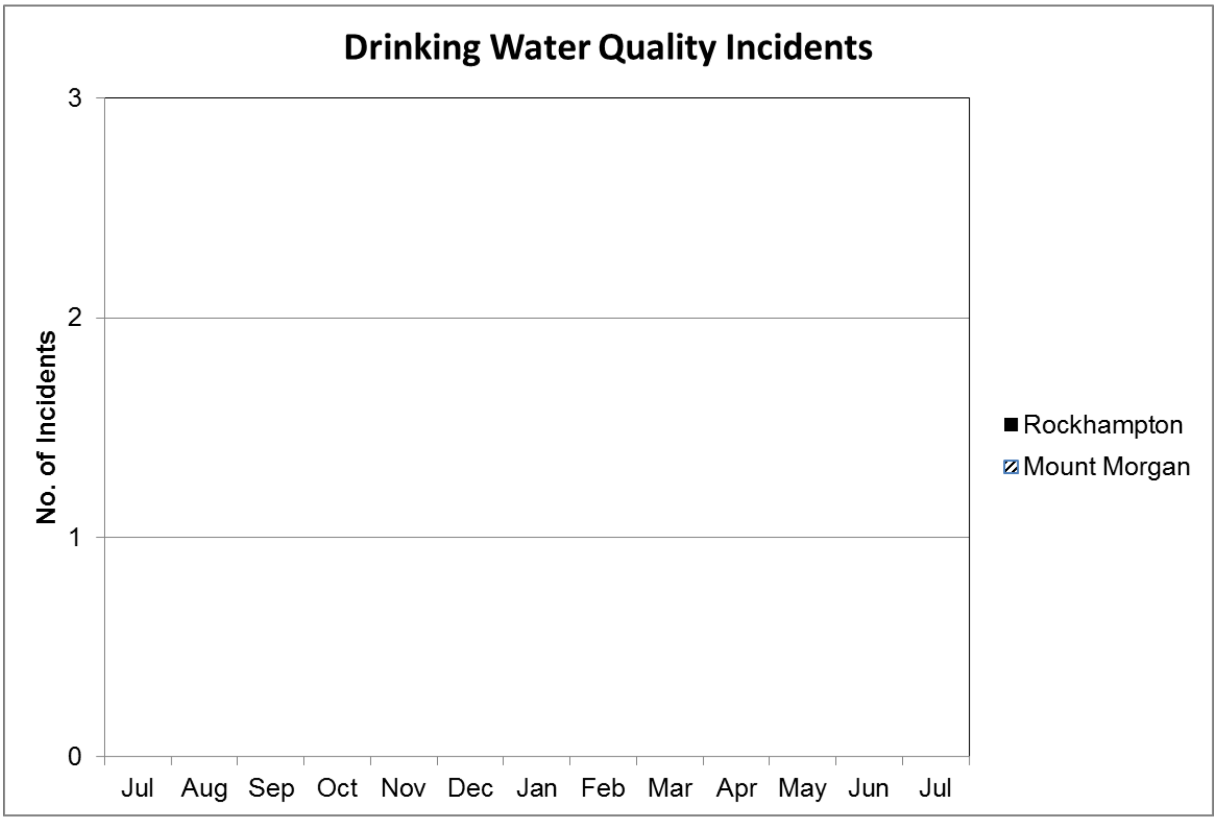
Average daily water consumption in Mount Morgan during July (0.95 ML/d) increased compared to that recorded in June and was greater than that reported for the same period last year. The higher consumption was due to the relatively low rainfall during the month. The No. 7 Dam is currently at 88% of the accessible storage volume and well above the 50% storage threshold value in the Drought Management Plan that is used to trigger the implementation of water restrictions in Mount Morgan.

Bulk Supply to Livingstone Shire Council



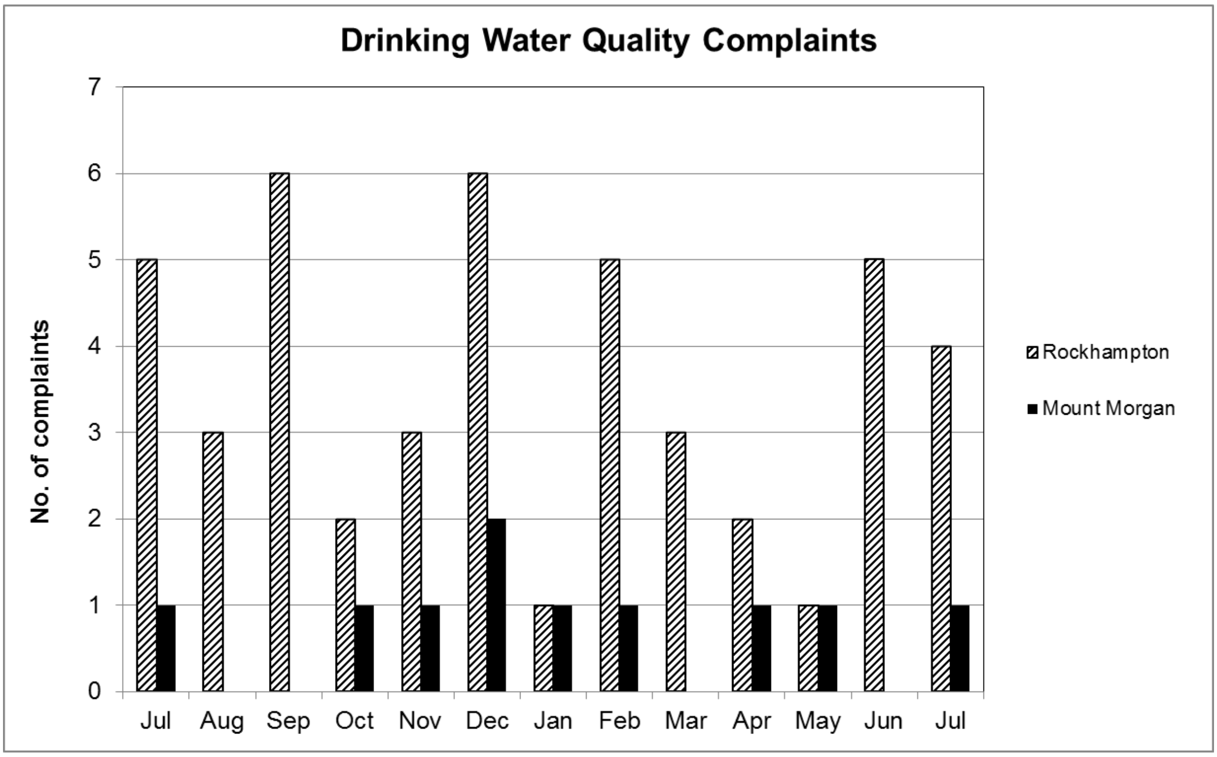
The average daily volume of water supplied to LSC during July increased slightly compared to that recorded in June to be 7.56 ML/d. This volume is higher than that recorded for the same period last year. The increase in bulk supply was due mainly to the relatively low rainfall during the month which contributed to the supply of greater volumes at each of the three sites.

Drinking Water Quality Incidents



No water quality incidents occurred during the month of July. No water quality incidents have occurred in the last two years.

Drinking Water Quality Complaints

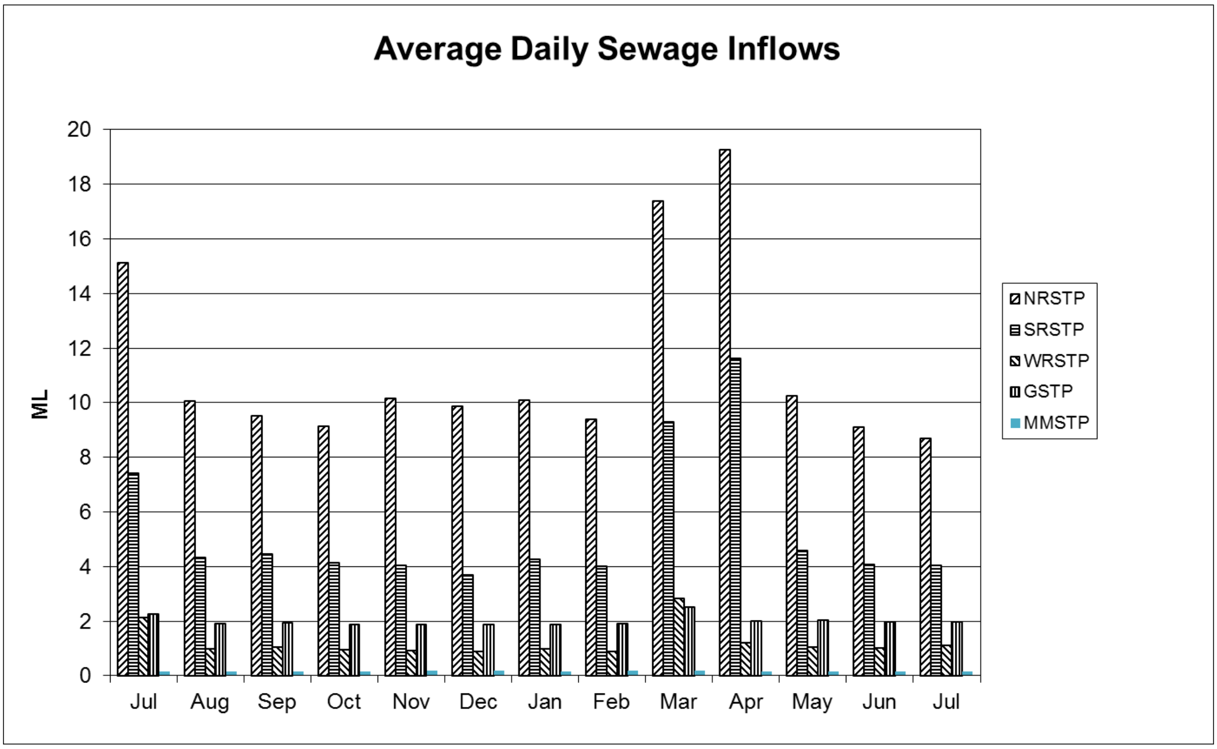


	Elevated Chlorine	Taste/Odour/Quality	Discoloured Water	Physical Appearance (e.g. residue or air)
No. Complaints	0	1	1	3

The total number of drinking water quality complaints (5 complaints) received during July was the same as the number of complaints received during June.

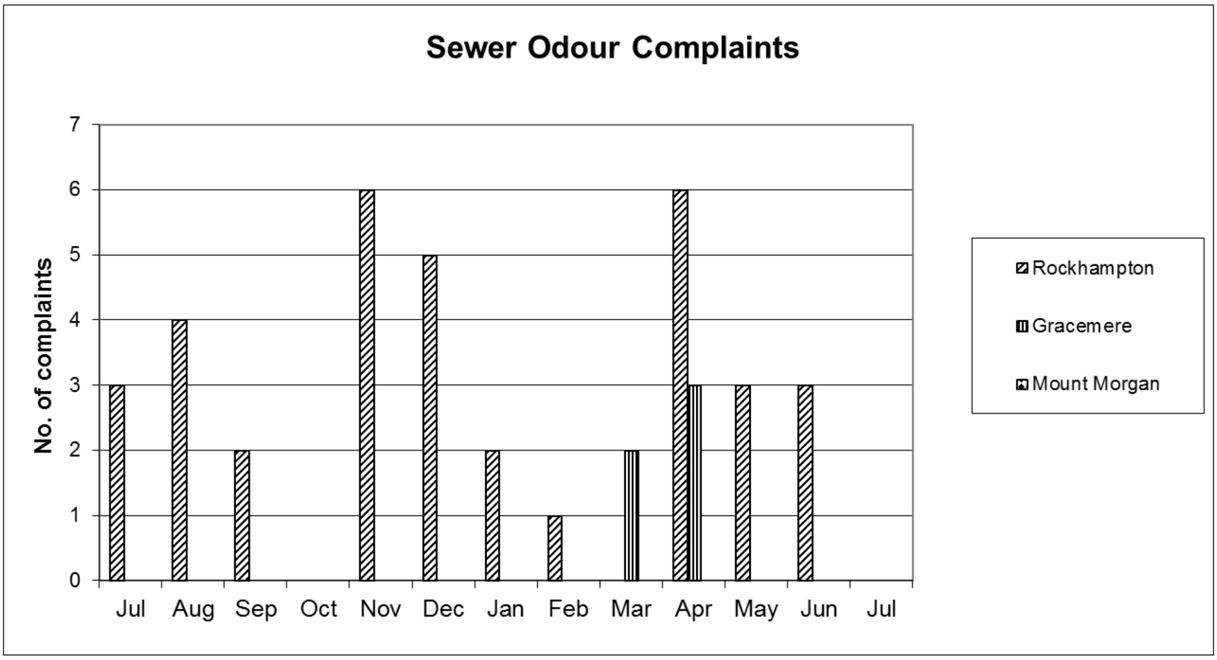
Four of the complaints were received from customers in Rockhampton and the other from a customer in Mount Morgan. Three of the complaints were associated with cloudy or milky water possible due to entrained air, one complaint was related to an unacceptable odour and the other complaint was due to discoloured water. In each instance, FRW responded and the complaints were resolved by flushing the water mains to clear or refresh the water provided to the customer. Water quality testing was used as appropriate to confirm the return to normal high quality water.

Sewage Inflows to Treatment Plants



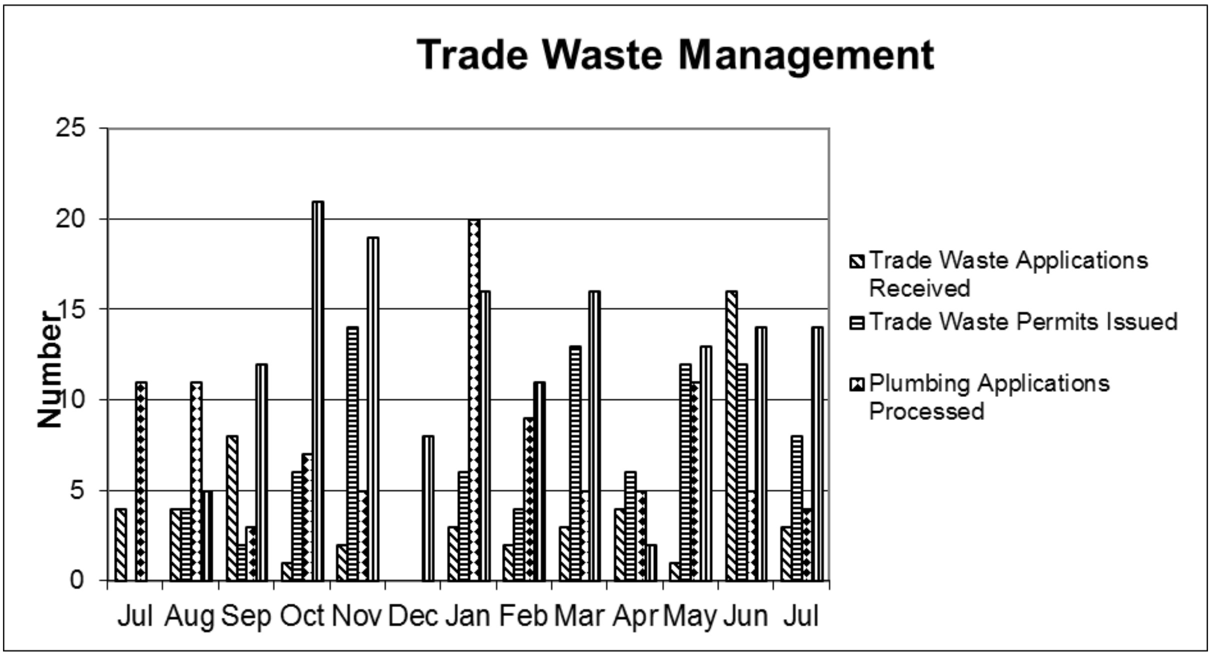
Average daily sewage inflows during July were similar to those recorded in June with the exception of NRSTP which decreased slightly. The ongoing low inflows were due to the relatively low rainfall during the month and therefore an absence of significant stormwater inflow or infiltration into the sewerage networks. These inflows are lower than that reported during the same period last year.

Sewer Odour Complaints



No sewer odour complaints were received during the month of July.

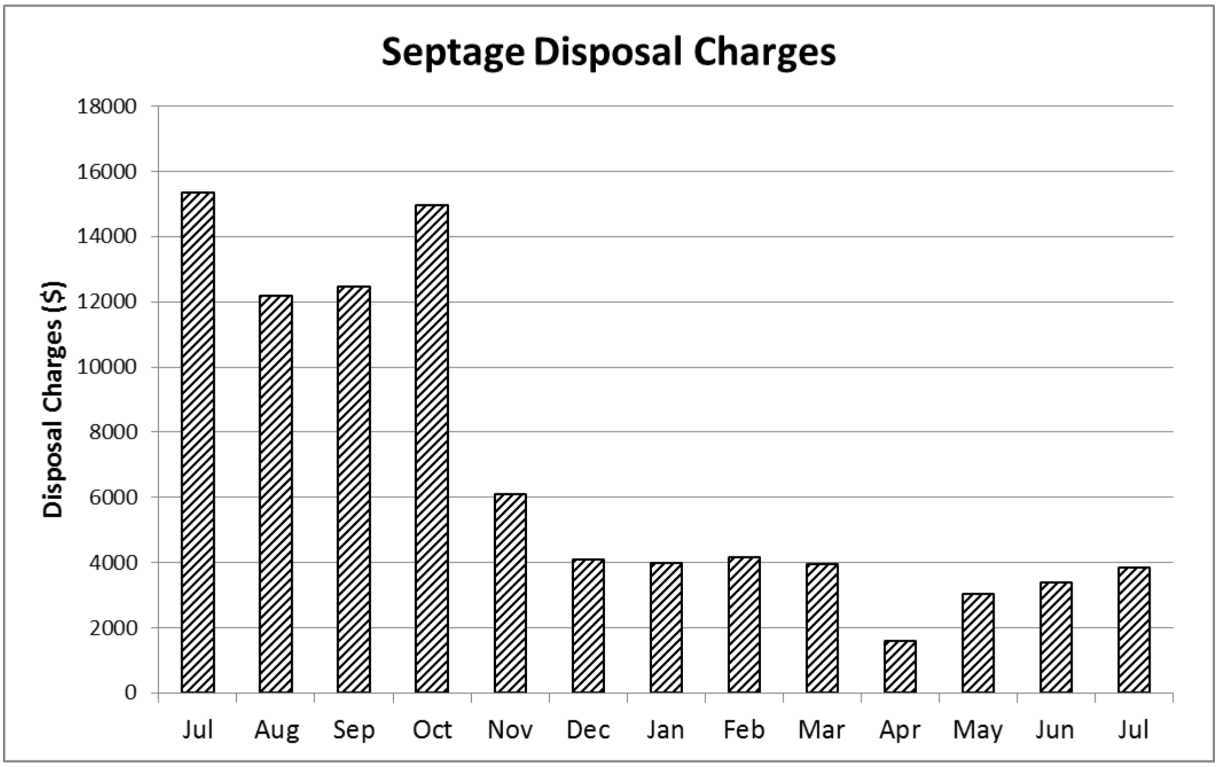
Trade Waste and Septage Management Activities



Three Trade Waste applications were received and 8 Trade Waste permits were issued during the month of June. A total of 4 Plumbing Applications were processed and another 14 Trade Waste assessments or inspections were completed by the team.

The table below shows those permits which contained a significant change either to their Category rating or due to the inclusion of a Special Condition in order to comply with Council's Trade Waste Environmental Management Plan.

Industry/Trade	**New or Renewal**	**Permit Category**	**Special Condition**	**Comments**
Bakery	Renewal	1	Repair and rehabilitate the grease trap	
Mechanical Workshop with Washbay	Renewal	1	Bunding of oil/chemical storage areas	

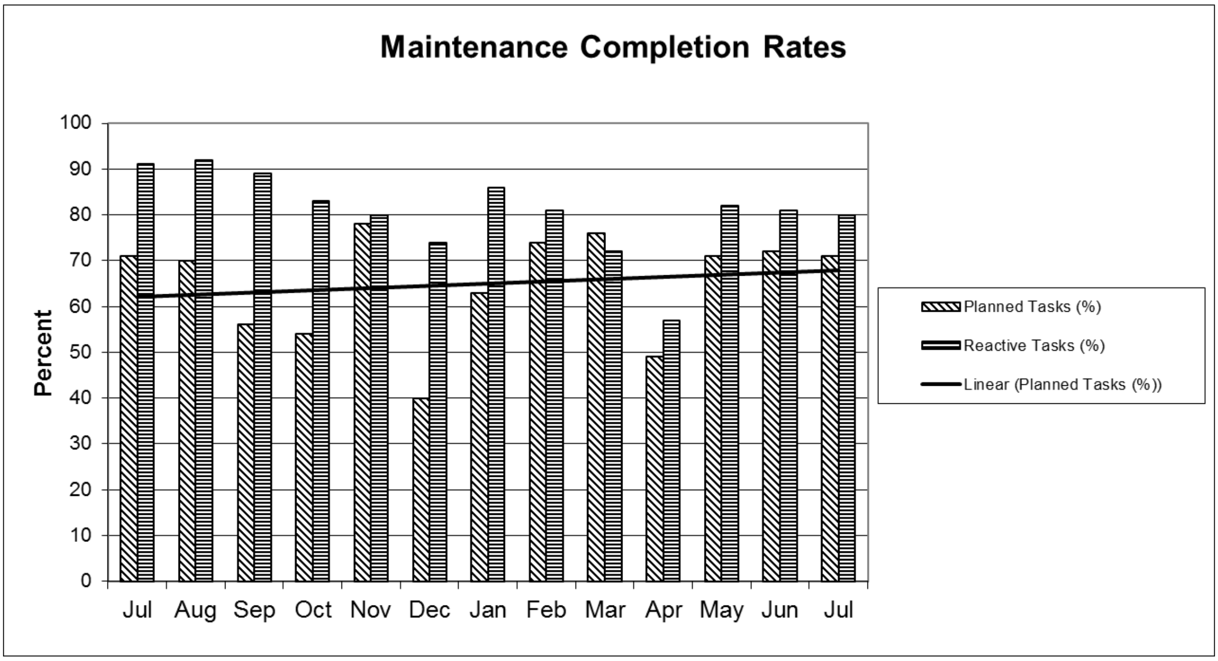


Revenue from the disposal of septage liquid waste at the North Rockhampton STP increased slightly for the month of July. The lower revenue compared to last year probably reflects the slight downturn in industrial works and the disposal of these wastes at other locations.

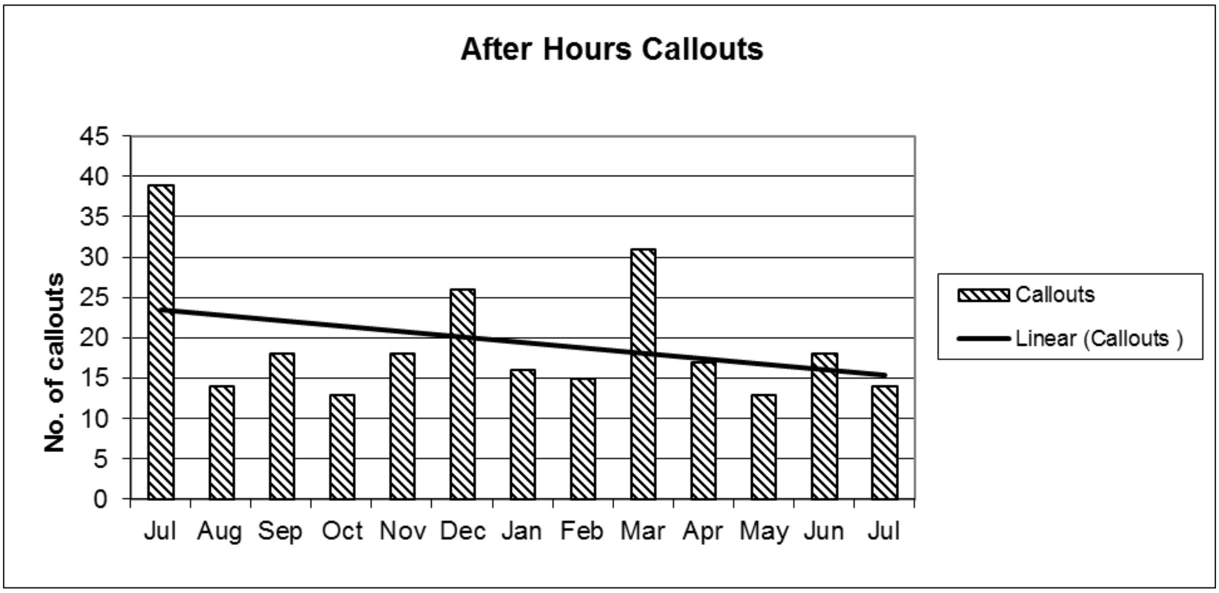
<u>Treatment and Supply Maintenance Activities</u>

The table below shows the breakdown of work completed based on the category of the work activity.

Maintenance Type	Work Category			
	Electrical	Mechanical	General	Operator
Planned	73	51	98	N/A
Reactive	45	17	3	0
After hours callouts	10	4	0	0
Capital	3	1	1	N/A
Safety and Compliance	5	1	2	0



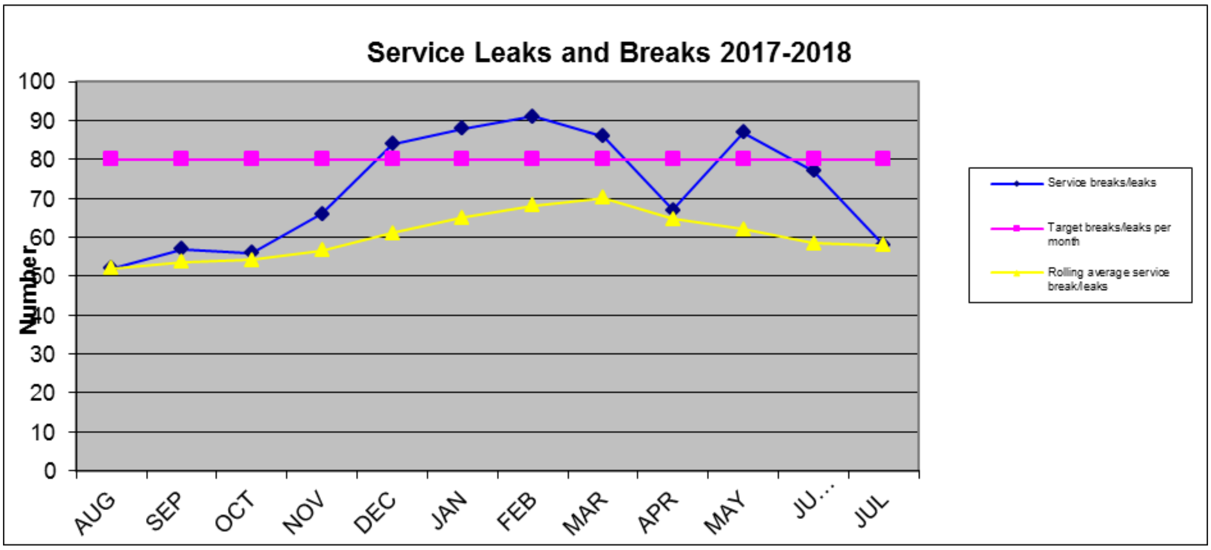
A total of 314 preventative maintenance activities were scheduled and 137 reactive maintenance activities were requested during the month of July. Completion rates for each type of maintenance activity by the end of the month were 71% and 80% respectively. The long term trend line shows continued improvement in the completion rate for planned maintenance tasks.



The number of after-hours callouts for electrical and mechanical reactive maintenance (14 call-outs) decreased during July compared to June. The number of callouts was less than the 12 month rolling average of 20 call-outs per month. The long term trend line in the graph indicates an overall decrease in callouts, with the highest numbers of callouts typically associated with months where heavy rainfall events occurred. In the majority of cases, the faults were rectified within the targeted rectification time according to the Priority Ratings used to rank reactive maintenance events.

NETWORK

Regional Service Leaks and Breaks



Performance

Target met with a continued reduction in service breaks from previous months, large number of class 12 poly service failures continues to be an issue, continued failures of threaded poly sections installed during water meter installations. A $150,000 capital water service replacement program to be implemented during future financial years based on service failure data.

Issues and Status

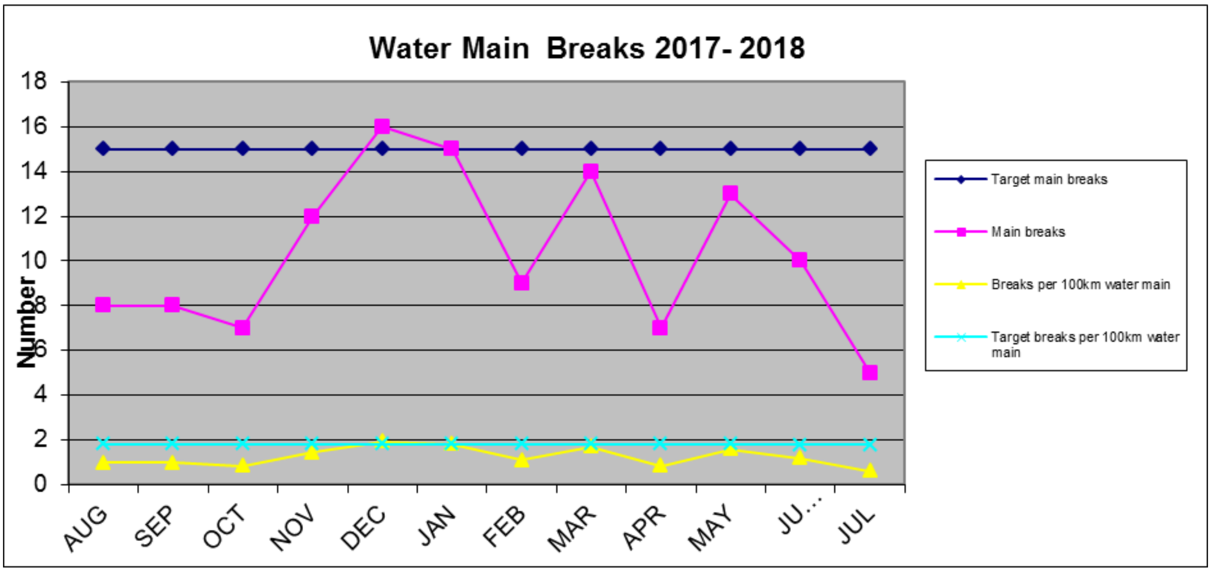
Maintenance records indicate a high percentage of service breaks and joint failures consistently occurring on older Class 12 poly services.

Response to Issues

Water services subject to repeated failures are being prioritized within the capital replacement program to minimise the risk of continued failures.

Locality	Service Leaks / Breaks
Rockhampton	56
Mount Morgan	2
Regional Total	**58**

Regional Water Main Breaks



Performance

Target achieved, decrease in water main breaks in Rockhampton when compared to previous months. Overall trending decrease in water main failures as a result of the implementation of a strategic Capital Water Main Replacement Program continues.

Issues and Status

The following table shows the number of breaks per month.

Water Main Type	May 2017	June 2017	July 2017
Cast Iron	3	2	0
AC	4	5	5
PVC	3	3	0
GWI	0	0	0
Mild Steel	0	0	0
Poly	3	0	0
TOTAL	**13**	**10**	**5**

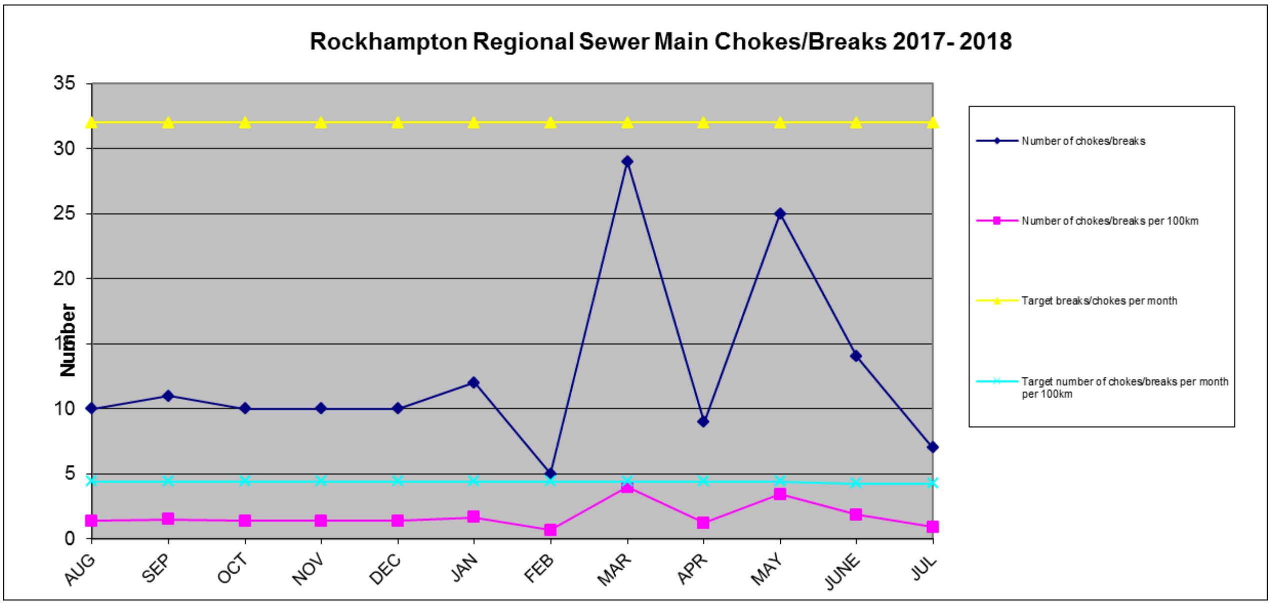
Response to Issues

Continued defect logging and pressure management will reduce failure occurrences. Water mains experiencing repeated failures are assessed for inclusion in annual Water Main Replacement capital program.

	Number of Main Breaks	Target Main Breaks	Breaks per 100 km	Target Breaks per 100 km	Rolling average per 100 km
July	5	**15**	0.6	**1.80**	0.6

Locality	Main Breaks
Rockhampton	3
Mount Morgan	2
Regional Total	**5**

Rockhampton Regional Sewer Main Chokes/Breaks



Performance

Target achieved, apart from some issues during recent extreme weather events, it’s evident that mainline sewer blockages are continuing to trend down in line with capital sewer refurbishment programs.

Issues and Status

Data indicates that a high percentage of blockages / overflows continue to be caused by defective pipes resulting in tree root intrusion.

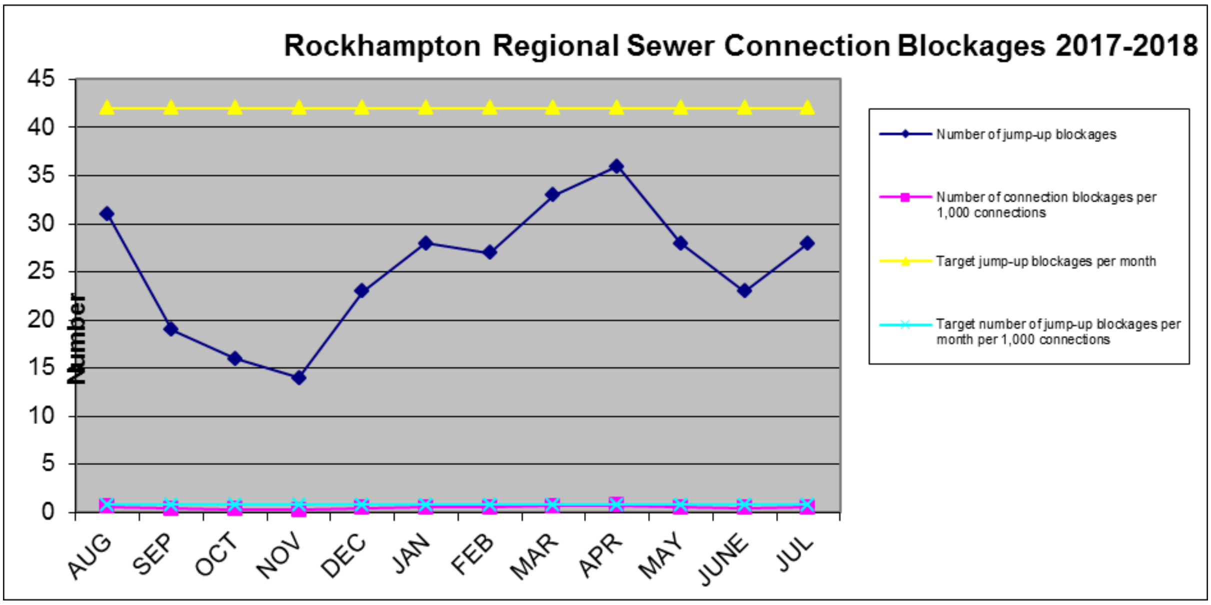
Response to Issues

Continue to log defects and monitor outcomes to ensure inclusion in the Capital Sewer Main Relining and rehabilitation programs.

	Number of chokes/ breaks	**Target chokes/breaks per month**	**Number of chokes/ breaks per 100 km**	**Target number of chokes / breaks per month per 100km**	**Rolling 12 month average per 100 km chokes / breaks**
July	7	**32**	0.9	**4.41**	0.9

Locality	**Surcharges**	**Mainline Blockages**
Rockhampton	6	7
Mount Morgan	0	0
Regional Total	**0**	**7**

Rockhampton Regional Sewer Connection Blockages



Performance

Target achieved with a slight increase in blockages when compared to the previous month. It's evident that sewer connection blockages are continuing to trend down gradually in line with capital sewer refurbishment programs. Sewer connections are prioritised for inclusion in these capital refurbishment programs in line with failure information.

Issues and Status

Data indicates blockages are been caused by broken pipes due to age, along with the resulting tree root intrusion.

Response to Issues

Continue to assess properties with repeat breaks and chokes for inclusion in the capital sewer refurbishment programs.

	Number of connection blockages	Target connection blockages per month	Number of connection blockages per 1,000 connections	Target number of connection blockages per 1,000 connections	Rolling 12 month average per 1,000 connections
July	28	**42**	0.55	**0.83**	0.55

Locality	Connection Blockages
Rockhampton	28
Mount Morgan	0
Regional Total	**28**

Sewer Rehabilitation Program

	Number completed	FY to date totals
Access Chambers raised	6	**6**
Sewers repaired	4	**4**

Inflow/Infiltration Program (South Rockhampton)

	Number completed	FY to date totals

Defective Properties Rectified	31	**31**

Inflow/Infiltration Program (North Rockhampton)

	Number completed	FY to date totals
Properties Inspected	484	**484**
Defects Identified	101	**101**

Private Works

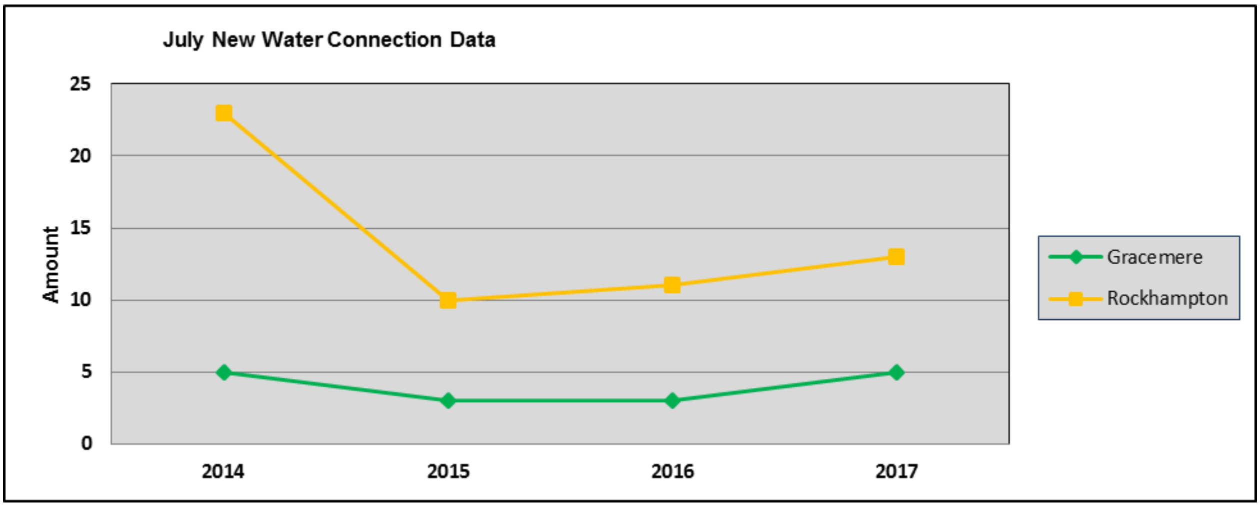
New Water Connections

Region	July 2017	FY to Date 2017	FY to Date 2016	FY to Date 2015	FY to Date 2014
Gracemere	5	5	3	3	5
Rockhampton	13	13	11	10	23
Mount Morgan	n/a	n/a	n/a	n/a	n/a
Regional Total	**18**	**18**	**14**	**13**	**28**

This table and graph shows the water connection data, for July, for the past four years.

Region	July 2017	July 2016	July 2015	July 2014
Gracemere	5	3	3	5
Rockhampton	13	11	10	23
Mount Morgan	n/a	n/a	n/a	n/a
Total	**18**	**14**	**13**	**28**

New Connection Data



Details on Private Works Jobs

The table below shows the quantity of private works jobs quoted and accepted during the reporting period and year to date. Jobs include both water and sewerage.

	July	Amount	FYTD	FYTD Amount
Quotes Prepared	10	$34,418.22	10	$34,418.22
Quotes Accepted	5	$16,066.65	5	$16,066.65
Jobs Completed	3	$8,776.19	3	$8,776.19

Water Meters

Sectors 1, 2, 3 and 4 were read during the month of July 2017 with a total of 11,159 meters being read.

Sectors Read	1	2	3	4	Total
No. of Meters in Sector	2,300	3,469	2,427	2,963	11,159
No-Reads	2	4	3	16	25
% Of No-Reads	0.08	0.11	0.12	0.53	0.22

Special Water Meter Reads

Reading Type	No. of Reads	$ Value
Water Account Search - Averaged Readings $31 per read	73	$2,263
Water Account Search - On-Site Readings $158 per read	13	$2,054
Total $ Value for July		$4,317
Total $ Value Financial Year to Date		$4,317

Building Over Sewers

The following summary is an overview of this core business activity that requires ongoing negotiations with the respective stakeholders and detailed investigations to determine location and condition assessments of the associated infrastructure.

Activity Summary

	July	FYTD
General Enquiries / BOS	6	6
Inspections	5	5
Meetings	2	2
Site Visits	21	21
Pre-Starts	1	1
Approval Permits Issued	0	0
Permits closed	3	3
Total	**38**	**38**

Building Over Sewer Applications under Assessment

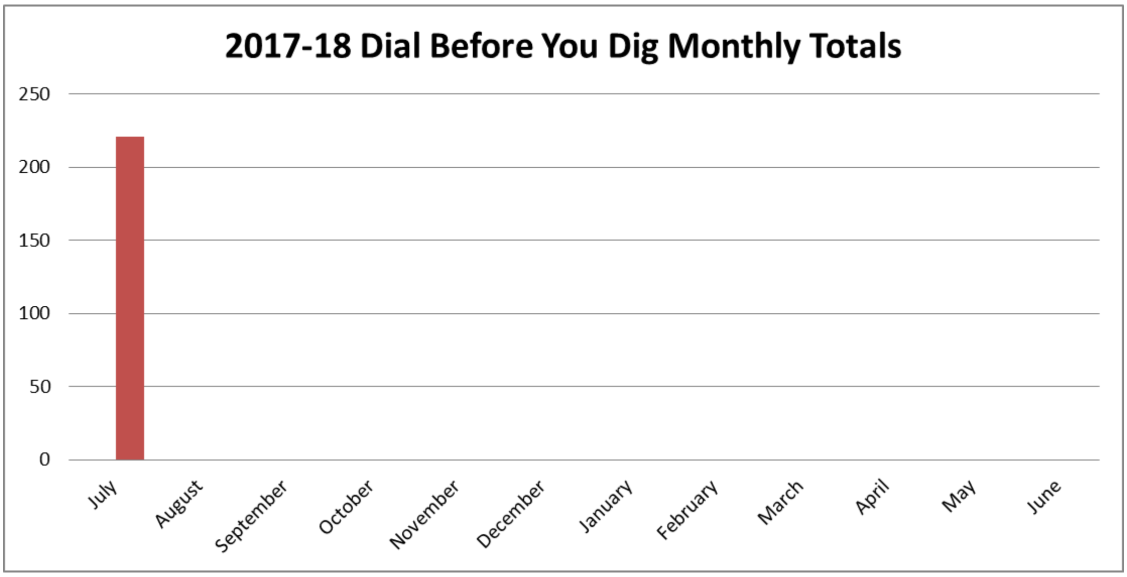
There are four permits currently under assessment as at 31 July 2017.

ADMINISTRATION

Dial Before You Dig (DBYD)

The average number of requests received per day for July was 7.13 a slight increase from 5.23 in June.

	May 2017	June 2017	July 2017	FY Total 17/18
Requests Processed	227	157	221	221



Site Tours

There were no site tours of the Glenmore Water Treatment Plant (GWTP) in July.

Undetected Leaks (Residential)

	July	FYTD
New requests	16	16
Number declined	2	2
Number approved	4	4
Require more info	8	8
Being held until next meter read	20	20
Total kL rebated	2,439	2,439
Total value approved	**$4,750.27**	**$4,750.27**

Undetected Leaks (Commercial)

	July	FYTD
New requests	1	1
Number declined	0	0
Number approved	0	0
Require more info	1	1
Being held until next meter read	1	1
Total kL rebated	0	0
Total value approved	**$0.00**	**$0.00**

Residential Rebates

	July	Total FYTD Applications	Total FYTD $
Washing machines	21	21	$2,100
Stand alone tank	0	0	$0
Integrated tank	0	0	$0
Dual flush toilet	0	0	$0

Shower rose	0	0	$0
Total	**21**	**21**	**$2,100**

Two applicants have been requested to provide additional information as they are not enrolled on the AEC at the installation address.

<u>Communication and Education</u>

Barrage Open Day

The Fitzroy River Barrage Open Day was held from 9am until 1pm Saturday, 29 July 2017 at the Fitzroy River Barrage (Larcombe Street entrance, Park Avenue). Approximately 1,200 people took part in walking across the Barrage, with many others enjoying the range of stalls and food available on the day.

With barrage walks, baby crocodiles and kids' activities among the day's program, the popular event which occurs every three years was one not to be missed. The day was about celebrating and raising awareness of the vital role our water resources and Barrage play in our day-to-day lives. Among the activities on offer, there were tours of the barrage and an opportunity to capture a very rare and picturesque view of the mighty Fitzroy River from atop the Barrage.

Hosted by Fitzroy River Water, the event also provided an impressive learning opportunity about our local water supply and our water catchment. Attendees were able to learn firsthand the behind the scenes of water supply, from treatment to tap. A range of things could be learnt through our displays and stalls from water meter readings to water conservation and even how FRW treats the water that ends up in your home. Fitzroy Basin Association, Capricornia Catchments, Fisheries Queensland as well as Koorana Crocodile Farm, Council's Recreational Fishing Strategy, Environmental Health, Pest and Vector Management were all available to discuss how to enjoy and look after our catchment as well.

Media Releases

28 July 2017 Countdown on for Fitzroy River Barrage Open Day

Social Media

Barrage Open Day event was created on Rockhampton Regional Council's Facebook page in June with the event generating over 500 interested and 78 shares.

Monday 21 July 2017 reminder post about the event generated 146 comments and 100 shares and a reminder post on Friday 28 July 2017 generated 33 comments and 30 shares.

Radio Advertising

Radio advert placements commenced on Monday 24 July 2017 leading into the event. A total of 71 placements were played throughout the week and 6 live broadcasts were played from the event as part of the road show package.

Newspaper

Full page editorial about the event was published on Thursday 27 July 2017 in addition to two banner advertisements placed in Friday 28 and Saturday 29 July 2017 The Morning Bulletin.

INFRASTRUCTURE PLANNING

Sewer Network Investigations

PFTI Review

No further development

Inflow / Infiltration

Internal drainage plans for Range Convent have been reviewed to develop plan for detailed internal inspection.

Sewer Area Maps

No further development

North Rockhampton Flood Mitigation Investigation (NRFM)

No further development.

Mt Morgan Sewerage Strategy

The Railway Parade sewer pump station Planning Report has been revised with the new recommendation to discharge directly into the Dee Street sewer pump station. The revised Planning Report is currently with FRW for endorsement.

Parkhurst Sewerage Pump Station Implementation Strategy

No further development.

Gracemere - Rahima Sewerage Pump Station

A Planning Report is being prepared to investigate the existing and future capacity for the Rahima Sewerage Pump Station. The report will document, detail and estimate the timing of previously identified PFTI works.

Gracemere – Fisher Street Sewerage Pump Station

No further development

Water Network Investigations

Network Performance Maps

The maps have been received by the Queensland Fire and Emergency Services (QFES) who acknowledged their appreciation and advised the maps had been distributed to their crews.

Parkhurst 600mm Trunk Main Replacement Analysis

The loss of the existing 200mm water main in Norman Road between Mason Street and Olive Street was highlighted due to the unavoidable alignment clash with the proposed 600mm trunk main. The proposed locations of the two pressure reducing valve connections at the Norman Road intersections of Newton Street and Vermont Drive will maintain the existing service levels. A third connection at the intersection of Rosedale Street was nominated as a potential supply option to service future development on the eastern side of Norman Road to compensate for the loss of the 200mm water main.

Water Area Maps

No further development

Mt Morgan – Future Water Supply

No further development.

Water Meter – Thematic Mapping of Consumption

No further development

System Leakage Management Plan

No further development

Mt Morgan – Water Reticulation Planning Report

The Planning Report will document the demand management strategy that has been gradually implemented over the last six years and the various network augmentations that have been implemented in this time.

The ultimate objective to decommission the Black Street pressure reduction valve located at the head of the network is now imminent and the impact this will have on the existing pump stations will also be addressed in the Planning report.

Gracemere - Old Capricorn Highway Pump Station Upgrade Investigation

The potential opportunity to utilise the additional Agnes Street pump station capacity to compliment the Old Capricorn Highway pump station is currently being investigated.

8.4 SCADA UPGRADE AT FITZROY RIVER WATER FOR IMPROVED SECURITY AND FUNCTIONALITY

File No:	**1466**
Attachments:	**1. Security of Critical Water Infrastructure - Queensland Audit Office June 2017** **2. FRW SCADA Risk Assessment Summary Report**
Authorising Officer:	**Peter Kofod - General Manager Regional Services**
Author:	**Jason Plumb - Manager Fitzroy River Water**

SUMMARY

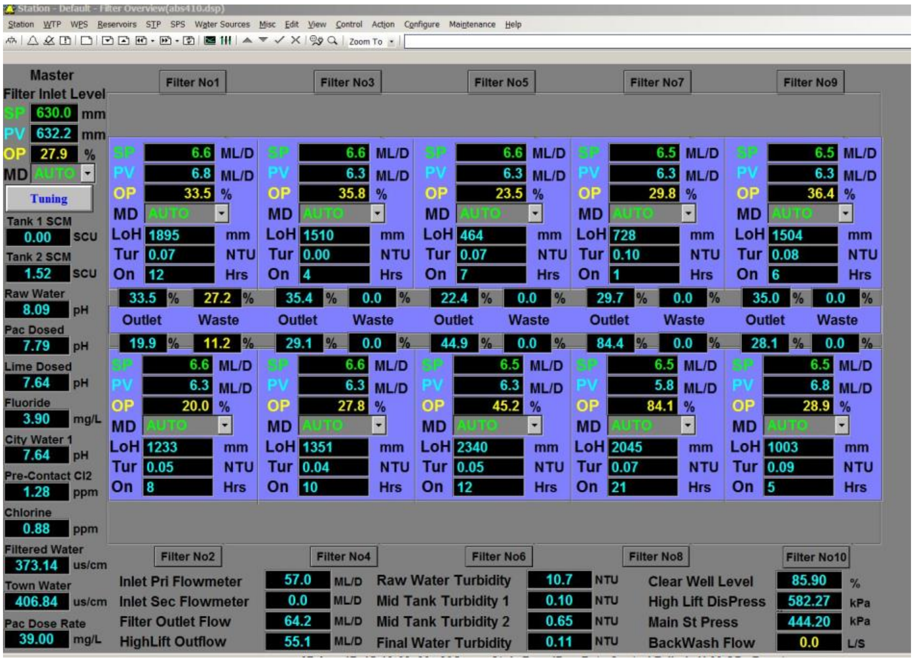
Fitzroy River Water is currently completing the renewal and upgrading of the SCADA system that is used to monitor and control its many water and sewerage assets and associated operations. The new system will provide a safe and reliable solution to meet the needs of both FRW and the community. The project has assessed the risks posed by cyber-attacks and other threats to the security of water and sewerage infrastructure. and it is expected that the new SCADA system will provide a high level of cybersecurity and increased functionality for the management of important water and sewerage assets and related services.

OFFICER’S RECOMMENDATION

THAT the information provided in this report be received and the importance of the SCADA system be noted.

COMMENTARY

The water and sewerage operations conducted by Fitzroy River Water (FRW) play an important role in protecting public and environmental health. It is therefore very important that all aspects of these operations are able to be managed in a safe and reliable manner so that any risks to the continuity and performance of these water and sewerage operations and their related services are managed accordingly. The water industry like many other industrial sectors relies on a system called Supervisory Control and Data Acquisition (SCADA) to safely and reliably manage these important operations. SCADA describes the way in which the operation of local or remote field equipment can be monitored and controlled by a person in a dedicated control room or other remote location to ensure that this equipment is operating as intended. Information from the local or remote field equipment (e.g. water pump) is transmitted by radio, microwave or other form of telemetry to a central communications facility where it is converted into a usable format. The figure below shows a screen shot of one of the main SCADA pages at the Glenmore WTP that shows a range of information relating to the operation of the WTP such as water quality information, filter and other process operations, and pumped flows from the associated pump stations.


Station - Default - Filter Overview(abs410.dsp)
Station WTP WPS Reservoirs STP SPS Water Sources Misc Edit View Control Action Configure Maintenance Help
Zoom To
Tuning

Master
Filter Inlet Level
SP 630.0 mm
PV 632.2 mm
OP 27.9 %
MD AUTO

Tank 1 SCM	0.00 SCU
Tank 2 SCM	1.52 SCU
Raw Water	8.09 pH
Pac Dosed	7.79 pH
Lime Dosed	7.64 pH
Fluoride	3.90 mg/L
City Water 1	7.64 pH
Pre-Contact Cl2	1.28 ppm
Chlorine	0.88 ppm
Filtered Water	373.14 us/cm
Town Water	406.84 us/cm
Pac Dose Rate	39.00 mg/L

	Filter No1	Filter No3	Filter No5	Filter No7	Filter No9
SP	6.6 ML/D	6.6 ML/D	6.6 ML/D	6.5 ML/D	6.5 ML/D
PV	6.8 ML/D	6.3 ML/D	6.3 ML/D	6.3 ML/D	6.3 ML/D
OP	33.5 %	35.8 %	23.5 %	29.8 %	36.4 %
MD	AUTO	AUTO	AUTO	AUTO	AUTO
LoH	1895 mm	1510 mm	464 mm	728 mm	1504 mm
Tur	0.07 NTU	0.00 NTU	0.07 NTU	0.10 NTU	0.08 NTU
On	12 Hrs	4 Hrs	7 Hrs	1 Hrs	6 Hrs
Outlet	33.5 %	35.4 %	22.4 %	29.7 %	35.0 %
Waste	27.2 %	0.0 %	0.0 %	0.0 %	0.0 %

	Filter No2	Filter No4	Filter No6	Filter No8	Filter No10
Outlet	19.9 %	29.1 %	44.9 %	84.4 %	28.1 %
Waste	11.2 %	0.0 %	0.0 %	0.0 %	0.0 %
SP	6.6 ML/D	6.6 ML/D	6.5 ML/D	6.5 ML/D	6.5 ML/D
PV	6.3 ML/D	6.3 ML/D	6.3 ML/D	5.8 ML/D	6.8 ML/D
OP	20.0 %	27.8 %	45.2 %	84.1 %	28.9 %
MD	AUTO	AUTO	AUTO	AUTO	AUTO
LoH	1233 mm	1351 mm	2340 mm	2045 mm	1003 mm
Tur	0.05 NTU	0.04 NTU	0.05 NTU	0.07 NTU	0.09 NTU
On	8 Hrs	10 Hrs	12 Hrs	21 Hrs	5 Hrs

Inlet Pri Flowmeter	57.0 ML/D	Raw Water Turbidity	10.7 NTU	Clear Well Level	85.90 %
Inlet Sec Flowmeter	0.0 ML/D	Mid Tank Turbidity 1	0.10 NTU	High Lift DisPress	582.27 kPa
Filter Outlet Flow	64.2 ML/D	Mid Tank Turbidity 2	0.65 NTU	Main St Press	444.20 kPa
HighLift Outflow	55.1 ML/D	Final Water Turbidity	0.11 NTU	BackWash Flow	0.0 L/S

Figure 1. Screenshot of a SCADA page for the Glenmore WTP showing relevant information.

Modern SCADA systems are now developing to provide greater functionality and reliability. The traditional capability of simple trending of data, configuration of basic alarms for deviations from operational set-points or specified operating ranges has been developed further with modern systems now able to incorporate more advanced means of configuring alarms based on customizing alarms based on multiple parameters, selectable reporting of operational data, and incorporation and management of CCTV surveillance and site security.

As more and more important public or private infrastructure is controlled using SCADA, the development of SCADA system security to meet current and future threats is paramount. The increased prevalence of cyber-attacks against public and private infrastructure entities highlights the need for vigilance with SCADA and other information and communication technology systems to ensure that critical infrastructure or high value information is protected as appropriate. A report tabled to Queensland Parliament by the Queensland Audit Office (QAO) into *Security of Critical Water Infrastructure (June 2017)* revealed that in some parts of Queensland, water infrastructure was not as secure as it should be with respect to both physical and site security as well as information technology or cyber security. The report outlined a number of recommended actions for both water service providers and government agencies to improve the overall security of critical water infrastructure, with specific emphasis on cyber security. A copy of the full QAO report is attached to this report.

BACKGROUND

FRW has used SCADA for the monitoring and control of its water and sewerage operations for at least 15 years. During this time the renewal and upgrading of infrastructure has increased the extent to which SCADA is used, with major additions to FRW's SCADA system following amalgamation in 2008. In recent years, FRW identified the need to upgrade its SCADA system to improve its functionality but also to ensure that it remains as secure for the safe and reliable operation of water and sewerage assets.

In late 2016, FRW awarded a contract to Honeywell Process Solutions for the renewal and upgrading of the SCADA system. The new SCADA system will have new functionality including advanced alarm configuration capability, automated reporting and escalation to other systems or key individuals, and management of CCTV surveillance, and the ability to securely publish selected SCADA information to the publicly accessible internet. In addition to the new functionality, the scope of the project included the upgrading of the SCADA system in accordance with the newly published *SCADA Guideline (Water Services Association of Australia, WSAA, 2016)* which amongst other requirements includes the completion of a detailed risk assessment on the cybersecurity of the new SCADA system to ensure that it was robustly designed to withstand any threats to cybersecurity. In early 2017, a risk assessment workshop was hosted by Honeywell Process Solutions' international cybersecurity expert held with represents from FRW and Council's IT section to provide a thorough evaluation of the design of the new SCADA system but also to recommend improvements to related access and physical security measures. A copy of the main findings and recommendations of the risk assessment workshop are provided as an attachment to this report.

The SCADA upgrade project is now nearing completion following some delays due to the implementation of the cybersecurity risk assessment recommendations and minor technical issues. It is expected that the improvements to this important system will help to ensure that FRW's water and sewerage operations are safe and reliable into the future. The increased functionality of the SCADA system is also expected to improve the overall security of remotely located water and sewerage assets through improved surveillance as CCTV is installed at other critical sites.

BUDGET IMPLICATIONS

The renewal and upgrading of the SCADA system was funded as a capital project in the 2016-17 Council Budget and has a contract value of approximately $270,000.

RISK ASSESSMENT

The risk of cyber-attacks and other threats to FRW's water and sewerage assets and operations continues to be a focus of key legislative documents such as the Drinking Water Quality Management Plan and also Council's risk registers.

CORPORATE/OPERATIONAL PLAN

This project is related to a number of Corporate and Operational Plan actions in the *Regional Infrastructure and Facilities* component that are specific to the services associated with the operation of water and sewerage assets. These services include raw and potable water supplies, sewerage services, recycled water services and the operation and management of raw water storages.

CONCLUSION

The renewal and upgrading of the FRW SCADA system is an important project for the future safe and reliable operation of water and sewerage infrastructure. This report demonstrates the due consideration that has been given to this important project and the overall importance of security for this critical infrastructure.

SCADA UPGRADE AT FITZROY RIVER WATER FOR IMPROVED SECURITY AND FUNCTIONALITY

Security of Critical Water Infrastructure - Queensland Audit Office June 2017

Meeting Date: 15 August 2017

Attachment No: 1

Queensland Audit Office
better public services

Security of critical water infrastructure

Report 19: 2016–17

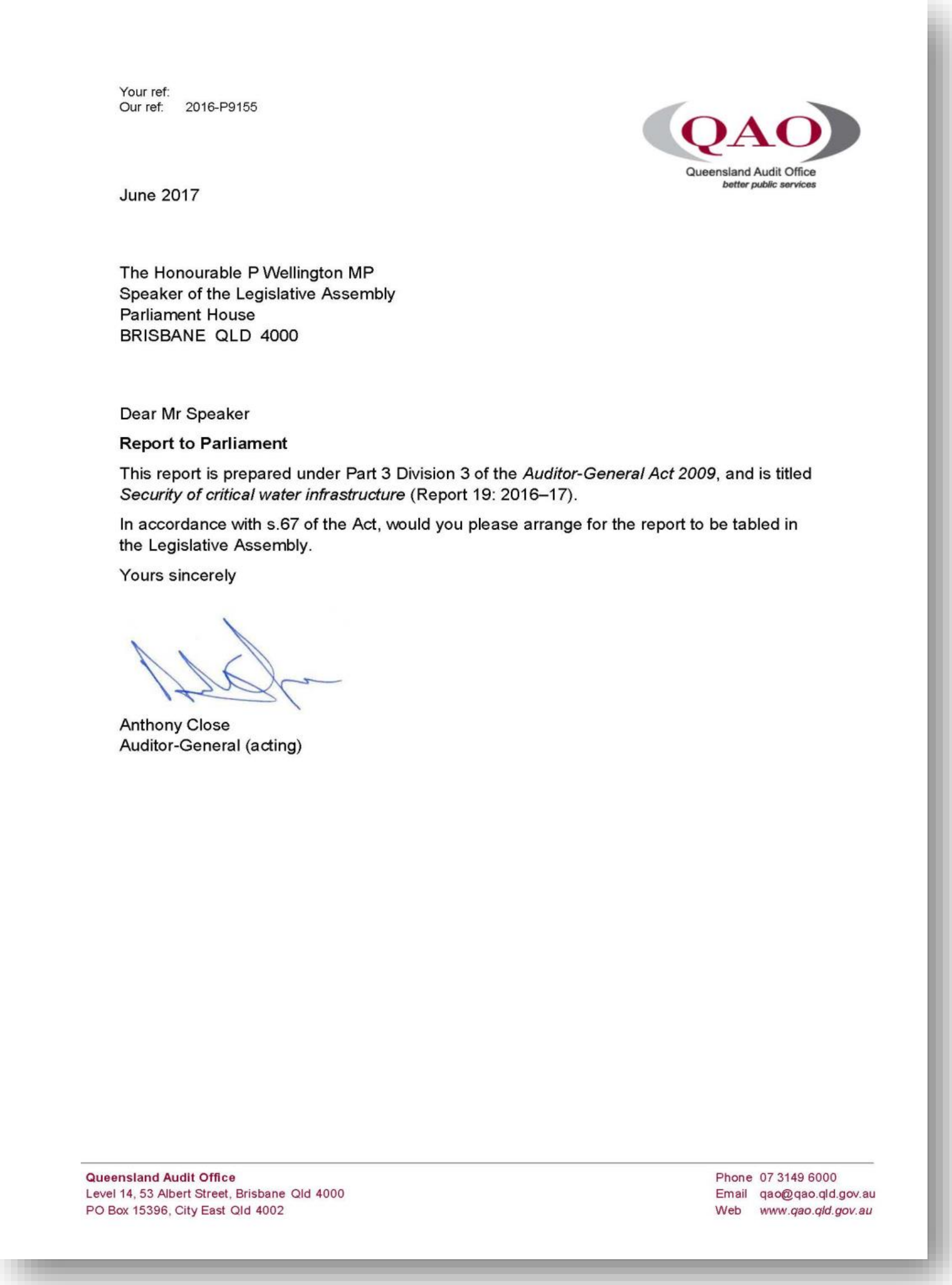
www.qao.qld.gov.au LinkedIn: Queensland Audit Office June 2017

Queensland Audit Office

Location Level 14, 53 Albert Street, Brisbane Qld 4000
PO Box 15396, City East Qld 4002
Telephone (07) 3149 6000
Email qao@qao.qld.gov.au
Online www.qao.qld.gov.au

Front cover image is an edited photograph of Queensland Parliament, taken by QAO.

ISSN 1834-1128



Your ref:
Our ref: 2016-P9155

QAO
Queensland Audit Office
better public services

June 2017

The Honourable P Wellington MP
Speaker of the Legislative Assembly
Parliament House
BRISBANE QLD 4000

Dear Mr Speaker

Report to Parliament

This report is prepared under Part 3 Division 3 of the *Auditor-General Act 2009*, and is titled *Security of critical water infrastructure* (Report 19: 2016–17).

In accordance with s.67 of the Act, would you please arrange for the report to be tabled in the Legislative Assembly.

Yours sincerely

Anthony Close
Auditor-General (acting)

Queensland Audit Office
Level 14, 53 Albert Street, Brisbane Qld 4000
PO Box 15396, City East Qld 4002

Phone 07 3149 6000
Email qao@qao.qld.gov.au
Web *www.qao.qld.gov.au*

Contents

Summary

Reliable drinking water and wastewater services are essential to all Queenslanders. Water service providers generally use computer systems to control operations of water treatment plants, and related facilities and assets. The security of these control systems is therefore important in maintaining continuity of service.

It is common practice for organisations to secure their financial systems, but this is not always the case for computer systems controlling operational infrastructure. Yet failure or security breaches in these control systems can have major consequences for the health of citizens, the environment, and the businesses that rely on these services.

Owners of critical water infrastructure are responsible for protecting these control systems from potential attacks. These threats may be through acts of terrorism, or carried out by curious and technically competent individuals, or by trusted insiders with malicious intent to harm. Staff can also compromise security by making simple technical errors. Recent security threats and incident reports show that, as the security industry advances, so do the hackers and cyber criminals. Attackers can easily access malicious software online to use in attempts to breach control systems. This software is becoming harder to control as it has become more resilient to the solutions developed to protect control systems.

Reported incidents also show that some critical infrastructure breaches and cyber threats come from inside the entities, or from 'lone wolf' attackers. The increased incidence of these types of attacks means that owners of control systems must continually assess and improve the defences that they have built within their control environment.

In this audit, we assessed whether a selection of entities responsible for critical water infrastructure have processes in place to protect their water control systems. We carried out our own tests, known as penetration tests, to identify and exploit security vulnerabilities. We also assessed whether these entities could detect the security breaches and restore the systems in the event of an attack.

Audit conclusions

The water control systems were not as secure as they should have been at the time of our audit testing. The age of many of these control systems, combined with more recent integration with corporate networks, had resulted in higher risks that had not always been recognised and tested by the entities themselves. Security controls did not sufficiently protect them from internal or external information technology-related attacks. Information security is like a chain—it is only as strong as the weakest link. All entities were susceptible to security breaches or hacking attacks because of weaknesses in processes and controls.

At the time of our testing, attacks could disrupt water and wastewater treatment services. They could also disrupt other services that relied on the entities' information technology environments. There was a risk to public health and appreciable economic loss in terms of lost productivity, not only to water service providers but also to citizens and businesses. A sewage spill could also have a significant impact on the environment.

We acknowledge the efforts of the critical infrastructure owners since our testing to mitigate the risk of security incidents, including cyber attacks, on their systems to minimise the impact of such events.

All entities we audited had the capability to respond to information security incidents if they detected them. However, they were not well prepared to respond to cyber attacks. They had not planned or tested their response and recovery from a malicious or cyber incident. These can occur without notice and can affect availability and integrity of multiple systems.

The entities audited reported that they could operate smaller plants or parts of their larger water treatment plants manually in the event of disruption to computer systems, but they had not demonstrated this capability. Only one entity had documented its manual operating procedures, and none had ever tested running their whole plants manually. This places a high reliance on individual knowledge, experience and physical presence to continue water services in the event of an attack.

The results of this audit serve as a timely reminder for any public sector entity managing critical infrastructure. Entities should assess and strengthen defences to protect their systems from information technology and cyber threats, and ensure that manual operation of critical infrastructure is documented and well tested.

Audit findings

The entities we audited needed to improve their processes for managing information technology risks and business continuity planning for water control systems.

Managing control system risks

Water service providers needed to:

- identify risks of information technology security breaches
- implement controls to protect their systems
- monitor and review the effectiveness of the controls.

While entities we audited have taken steps in recent years to improve their information technology security, the results of this audit shows that management needs to do more. The entities need to do more in terms of oversight, leadership, and direction.

- Roles and responsibilities—several Queensland Government departments deal with counter-terrorism and response, but no central agency is responsible for supporting critical water infrastructure owners to protect these systems from security events resulting from information technology risks. The entities we audited understand they are accountable for protecting these systems from adverse events. They have established teams to manage corporate systems and water control systems. But they have not clearly defined roles and responsibilities, or held individuals accountable for their respective control environments.
- Security of critical infrastructure guidelines—the Australian Government guidelines for protecting critical infrastructure systems require the state government to assist critical infrastructure owners to implement security controls. However, Queensland has not yet established this assistance for water control systems.
- Identifying security risks—entities were not aware of some of the security risks for water control systems that related to information technology. This is because they did not critically assess each of the assets relating to water control systems and the need to protect them from physical and technical security breaches.
- Designing network controls—entities did not design their networks to provide adequate protection for control systems. They did not have adequate controls to secure the servers and workstations that connect users with the control systems. We understand that management cannot always keep water control systems up to date with technical controls, due to operational reasons and costs. However, we expect that entities will assess the risk of not implementing network security controls that compensate for vulnerabilities within water control systems.

- Communication—all entities have processes for obtaining and communicating relevant information about the security of information technology. However, they have not developed key performance indicators to measure the improvement in their security. In addition, the entities can improve their communication to staff about how to respond to security risks and issues.
- Security reviews—all entities have undertaken security reviews and penetration tests (tests of a computer system to find vulnerabilities that an attacker could exploit). However, they did not promptly address all the security issues raised by those reviews and tests. They limited the scope of penetration tests to cover mainly corporate networks and business systems—they did not include water control systems as targets for penetration tests.

Continuity of water systems

We assessed the ability of the entities to respond to, and fully recover from, security breaches relating to water control systems.

While all entities we audited have business continuity and resilience programs, they need to extend these to include all components of water control systems. None of the entities has comprehensive end-to-end processes for responding to a major security incident that would result in multiple systems failure.

All entities have disaster recovery plans for information technology and business continuity plans that they can invoke in the event of information technology systems failure. Both the information technology and operational technology teams know their components of the systems well and can respond to specific system outages in their own area. However, none of the entities has integrated information technology disaster recovery plans for all their information technology systems, including systems that external service providers may manage.

All entities advised that they could manually operate their smaller plants or parts of the larger drinking water and wastewater plants, if required. This would be a challenging task, depending on the skills, experience, and availability of critical staff. Therefore, all the entities need to ensure they are continually training staff and maintaining on-site manuals for individual components of water infrastructure. We note that each entity operates small sections of the plants manually during regular maintenance.

Recommendations

We recommend that the Department of Energy and Water Supply:

1. integrate information technology risks and cyber threats into the existing risk management framework for drinking water services and in the Queensland water and sewage service provider performance reports. (Chapter 2)
2. facilitate information sharing about adopting standards for securing information technology amongst entities that manage water control systems. (Chapter 2)

We recommend that the entities we audited:

3. improve oversight, identification and monitoring of information technology risks and cyber threats to water control systems. (Chapter 2)

   This should include:

   - clearly articulating and assigning roles and responsibilities for all parties, including any external service providers in securing the systems
   - maintaining a complete and up-to-date list of assets for water control systems and assessing the risk exposure of each asset
   - developing and implementing a security plan for water control systems based on risk assessments
   - implementing appropriate user access and authentication policies
   - using a phased approach to implementing the Australian Government's ’essential eight’ security controls based on each entity's risk assessment
   - establishing performance indicators for security and periodically testing these controls to monitor the maturity and strength of defences built into the information technology control environment
   - improving understanding of how to manage information technology risks and how they relate to other forms of operational risks.

4. establish enterprise-wide incident response plans, business continuity, and disaster recovery processes for information technology. (Chapter 3)

   This should include:

   - testing the capability to respond to wide-scale information technology security incidents either through scenario testing or through desktop exercises
   - training staff to identify, assess, and have a coordinated response to information technology security breaches
   - adopting appropriate business continuity plans that include processes for reporting incidents to stakeholders and building on lessons learned
   - updating and testing information technology disaster recovery and business continuity plans to include processes to recover from a wide-scale information technology security breach
   - considering the impact of multiple system failures on business continuity planning and how entities can operate water and wastewater plants manually, if required.

Reference to comments

In accordance with section 64 of the *Auditor-General Act 2009,* we provided a copy of this report to the entities we audited. The entities have accepted all our recommendations.

We received comments from the Minister for Main Roads, Road Safety and Ports and Minister for Energy, Biofuels and Water Supply; the Department of Energy and Water Supply; and the Department of the Premier and Cabinet. Their responses are in Appendix A.

Report structure

Chapter	
Chapter 1	provides the background to the audit and the context needed to understand the audit findings and conclusions.
Chapter 2	examines whether water service providers have established effective security processes and controls for managing information technology risks.
Chapter 3	assesses whether water service providers have the capability to detect, respond and recover in the event of an attack.
Appendices	Appendix A contains responses received from agencies Appendix B describes the audit methodology Appendix C contains The Australian Signals Directorate—essential eight controls Appendix D explains information technology security assessments.

Report cost

This audit report cost $350 000 to produce.

1. Context

Queensland's water service providers protect the quality of drinking water by operating treatment plants that remove contaminants from the water. Some water service providers also treat and dispose of wastewater.

Because of the critical importance of clean drinking water to the community, it is vital that water service providers identify and manage the risks associated with this infrastructure. Entities cannot always prevent attackers from attempting to break into these systems, but they can strengthen their systems with appropriate controls to detect and recover from breaches.

Water service providers in Queensland

Water service providers monitor and control water transport, treatment and distribution. These include:

- the water distribution network for drinking water, reservoirs, and pump stations
- the collection and treatment of wastewater.

Water service providers in Queensland include:

- bulk water service providers and water authorities (Seqwater and Sunwater)
- drinking water service providers (primarily local governments).

Figure 1A describes the roles of these providers.

Figure 1A
Roles of water service providers

Entity	Roles
Queensland Bulk Water Supply Authority (trading as Seqwater)	sells and distributes bulk water to the following entities for South East Queensland: ▪ Queensland Urban Utilities covers Brisbane, Ipswich, Lockyer Valley, Scenic Rim, and Somerset ▪ Unitywater covers Sunshine Coast and Moreton Bay ▪ City of Gold Coast, Logan City Council, and Redland City Council.
Sunwater	sells and distributes bulk water to entities outside South East Queensland.
Local governments	sell and distribute water to households and manage wastewater.

Source: Queensland Audit Office.

Water control systems

Over 50 years ago, operators controlled water infrastructures manually—people walked around each facility, turning pumps on and off. Supervisory Control and Data Acquisition systems were first introduced in the 1960s to monitor and control water infrastructure remotely. In this report, we refer to Supervisory Control and Data Acquisition systems as water control systems.

Today, new technologies enable the systems to automate processes, collect and store information, produce analytics, and report real-time operational data. Further advances in wireless and digitally connected systems enable operators to access multiple sites remotely through the internet on any device, including a mobile phone. The entities we audited use water control systems to enable operators and facility personnel to monitor and control the water treatment plants locally and remotely.

Threats to water control systems

Attackers have been known to target water control systems to endanger public health and safety. This has resulted in overflows of untreated sewage, reductions in water pressure, or shutdowns in the distribution of water.

Water service providers sometimes connect their control systems to other networks and the internet. The risk of unauthorised access increases when systems are connected to other networks that may not be secure. However, security breaches can also occur when the operators do not connect the control systems to other networks. These breaches can occur through social engineering techniques and/or distributing malicious software (malware) via portable (USB) drives.

Examples of reported security incidents affecting control systems include the following:

- In April 2017, someone breached radio signals to trigger all emergency alarm systems used by the City of Dallas for tornado warnings and other emergencies. This person kept the alarms in action for 95 minutes.
- In March 2016, Verizon's security research reported the hacking of an unnamed water processing plant through unpatched web vulnerabilities in its internet-facing customer payment portal.
- In December 2015, there were attacks against three Ukrainian electrical distribution sub-stations where destructive malware was used in a broad and sophisticated cyber attack. This attack resulted in approximately 225 000 customers losing power for three hours.
- In August 2013, a security research company in the United States created a mock water utility system and received 74 security attacks from more than 16 countries. Ten of them were able to take complete control of the mock system.
- In 2011, infiltration of a water treatment and delivery plant in the US resulted in damage to a water pump through manipulation of water control systems.
- In 2010, an Iranian nuclear facility was infected with Stuxnet. Stuxnet is a malware detected in control systems running on Microsoft Windows. It had entered the facility’s systems through an infected USB drive. According to published reports, Stuxnet ruined almost one fifth of Iran's nuclear centrifuges.
- In 2000, a security breach caused sewage overflow in Maroochy Shire. This incident was an act of revenge from a contractor who implemented the system. He changed the system control remotely causing approximately 800,000 litres of raw sewage to overflow into local rivers and parks.

Responsibilities for security of water systems

Several Australian Government entities play a role in setting guidelines and strategies for securing critical infrastructure, and assisting critical infrastructure owners when a security breach occurs. Water service providers own critical water infrastructure and are responsible for securing their own water assets.

Australian Government

Nationally, CERT Australia—the Computer Emergency Response Team—and the Australian Signals Directorate play advisory roles for the water service providers. CERT Australia advises on cybersecurity threats to owners and operators of Australia's critical infrastructure. The Australian Signals Directorate provides advice to mitigate targeted cyber or information technology intrusions. The Australian Signals Directorate 'essential eight' are well-regarded strategies for preventing up to 85 per cent of cyber security intrusions and are mandatory for the Australian Government.

Both CERT Australia and Australian Signals Directorate are partner agencies of the Australian Cybersecurity Centre. The Australian Government established the Australian Cybersecurity Centre in 2014 to combine cybersecurity capabilities across Australian governments.

In January 2017, the Australian Government established the Critical Infrastructure Centre to provide a coordinated approach to securing critical infrastructure. This centre also provides security advice to government about foreign-owned critical infrastructure. This is a new unit and is currently establishing its roles and approach to carry out its functions.

State government

At the state level, the Department of Energy and Water Supply regulates the water service providers' compliance with the *Water Supply (Safety and Reliability) Act 2008*. The safety of water supply in the legislation relates to making sure there is a supply of water, rather than providing information technology security. The legislation does not require the Department of Energy and Water Supply to provide guidance on information technology security for critical water infrastructure.

The responsibilities for setting information technology strategy and policies for Queensland Government departments sit with the Queensland Government Chief Information Officer. In February 2016, the Queensland Government Chief Information Officer also established a cybersecurity unit to expand whole-of-government protection against cyber threats.

However, the Queensland Government Chief Information Officer is not responsible for developing security policies, standards, or guidelines for critical infrastructure systems.

Water service providers

Each entity that owns critical water infrastructure is responsible for securing its own water assets. The entities we audited generally had two teams responsible for the security of water systems—information technology services and water operations. Each of the teams is responsible for securing its respective part of the water and wastewater systems. Figure1B details the roles and responsibilities of these teams.

Figure 1B
Water service provider responsibilities for securing water control systems by business unit

Business unit	Roles
Information technology services	Responsible for the information technology and security of computers, storage, and networking devices. This team may report to the chief financial officer, the general manager responsible for assets, or the director for organisational services.
Water operations	Responsible for installing and maintaining hardware and software for the water control systems and field devices. These are also known as operational technology. This team typically reports to the general manager of water operations.

Source: Queensland Audit Office.

Security standards and good practice

Queensland legislation does not define standards for the security of control systems.

However, the Information Technology Security Expert Advisory Group of the Australian Commonwealth Government's Trusted Information Sharing Network for Critical Infrastructure Resilience has developed some good practice guides. The following guides are available for use by operators of national critical infrastructure:

- *Generic Supervisory Control and Data Acquisition Risk Management Framework*
- *Supervisory Control and Data Acquisition Architecture Principles*
- *Knowing Your Supervisory Control and Data Acquisition Network*
- *Hardening of Supervisory Control and Data Acquisition ICT Systems*
- *Implementing Gateways*
- *Monitoring of Supervisory Control and Data Acquisition Networks.*

In addition to the Trusted Information Sharing Network guidelines, the Australian Signals Directorate published 35 strategies to mitigate targeted cyber intrusions. The Australian Signals Directorate also mandated the 'essential eight' from these strategies for Australian Commonwealth Government agencies. The Australian Signals Directorate has made these mandatory, based on research showing that these mitigate 85 per cent of the cyber intrusions investigated by the Australian Signals Directorate.

Many international standards also outline good practices for securing systems of value. These include:

- National Institute of Standards and Technology 2014, *Framework for improving critical infrastructure cybersecurity*
- The Committee of Sponsoring organisations of the Treadway Commission*, Internal Control—Integrated Framework*
- AS/NZS ISO 31000:2009, *Risk management—Principles and guidelines*
- ISO/IEC 27001:2013, *Information technology—Security techniques—Information security management systems—Requirements*
- ISO/IEC 27005:2012, *Information technology—Security techniques—Information security risk management*
- ISO/IEC 27031:2011, *Information technology—Security techniques—Guidelines for information and communications technology readiness for business continuity*
- National Institute of Standards and Technology 2008, *Technical guide to information security testing and assessment*
- Australian Signals Directorate, Australian Cyber Security Centre 2017*, Strategies to Mitigate Cyber Security Incidents*
- The 2015 *National Guidelines for Protecting Critical Infrastructure from Terrorism*—focuses on potential disruptions of infrastructure systems by terrorists
- The Critical Infrastructure Resilience Policy and Strategy
- The National Strategy for Disaster Resilience—provides a wider context for the work of the critical infrastructure centre
- AS/NZS 5050:2010, *Business continuity—Managing disruption-related risks.*

2. Managing control system risks

Chapter in brief

Water infrastructure owners need to actively protect control systems so they can operate as intended. In an effective control environment, management:

- sets an appropriate tone at the top about the importance of security and controls
- is clear about governance, roles and responsibilities
- establishes appropriate security policies and procedures
- develops robust risk management processes
- designs, implements, and monitors controls.

In this chapter, we assess the governance and oversight processes that the owners of water control systems use to manage information technology risks. We also assess whether the entities we audited have designed network architecture and implemented adequate security controls across the information technology environment to protect water control systems.

Main findings

- While several Queensland Government departments deal with counter-terrorism and response, no central agency is responsible for supporting critical water infrastructure owners to protect these systems from security events resulting from information technology risks.
- All entities we audited have appropriate information security policies, procedures, and organisation structures to manage water control systems. However, they have not clearly defined the roles and responsibilities for securing the information technology systems.
- All entities we audited have governance structures and frameworks in place to manage risks. However, they have not identified information technology security risks relating to all aspects of water control systems.
- All entities we audited need to strengthen the design of their information technology networks and tighten the controls relating to physical security, user access management and technical configuration of network devices, workstations, and servers.
- None of the entities audited had security plans or established security requirements for their water control systems. As a result, these entities did not measure and monitor key performance indicators relating to the strength of their controls.
- Each entity had staff awareness and training for security of information technology. However, none of the entities audited had comprehensive programs to educate staff about ways to prevent an intruder physically entering facilities and gaining access to systems.
- All entities audited undertook internal audits and security assessments. However, they did not always address risks promptly. In addition, there was inadequate monitoring of system activities to detect any covert misuse of these systems.

Introduction

The infrastructure for water supply consists of elements that pump, divert, transport, store, treat, and deliver safe drinking water. Entities that also manage wastewater have infrastructure to collect, pump, treat, and dispose of wastewater. These functions rely on industrial control systems that monitor and control the treatment, supply, distribution and, in the case of wastewater, appropriate disposal.

Entities are increasingly connecting control systems to corporate computer networks and to the internet. This opens them to internal and external threats. Therefore, critical infrastructure owners need to have a robust control environment in place to protect these systems so that they can continue to operate as intended.

Implementing optimal level of security requires owners of water control systems to:

- establish a control environment with management setting the tone from the top, with security policies, procedures and organisational structures and holding individuals accountable for their control environment
- implement risk management frameworks that enable management to identify risks and to develop a security plan for water control systems
- build security controls into the design of the information technology networks and computer systems to protect them from both internal and external unauthorised users
- obtain, use, and communicate relevant information on how the control environment functions
- monitor control activities and communicate control deficiencies for corrective actions.

In this chapter, we assess whether the water control systems we audited are secure and whether the owners of water control systems have adequate oversight in managing information technology risks and cyber threats. In addition, we examine and test entities' computer networks and the technical and process controls.

Audit conclusions

The water control systems we audited were not as secure as they should have been. This is because these entities did not identify some of the key risks and, therefore, did not have control processes in place to mitigate those risks.

While each entity had appropriate security policies, procedures and organisational structures in place, none of the entities has developed security plans for their water control systems. In addition, there is no state level support for the owners of water control systems about how to manage and report information technology risks.

Entities we audited can improve the way they are designing their networks or implementing controls to strengthen their defences against harmful attacks. In addition, the entities we audited did not always recognise the importance of the physical security of their offices when designing the security of their information systems.

One of the entities needs significant improvements in all areas of the control activities, from physical security of office buildings, to the design of the information technology systems and their connectivity to the critical infrastructure systems. The other entities had done work to strengthen their information technology security over recent years. All entities we audited had either planned or were planning projects that would address information technology security risks.

It is unlikely, at the time of testing, that the entities we audited would have promptly detected unauthorised access or covert misuse of the water control system because they did not always monitor activities within the computer network. Since our audit, these entities have reported to us that they have taken steps to improve their processes to monitor security incidents.

Establishing the control environment

All critical infrastructure owners we audited have established elements of a control environment, with appropriate information security policies and procedures, organisation structures, and management oversight committees.

Whole-of-government guidance and monitoring

There is a wide policy platform for information security across government and individual public sector entities. According to the Australian national guidelines for protecting critical infrastructure, state and territory governments and their agencies have a role in assisting owners of critical infrastructure with prevention, response, and recovery planning in their jurisdictions. It also states that critical infrastructure owners are responsible and accountable for protecting these systems.

Several departments, business units, and committees within Queensland Government deal with counter-terrorism and response activities. However, no central agency is responsible for setting policy and guidelines to protect critical infrastructure assets from security events resulting from information technology risks. The Australian Government has guidance material for protecting critical infrastructure, but the water service providers we audited are either not aware of, or are not implementing, key aspects of those guidelines.

The Department of Energy and Water Supply (DEWS) administers the *Water Supply (Safety and Reliability) Act 2008* and requires water service providers to develop a management plan for water quality. Within this plan, water service providers document hazards and hazardous events that may affect the quality of water.

DEWS provides a definition of a hazard in their guidelines. It has defined a hazard as ‘a biological, chemical, physical or radiological agent that has potential to cause harm’. This definition does not include information technology or cyber threats that have the potential to affect the water control systems and cause them to stop operating as intended. As a result, DEWS does not provide guidance on how to secure critical infrastructure. Neither does DEWS require water service providers to implement security measures to protect the water control systems from information technology risks or cyber threats.

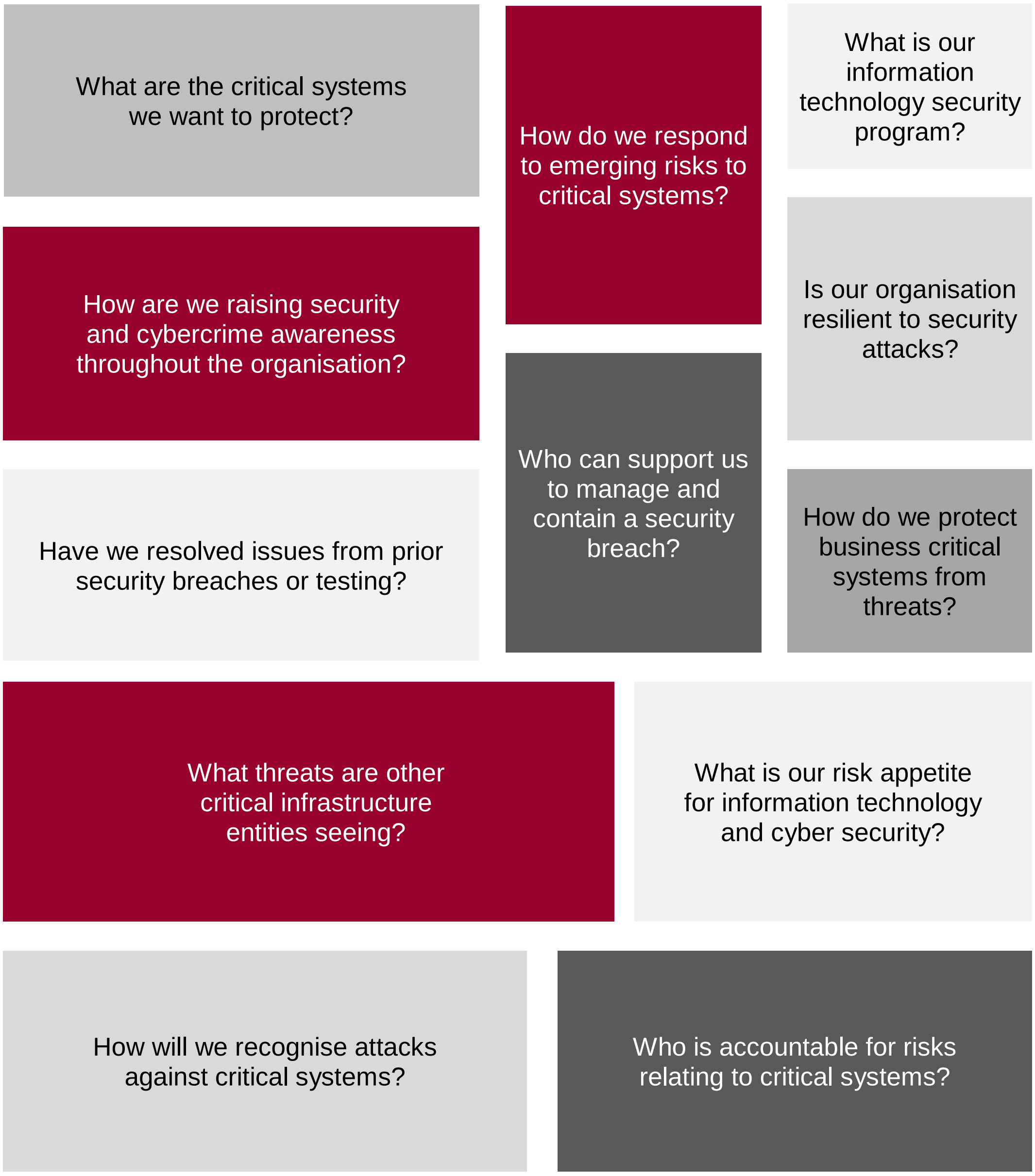
As the regulator for multiple critical water infrastructure entities, DEWS is in a good position to monitor that water service providers manage information technology risks. In addition, DEWS can encourage owners of water control systems to use standards and guidelines available nationally and internationally to design and implement security for their information technology environment.

Management oversight—owners of critical water infrastructure

A survey of six hundred corporate board directors and professionals from the National Association of Corporate Directors (NACD) in December 2016, reported that only 19 per cent believe their boards have a high level of understanding of cyber security risks. To improve the maturity of oversight for information technology risks, executive management needs to prioritise and consider information technology risks at an enterprise level.

In addition, those charged with governance need to seek answers about key aspects of information technology security risks that can have a significant impact on the entity. Figure 2A shows some of the key questions for senior management to consider.

Figure 2A
Key questions for senior management



What are the critical systems we want to protect?

How do we respond to emerging risks to critical systems?

What is our information technology security program?

How are we raising security and cybercrime awareness throughout the organisation?

Is our organisation resilient to security attacks?

Who can support us to manage and contain a security breach?

Have we resolved issues from prior security breaches or testing?

How do we protect business critical systems from threats?

What threats are other critical infrastructure entities seeing?

What is our risk appetite for information technology and cyber security?

How will we recognise attacks against critical systems?

Who is accountable for risks relating to critical systems?

Source: Queensland Audit Office.

Information security policies

While each of the entities had appropriate information security policies and procedures in place, we identified improvement opportunities for the entities in the following areas:

- One entity did not define security requirements for water control systems within their organisational level policies.
- One entity did not have service provider roles included in approved security policies.
- One entity did not comply with key aspects of its security policy to secure and monitor its water control systems.

Organisation structure

At each of the entities we audited, two teams had to work together to secure the water control systems: the information services team and the operations team.

Generally, operations teams manage the water control systems and information technology services teams manage the corporate networks and internet. This arrangement, involving separate teams to manage information technology and operational technology, is common for control systems. However, there is a trend for information technology and operational technology to converge and integrate to optimise business processes, and that has implications for how teams work together.

As the technologies converge, the teams need to collaborate and establish shared standards and processes to manage both information technology and operational technology. Lack of integration of the two teams increases the risk to the security of control systems. We found some indications of this risk materialising in all the entities we audited.

We found that:

- Those charged with governance have not clearly articulated the roles and responsibilities of the two teams in designing and implementing security for control systems.
- Operations teams have not documented the requirements for the security and availability of the corporate networks that are essential for protecting and operating control systems.
- Information technology teams do not always understand the impact of the corporate network on the security and availability of the water control systems.

One of the ways to improve the understanding of each team's roles is to document the information technology and operational technology environments and their respective roles and responsibilities. Those charged with governance need to notice the difference in the cultures of both teams and encourage collaboration and the mutual understanding of risks and their implications.

Identifying and assessing information technology risks

Risk management is the ongoing process of identifying, assessing and responding to risk. Entities we audited have identified several strategic level risks. However, two entities have not explicitly included information technology risks or cyber threats within their strategic risk registers. Therefore, they have not assessed the strategic impact of these risks materialising. One entity included cyber security risk in the strategic risk register but had not correctly recorded its own assessment of the maturity of the mitigating controls.

While these entities covered some of the risk areas for their corporate and business systems, they did not analyse those risks for water control systems. Figure 2B highlights examples of the areas of control that entities did not always apply to water control systems.

Figure 2B
Examples of gaps in risk treatments for water control systems

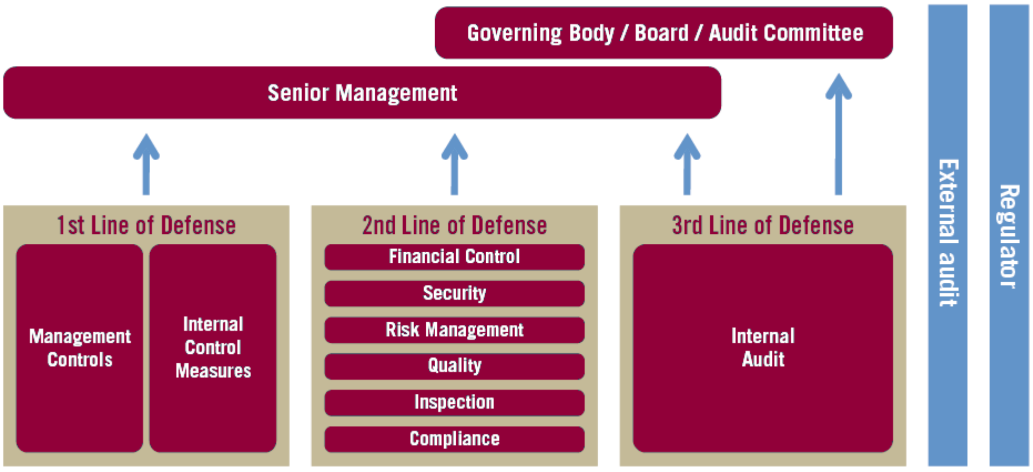
Areas of controls	Risk treatments	Gap in risk treatment for water control system
Governance	ICT governance frameworks are in place and consist of policies and procedures for information technology security.	Some entities did not define security requirements for water control systems. As a result, they did not apply information technology policies and procedures to water control systems.
Information security plan	Align security strategy with business strategic requirements.	ICT security strategy for water control systems is either in draft form, or does not exist. Critical systems and threats are not always documented. This limits the ability to formulate effective information security plans.
User access reviews	Perform user access review regularly on finance systems. This is to determine validity of users and appropriateness of access level.	Entities do not always review user access levels for water control systems.
Information classification controls	Review corporate information systems classification and realign controls.	Entities do not always apply information classification controls to critical infrastructure systems.

Note: ICT—information and communications technology.

Source: Queensland Audit Office.

To understand why all the entities we audited had gaps in identifying risks for water control systems, we mapped their processes to the Institute of Internal Auditors' risk management model. Many organisations use this model effectively as an integrated approach for managing risks. It constitutes three lines of defence as illustrated in Figure 2C.

Figure 2C
Three lines of defence model in risk management



Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

Source: The IIA position paper: The three lines of defence in effective risk management and control, January 2013.

We found that all entities we audited could improve their practices of identifying and assessing risks in all three lines of defence.

Identifying and assessing risks as part of the first line of defence

As a first step, the entities need to identify their assets that connect with water control systems, and then to determine the threats and vulnerabilities related to those assets. These are key inputs in them assessing the impact and likelihood of security risks for each combination of assets. This process helps managers to prioritise and focus on the most important risks.

The next step is to design and implement only those controls that are required because of the risks. This also means that management cannot exclude some controls or put them on long-term plans simply because they are not convenient or are too costly.

If management decides not to implement some controls over a period, then they need to evaluate the risks they are accepting until they implement the controls. As managers implement controls to mitigate risks, they are implementing their first line of defence.

Identifying and assessing risks as part of second and third lines of defence

The entities we audited engaged external consultants as part of their second line of defence to review and provide recommendations to management for mitigating some of the risks. However, the entities did not promptly address some of the key risks that security reviews and audits identified. This indicates that entities need to improve their understanding of the consequences if security risks materialise. All entities have internal audits as their third line of defence to identify information technology risks.

Implementing control activities for information security

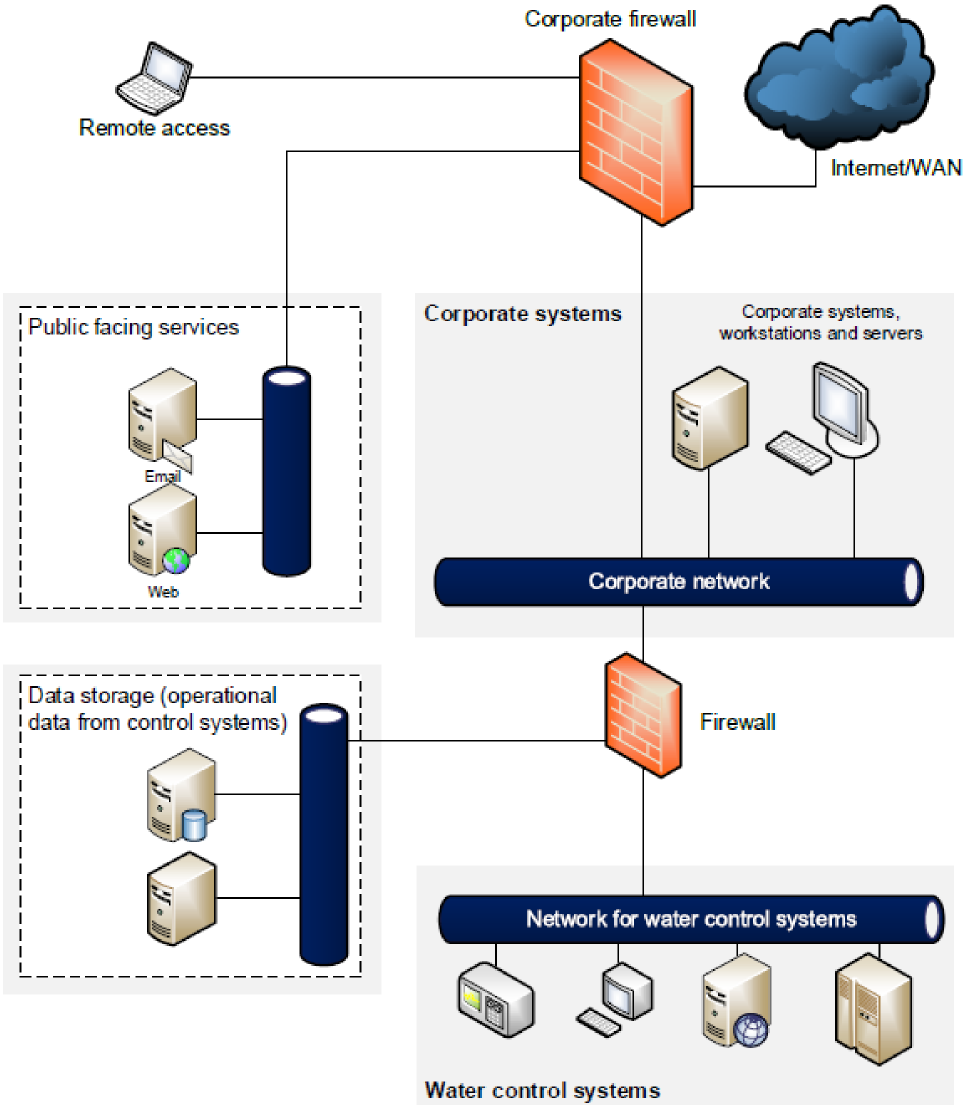
A sound security design within the computer network architecture is a crucial control. Entities can implement and configure security devices at various points within the network. In addition, entities can implement process controls, such as physical security and user access management, as well as technical controls to protect their servers and workstations from unauthorised access.

Information technology network architecture

Entities had not designed and implemented some of the network access controls effectively. This resulted in varying levels of separation within their corporate computer systems from the water control systems. Therefore, a security breach of their corporate network could potentially breach the security of the water control systems.

The Australian Government's Trusted Information Sharing Network guidelines recommend separate zones for control systems. In Figure 2D we illustrate how entities can organise their information technology networks to achieve this type of separation. It shows that entities can use security devices, such as firewalls, to separate various networks within the organisation. This illustration is a conceptual view of an information technology environment. Critical infrastructure owners need to assess their own environments and determine controls to suit their business.

Figure 2D
Example of network separation



Source: adapted from TISN Guidelines.

For the network design in Figure 2D to operate effectively, technical security controls within the devices on the network need to be implemented, as well as those connecting with the network.

Figure 2E highlights some of the essential practices that entities need to assess when designing controls for information technology networks. These can increase the effectiveness of separating the corporate network from control systems.

Figure 2E
Good practices—security of the information technology network

Controls that increase the effectiveness of information technology network security
Implement network segmentation to keep the control systems separate from other networks, including corporate systems and the internet. If a rule is relaxed for purposes of fixing issues, promptly tighten this after use.
Diligently manage user access controls, and regularly review and update network security.
Implement network access controls and system logging to detect unauthorised access and transfers of data from internal networks.
Use secure remote access methods and ensure external connections do not have full access to critical infrastructure systems.
Record logs of all connections to the control system networks. The lack of logs of network connections makes it harder, slower, and more expensive to investigate a security breach.
Use strong passwords, change default passwords and use more than two pieces of information to verify user identity, i.e. user name, password, and a security token for remote access.
Only enable network connections in public areas or meeting rooms when required.
Encrypt data that travels through the network. Connections without encryption can help a hacker to move from a basic compromise on the computer network to full access to key systems.
Enable the encryption services available within the radio communications devices.
Maintain awareness of vulnerabilities, implement security per vendor recommendations and decommission end-of-life systems as a priority.

Source: Queensland Audit Office.

Process and technical controls

While entities we audited had implemented security controls, the controls were not sufficient to protect water control systems from unauthorised access or targeted attacks. In this section, we discuss the strength of defences in the areas of physical security, access controls, servers and workstations, and staff awareness and training.

- **Physical security—**all entities audited had implemented different levels of physical security at their offices, public facilities, and water treatment sites. In conducting our audit tests, we tested security by attempting to gain unauthorised physical access into buildings. Not all offices had adequate controls to stop a member of the public from gaining access to the offices. As a result, we faced varying degrees of success in bypassing the physical security barriers to reach computers at each of the entities.

  Staff did not challenge people within the offices without a visitor or staff identification. We were also able to circumvent most procedural controls to gain access into buildings. Delays in detecting unauthorised physical access can increase the amount of damage done by intruders, and therefore the cost to recover from a physical security breach.

- **Access controls—**all entities we audited have developed access controls for water control systems but these are only partially effective. For example, entities used generic user identifiers and former staff still had access at the time of the audit. Some systems did not have strong password controls. These issues reduce the assurance that only authorised people can access the water processing interfaces.

- **Servers and workstations—**while all entities audited had implemented several security controls, they did not implement some of the controls within their servers and workstations.

  Entities had informal processes to assess the risks from security flaws in the software of the water control systems. They did not have risk-based plans to continuously review these and keep the software up to date with the recommendations of the software vendor.

  Controls for managing malicious software were ineffective as some computers had out-of-date software, while others did not have anti-virus installed. Where controls for malicious software are not effective, there is an increased risk of outages or the unauthorised manipulation of systems and related processes.

  Entities did not always address the security risks of lost or mobile workstations. We also found that entities did not enable encryption or implemented controls to make sure that users could only access authorised internet sites from some unsupervised computers. Lack of these technical controls increases the risk of unauthorised access to systems and data.

The Australian Signals Directorate recommends that entities implement a package of the essential eight controls as a baseline; this will make it harder for attackers to compromise systems. The Australian Signals Directorate's essential eight are provided in Appendix C.

Monitoring control environment

Control reviews

All entities audited undertook internal audit assessments and engaged external consultants to review and report on their control environments for information technology. In addition, they undertook various methods to test the strength of their controls. This included penetration testing, which is the practice of testing a system to find vulnerabilities that an attacker could exploit.

However, none of the entities moved quickly to fix the issues or mitigate risks that these reviews identified. The entities either incorporated the results of the assessments into longer-term programs of work or adopted a piecemeal approach to address some of the findings. In addition, the entities could not demonstrate that they improved their control environments after each penetration test. This is mainly because senior management did not prioritise information technology security risks for water control systems. In addition, the entities did not adopt a holistic approach for evaluating the overall information technology environment. In Appendix D, we have outlined various methods that entities can consider when developing plans for evaluating their control environment for information technology.

In addition, these entities have some monitoring tools that alert information technology staff to unusual events. However, none of the entities have a clear policy for recording, retaining or protecting security-related event logs.

Some water control systems did not generate activity logs; some systems retained logs for one day; while others retained logs for a few hours. In addition, the entities did not always monitor access logs for user activities within the network. Therefore, it is unlikely these entities would have detected unauthorised access or covert misuse of water control systems.

Information security reporting

All entities we audited have established processes for reporting on information security controls to managers and governance bodies. Two of these entities had ongoing security programs and projects. However, none of these entities defined and implemented key performance indicators to measure improvements in their control environment as they implement risk mitigation strategies.

We also noted there is a risk that staff could unwittingly help a security breach to occur. While each entity had awareness programs for the security of information technology, they did not have effective programs to ensure staff members were aware of intruder threats from breaching physical security. If staff members are not careful, they can allow unauthorised persons to gain physical access to office buildings. The entities we audited did not train their staff to challenge those that are in their building facilities and do not display identification.

We conducted an email campaign requesting a random sample of users to provide us with their user identification and passwords. Although about 20 per cent of users clicked on the emails and we attained some credentials, the information technology teams were quick to identify and block malicious sources of emails. A sound communication program can reduce the risk of users clicking on malicious links in emails by increasing awareness of staff in good control practices

3. Continuity of water systems

Chapter in brief

The two main functions of water control systems at the entities audited are:

- operating treatment and distribution plants for water and wastewater
- monitoring drinking water quality.

Computer-based attacks or malicious software can affect these services. High profile events increase the likelihood of these types of attacks.

In case of an attack, entities managing water control systems must respond quickly and efficiently to minimise the amount of damage to water and wastewater facilities and services.

This chapter outlines the capabilities of the entities we audited to detect, respond, and recover from wide-scale security incidents related to information technology.

Main findings

- Water service providers audited have processes to control and regularly test drinking water quality. This means they can detect and start responding to water quality issues within a reasonable timeframe.
- These entities have documented response and disaster recovery plans for information technology. They have tested these plans. But these plans do not cover all components of water control systems. Nor do they cover how they will respond to wide-scale information technology security incidents that result in multiple system failures.
- These entities reported that they could run their smaller plants or parts of their larger water and wastewater plants manually should the need arise, but only one entity has documented the manual procedures. They have tested running sections of the plants manually during regular maintenance, but none of the entities has tested the process for running the whole plant manually.
- Not all entities conduct regular competency training for site staff to run the plants manually.

Introduction

Entities can plan to operate continuously by identifying likely disruptive scenarios—such as natural disasters, power failures or cyber threats—and create plans to manage the effects. These plans are called disaster recovery plans.

New, diverse and more damaging attacks are emerging in relation to computer systems. It is imperative that entities respond efficiently and effectively to minimise the amount of damage and cost that may result from such a disruptive event.

The Australian/New Zealand Standard AS/NZS 5050: 2010 *Business continuity—Managing disruption-related risk* recommends that organisations' plans should cover not only their initial response to the incident, but also the steps necessary to recover systems and return to normal operations. Regular testing and review of these plans is equally important to ensure that team members have the knowledge and skills necessary to recover systems as required. Entities need comprehensive disaster recovery plans to fully restore information systems after initial recovery from an attack.

In this chapter, we assess whether the entities we audited have systems and processes in place to detect, respond, and recover from security incidents relating to information technology.

Audit conclusions

All entities audited either have, or can access, the capability to respond to a breach of information security. To recover the water control systems, they depend on the capabilities and availability of their internal operations and technology teams and the vendors of the water control systems.

Their disaster recovery plans and testing do not cover all aspects of the water control systems. They fall short of providing assurance that they would be able to recover these systems within a timely manner. The plans do not include information on how they will identify, respond, and recover from a harmful incident involving the water control systems.

We acknowledge that some entities have used these plans to recover their systems after a natural disaster. However, they have not planned for a wide-scale security incident that can occur without notice and affects multiple computer systems at the same time. Nor do the plans consider the scenario where the entities need to operate the plants manually. While all entities audited have operated sections of a plant manually during maintenance, they have never tested running the whole plant manually. Only one entity has documentation to manage such an event.

Detecting water quality issues

It is likely that the entities we audited will detect issues with the quality of drinking water within a reasonable timeframe. This is because they control the quality of drinking water using two approaches. Firstly, the water service providers program the control systems to release the appropriate levels of chemicals, such as chlorine, into drinking water. Secondly, the entities perform chemical tests on the water outputs daily. In addition, there is a time lapse of at least one day before the treated water reaches households. This gives water service providers time to address any water quality issues that they detect.

One of the entities we audited leads the way in implementing innovative solutions to monitor the quality of drinking water. These innovations have the potential to improve the speed with which water service providers can detect changes in water quality. Case study 3A shows this.

Figure 3A
Case study on improving water quality monitoring

Innovation in monitoring water quality

The audited entity is improving the speed of detecting water quality issues by:

- collaborating with a university to define what the water is normally made up of in terms of various chemicals and compounds i.e. its baseline composition. The entity plans to compare the results of water testing performed daily during major events to determine whether there are changes in the concentration of known or unknown compounds
- implementing systems and processes that record the water distribution system through a geographical information system. The entity uses this system to analyse and display chlorine residuals to identify priority areas for the disinfection program
- implementing online water quality analysers to continuously monitor parameters such as pH, chlorine etc. to identify contamination in the drinking water

These projects have many potential benefits for efficient monitoring of water quality.

Source: Queensland Audit Office.

Responding to security incidents

Even when an entity has established a strong control environment, persistent attackers with advanced capabilities can breach security. For this reason, it is important to implement and test incident response plans. In addition, entities need to train staff to use the plans, so they have an agreed and coordinated approach for responding to incidents.

The entities we audited have developed documentation for emergency and incident management. They have also conducted some testing of their response capability. However, these entities have not:

- assessed the impact that a sustained information technology security incident would have on operations
- established processes on how information technology and water operations teams would coordinate their activities when responding to wide-scale information technology security breaches and major system outages
- documented the end-to-end processes and procedures for responding to information technology security incidents across information technology and operations teams
- trained staff to identify, assess and respond to information technology security breaches.

Recovering information systems

A disaster recovery plan for information technology is a set of procedures to recover from a computer systems failure. It includes the systems and the priority for restoring each one. It also includes a list of stakeholders and communication protocols in the event of a disaster.

While all entities have disaster recovery plans for their corporate systems, they do not include recovery of water control systems. Nor have the entities reviewed and updated their plans for disaster recovery, considering wide-scale computer security incidents. As a result, there is no assurance that the entities could restore a fully compromised water control system within a timeframe acceptable to the business.

The water operations teams are responsible for managing their own servers, workstations and control systems. These teams typically know their systems well and have previously responded to incidents related to their own environments. However, without documentation for the recovery of these systems, an effective recovery process will be difficult if teams with specific site knowledge are not available.

In addition, contracts with any external service providers for information technology did not always include:

- roles and responsibilities for the recovery of control systems that may be managed internally or by external service providers
- key performance indicators, such as, maximum acceptable outage and recovery time objectives for water control systems.

Manually operating water and wastewater treatment plants

The water treatment plants and pumps contain additional (redundant) systems, aimed at minimising downtime. In the event of a control systems failure, all entities audited reported to us that manual operation of the smaller plants is possible for a short period. The entities we audited have not determined the periods for which they can run the plants manually.

One of the entities believes that it can manually operate the larger wastewater treatment plants. While such an endeavour would be challenging, this entity believes it has the expertise and training to operate its plants manually. This is because this entity:

- conducts competency training for site staff
- maintains onsite manuals for individual system components.

While all entities audited have operated sections of a large plant manually during maintenance, they have never tested running the whole plant manually.

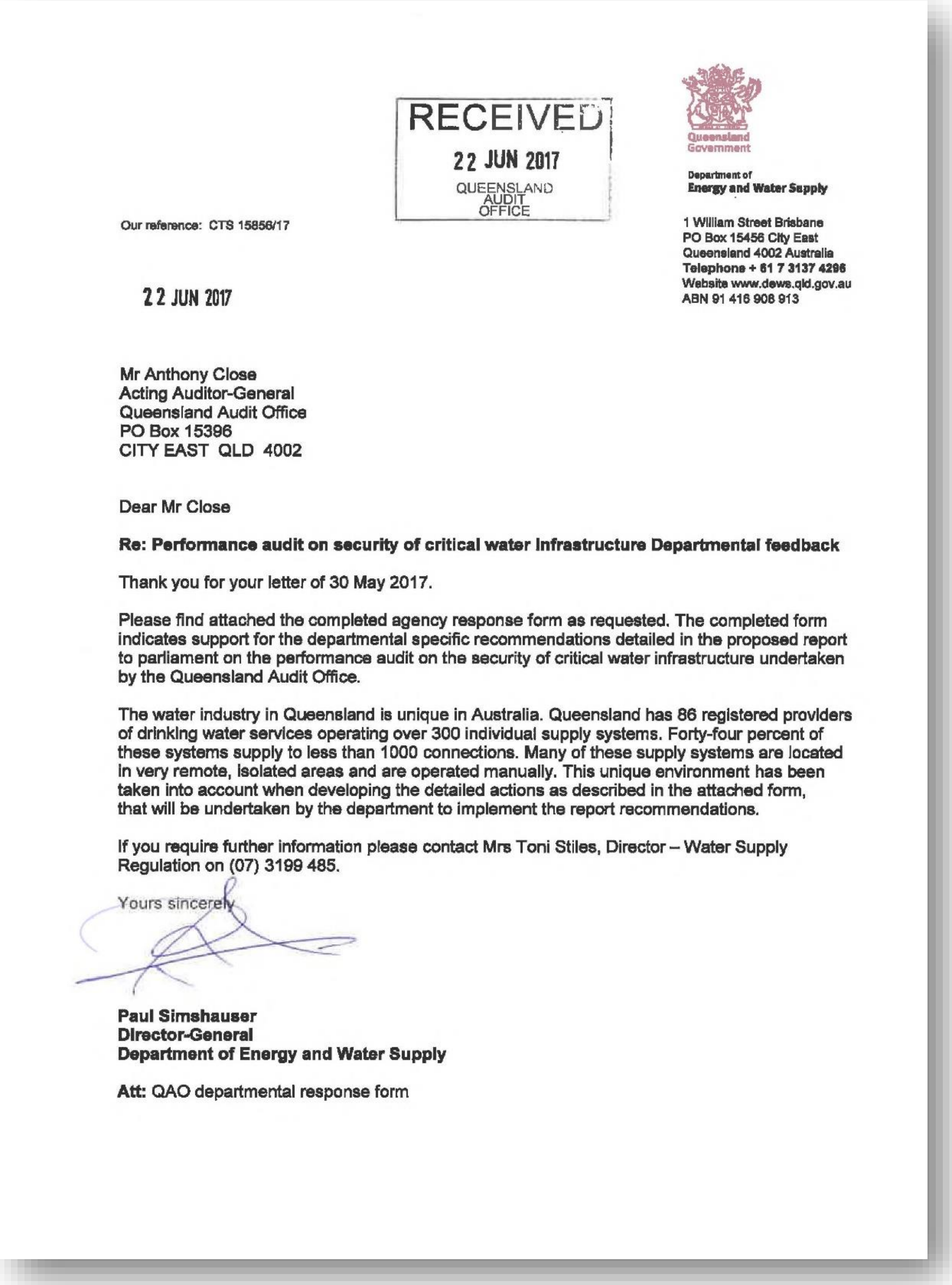
Appendices

Appendix A—Full responses from agencies

As mandated in Section 64 of the *Auditor-General Act 2009*, the Queensland Audit Office gave a copy of this report with a request for comments to the audited entities.

The head of these agencies are responsible for the accuracy, fairness and balance of their comments.

Comments received from Director-General, Department of Energy and Water Supply



Queensland Government

Department of
Energy and Water Supply

1 William Street Brisbane
PO Box 15456 City East
Queensland 4002 Australia
Telephone + 61 7 3137 4296
Website www.dews.qld.gov.au
ABN 91 416 908 913

Our reference: CTS 15856/17

22 JUN 2017

Mr Anthony Close
Acting Auditor-General
Queensland Audit Office
PO Box 15396
CITY EAST QLD 4002

Dear Mr Close

Re: Performance audit on security of critical water Infrastructure Departmental feedback

Thank you for your letter of 30 May 2017.

Please find attached the completed agency response form as requested. The completed form indicates support for the departmental specific recommendations detailed in the proposed report to parliament on the performance audit on the security of critical water infrastructure undertaken by the Queensland Audit Office.

The water industry in Queensland is unique in Australia. Queensland has 86 registered providers of drinking water services operating over 300 individual supply systems. Forty-four percent of these systems supply to less than 1000 connections. Many of these supply systems are located in very remote, isolated areas and are operated manually. This unique environment has been taken into account when developing the detailed actions as described in the attached form, that will be undertaken by the department to implement the report recommendations.

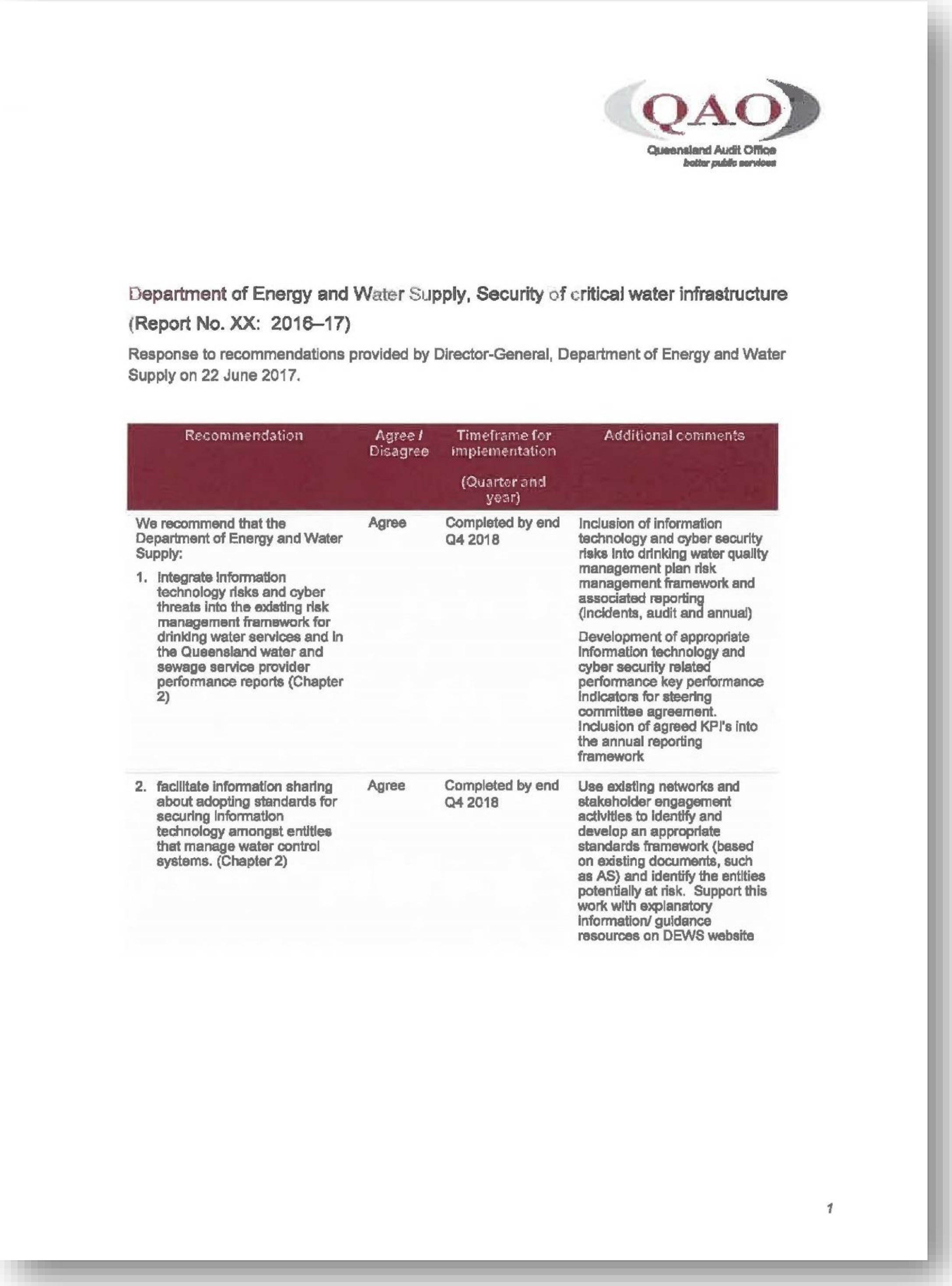
If you require further information please contact Mrs Toni Stiles, Director – Water Supply Regulation on (07) 3199 485.

Yours sincerely

Paul Simshauser
Director-General
Department of Energy and Water Supply

Att: QAO departmental response form

Responses to recommendations



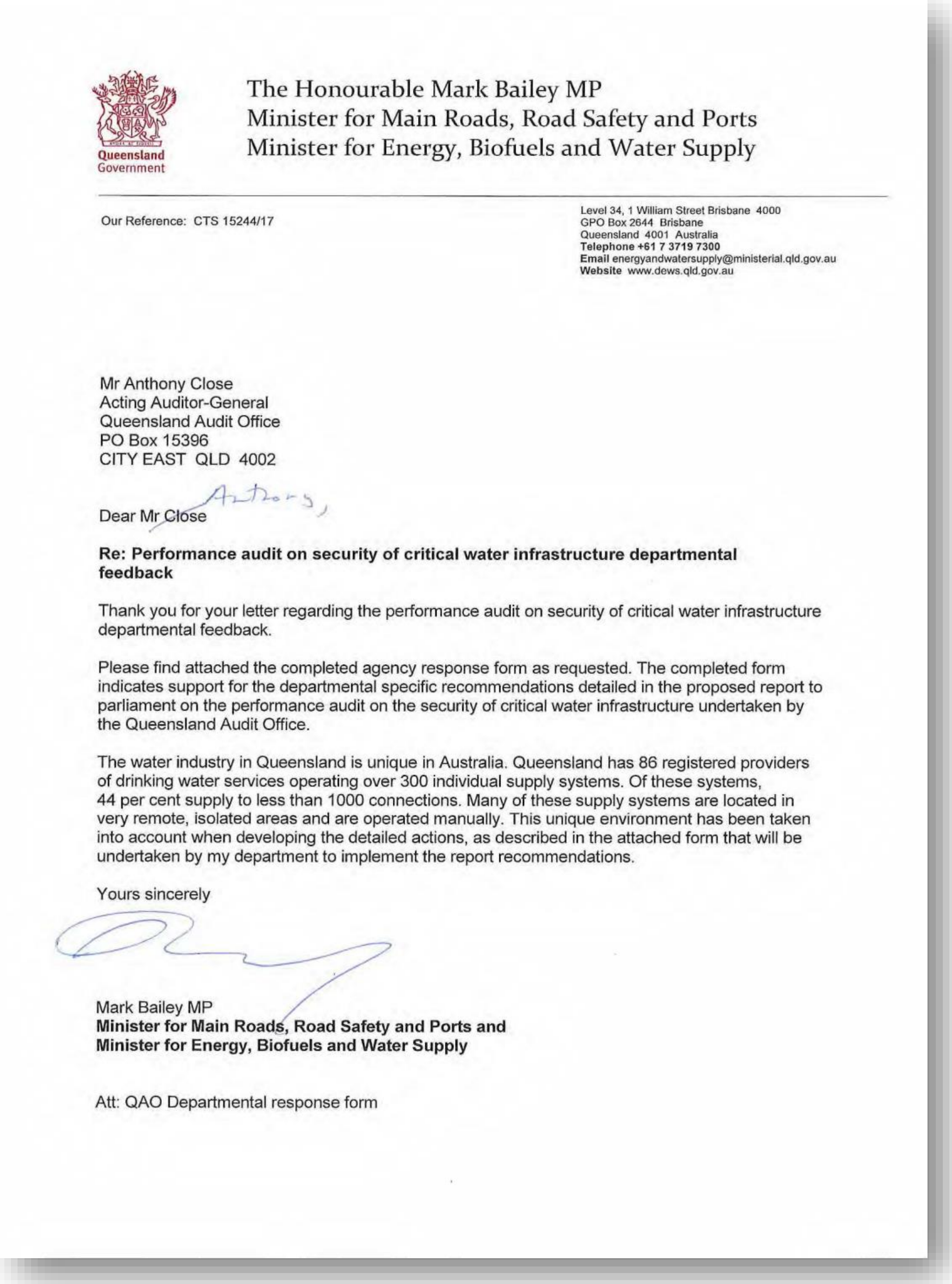
Department of Energy and Water Supply, Security of critical water infrastructure (Report No. XX: 2016–17)

Response to recommendations provided by Director-General, Department of Energy and Water Supply on 22 June 2017.

Recommendation	Agree / Disagree	Timeframe for implementation (Quarter and year)	Additional comments
We recommend that the Department of Energy and Water Supply: 1. integrate information technology risks and cyber threats into the existing risk management framework for drinking water services and in the Queensland water and sewage service provider performance reports (Chapter 2)	Agree	Completed by end Q4 2018	Inclusion of information technology and cyber security risks into drinking water quality management plan risk management framework and associated reporting (incidents, audit and annual) Development of appropriate information technology and cyber security related performance key performance indicators for steering committee agreement. Inclusion of agreed KPI's into the annual reporting framework
2. facilitate information sharing about adopting standards for securing information technology amongst entities that manage water control systems. (Chapter 2)	Agree	Completed by end Q4 2018	Use existing networks and stakeholder engagement activities to identify and develop an appropriate standards framework (based on existing documents, such as AS) and identify the entities potentially at risk. Support this work with explanatory information/ guidance resources on DEWS website

1

Comments received from the Minister for Main Roads, Road Safety and Ports, Minister for Energy, Biofuels and Water Supply



Queensland Government

The Honourable Mark Bailey MP
Minister for Main Roads, Road Safety and Ports
Minister for Energy, Biofuels and Water Supply

Our Reference: CTS 15244/17

Level 34, 1 William Street Brisbane 4000
GPO Box 2644 Brisbane
Queensland 4001 Australia
Telephone +61 7 3719 7300
Email energyandwatersupply@ministerial.qld.gov.au
Website www.dews.qld.gov.au

Mr Anthony Close
Acting Auditor-General
Queensland Audit Office
PO Box 15396
CITY EAST QLD 4002

Dear ~~Mr Close~~ Anthony,

Re: Performance audit on security of critical water infrastructure departmental feedback

Thank you for your letter regarding the performance audit on security of critical water infrastructure departmental feedback.

Please find attached the completed agency response form as requested. The completed form indicates support for the departmental specific recommendations detailed in the proposed report to parliament on the performance audit on the security of critical water infrastructure undertaken by the Queensland Audit Office.

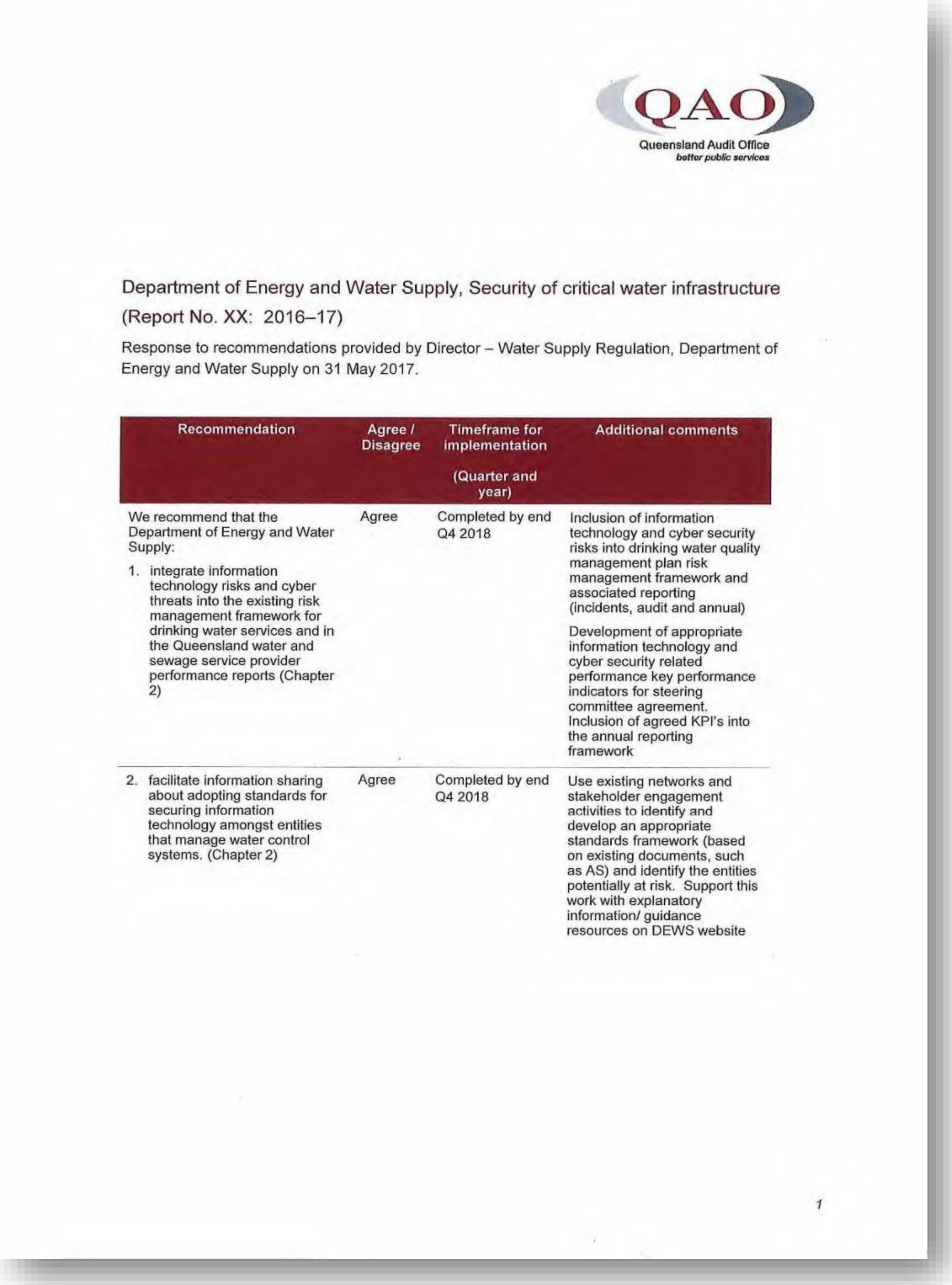
The water industry in Queensland is unique in Australia. Queensland has 86 registered providers of drinking water services operating over 300 individual supply systems. Of these systems, 44 per cent supply to less than 1000 connections. Many of these supply systems are located in very remote, isolated areas and are operated manually. This unique environment has been taken into account when developing the detailed actions, as described in the attached form that will be undertaken by my department to implement the report recommendations.

Yours sincerely

Mark Bailey MP
Minister for Main Roads, Road Safety and Ports and
Minister for Energy, Biofuels and Water Supply

Att: QAO Departmental response form

Responses to recommendations



Queensland Audit Office
better public services

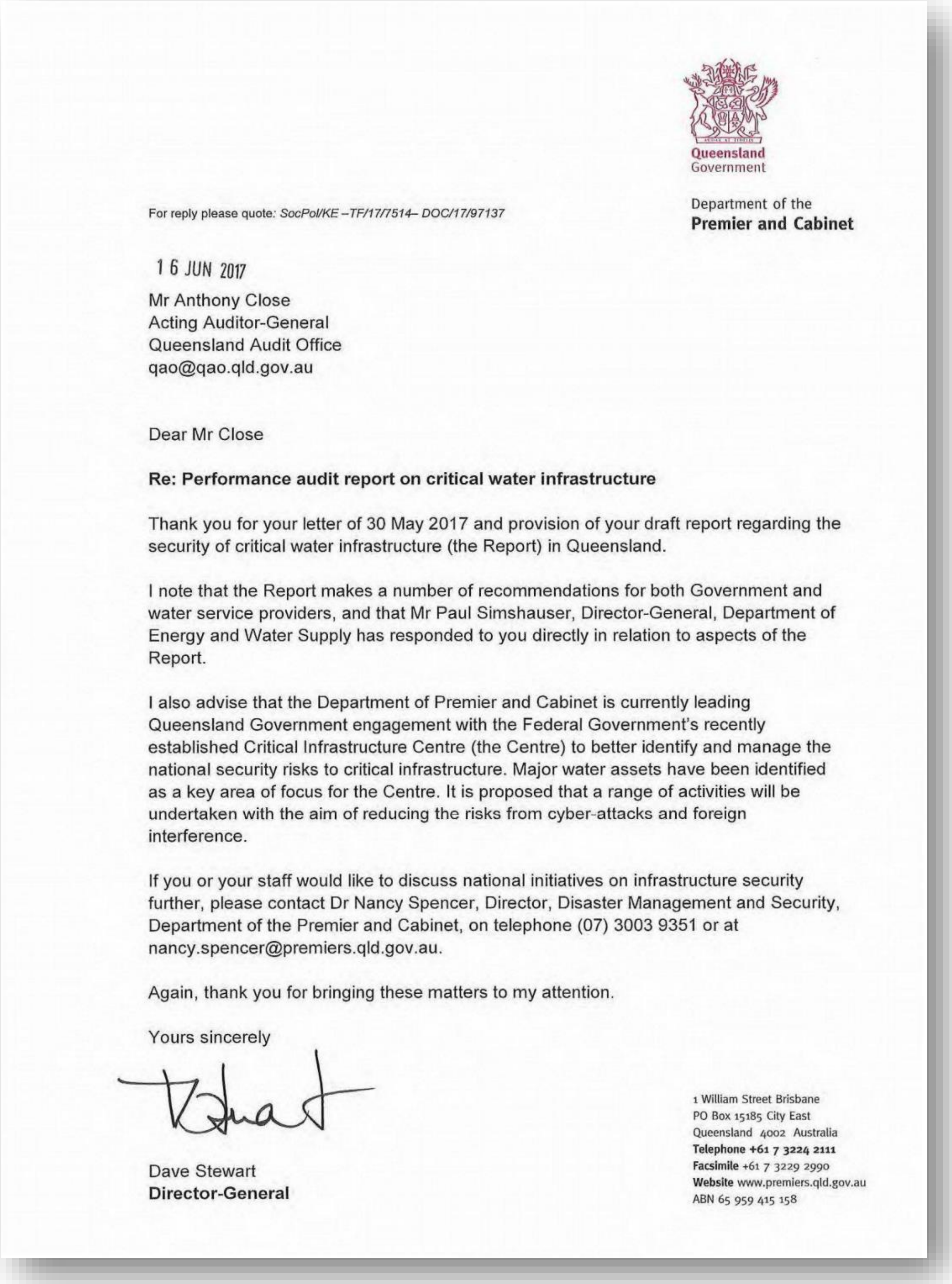
Department of Energy and Water Supply, Security of critical water infrastructure (Report No. XX: 2016–17)

Response to recommendations provided by Director – Water Supply Regulation, Department of Energy and Water Supply on 31 May 2017.

Recommendation	Agree / Disagree	Timeframe for implementation (Quarter and year)	Additional comments
We recommend that the Department of Energy and Water Supply: 1. integrate information technology risks and cyber threats into the existing risk management framework for drinking water services and in the Queensland water and sewage service provider performance reports (Chapter 2)	Agree	Completed by end Q4 2018	Inclusion of information technology and cyber security risks into drinking water quality management plan risk management framework and associated reporting (incidents, audit and annual) Development of appropriate information technology and cyber security related performance key performance indicators for steering committee agreement. Inclusion of agreed KPI's into the annual reporting framework
2. facilitate information sharing about adopting standards for securing information technology amongst entities that manage water control systems. (Chapter 2)	Agree	Completed by end Q4 2018	Use existing networks and stakeholder engagement activities to identify and develop an appropriate standards framework (based on existing documents, such as AS) and identify the entities potentially at risk. Support this work with explanatory information/ guidance resources on DEWS website

1

Comments received from Director-General, Department of the Premier and Cabinet



Queensland
Government

Department of the
Premier and Cabinet

For reply please quote: *SocPol/KE –TF/17/7514– DOC/17/97137*

16 JUN 2017

Mr Anthony Close
Acting Auditor-General
Queensland Audit Office
qao@qao.qld.gov.au

Dear Mr Close

Re: Performance audit report on critical water infrastructure

Thank you for your letter of 30 May 2017 and provision of your draft report regarding the security of critical water infrastructure (the Report) in Queensland.

I note that the Report makes a number of recommendations for both Government and water service providers, and that Mr Paul Simshauser, Director-General, Department of Energy and Water Supply has responded to you directly in relation to aspects of the Report.

I also advise that the Department of Premier and Cabinet is currently leading Queensland Government engagement with the Federal Government's recently established Critical Infrastructure Centre (the Centre) to better identify and manage the national security risks to critical infrastructure. Major water assets have been identified as a key area of focus for the Centre. It is proposed that a range of activities will be undertaken with the aim of reducing the risks from cyber-attacks and foreign interference.

If you or your staff would like to discuss national initiatives on infrastructure security further, please contact Dr Nancy Spencer, Director, Disaster Management and Security, Department of the Premier and Cabinet, on telephone (07) 3003 9351 or at nancy.spencer@premiers.qld.gov.au.

Again, thank you for bringing these matters to my attention.

Yours sincerely

Dave Stewart
Director-General

1 William Street Brisbane
PO Box 15185 City East
Queensland 4002 Australia
Telephone **+61 7 3224 2111**
Facsimile +61 7 3229 2990
Website www.premiers.qld.gov.au
ABN 65 959 415 158

Appendix B—Audit objectives and methods

Audit objective

The objective of the audit was to assess whether systems used to operate, manage, monitor water infrastructure are secure, and effective processes are in place to recover from adverse events.

Reason for the audit

We conducted the audit for the following reasons:

- The need for secure critical infrastructure. Recent security threats highlight the need to strengthen systems security for all critical infrastructure. Critical infrastructure owners can adopt some of the learnings from a number of security breaches on these systems worldwide.
- The heightened security risks and cyber attacks leading up to Commonwealth Games. Security research shows an increase in cyber attacks on countries and organisations hosting major events.
- In our previous audit of systems used to manage traffic, we found that the related control systems were not secure and susceptible to targeted attacks. It is time to ascertain whether water control systems have the required level of security.

Performance audit approach

The audit was conducted between August 2016 and May 2017.

Figure B1
Audit approach

Audit area	Approach
Security of water control system	▪ Evaluate the governance and oversight function for security of water control systems from the perspective of the whole of government and the entities we audited ▪ Evaluate the security and control designs of the water control systems ▪ Conduct penetration tests to identify and exploit security vulnerabilities—the tests include the use of social engineering techniques to manipulate staff members to provide access or information that we can use to plan for a penetration attack.
Business continuity management	▪ Perform desktop review on the information technology disaster recovery plan and business continuity plan ▪ Evaluate the capabilities and tests to respond to incidents and disasters.

Source: Queensland Audit Office.

Appendix C—The Australian Signals Directorate—essential eight controls

Figure C1
Key controls the Australian Signals Directorate recommends

Control	Description and practical application
Application whitelisting	A whitelist only allows selected applications to run on computers. While this needs to be applied across the board on all computers, entities can take a phased approach, implementing in risky areas first, for example, on computers in meeting rooms.
Patch application	A patch fixes security vulnerabilities in software applications. Entities need to schedule security patches into their maintenance process and assess the risks of not applying any security patches that the vendor is recommending.
Disable untrusted Microsoft Office macros	Microsoft Office applications can use software to automate routine tasks. Entities need to secure or disable these macros as adversaries are increasingly using these to download malware.
User application hardening	Block web browser access to Adobe Flash Player, web ads and untrusted Java code on the internet. These are popular ways to deliver malware to infect computers.
Restrict administrative privileges	These should be restricted to only those that need them. Admin accounts are keys to the kingdom and those that have this type of access should only use it to install software and apply patches. Those users should have separate accounts for their day-to-day operational work.
Patch operating systems	A patch fixes security vulnerabilities in operation systems. Entities need to schedule security patches into their maintenance process and assess the risks of not applying any security patches that the vendor is recommending.
Multi-factor authentication	The user is only granted access after successfully presenting multiple, separate pieces of evidence. Entities can use physical tokens, passphrase and/or biometric data.
Daily backup of important data	Regularly back up all data and store it securely offline. That way your organisation can access data if it suffers a cyber security incident.

Source: Australian Signals Directorate—Essential Eight.

Appendix D—Assessing information technology security

Assessing the security of information technology involves inspecting the environment, policies and security controls. Its main purpose is to determine the strength of the entity's defences in protecting the systems under review. Testing the controls can help in planning for unforeseen gaps in security risks and threats that the entity has not addressed.

Due to the complexities of systems and the continuous evolution of hackers and vulnerabilities, passing security tests is not an indication that flaws do not exist. Nor does it indicate that the system adequately satisfies the security requirements. New hacking techniques are continuously developed and easily accessible online. For this reason, a continuous review and improvement program is essential in protecting key systems from security threats and vulnerabilities.

Evaluating the strength of the information technology control environment

There are a number of techniques to evaluate the control environment. Typically, entities use a combination of these methods when conducting assessments. In this section, we discuss three methods of evaluating information technology controls:

- examining information technology controls
- penetration testing
- red teaming.

Examining detailed information technology controls

This method, when compared with other testing methods, does not provide definite proof that attacks are possible and does not clearly demonstrate the potential impact of an attack. Entities can use this method to assess the applicable threats and potential consequences of a breach.

This type of testing typically involves:

- Examining policies and procedures to assess whether the controls within the documents address potential risks. In addition, the entity needs to assess whether staff members follow the policies and procedures.
- Assessing the network design and mapping these to any existing security plans to determine whether the design is consistent with the plan.
- Testing the security of information technology infrastructure. Examples of this test includes:
    - analysing the firewall configuration and assessing access controls for network traffic
    - testing message transfers to evaluate the type of access across the network
    - assessing network devices, servers and other network infrastructure for security vulnerabilities (vulnerability scanning)
    - confirming security vulnerabilities exist without exploiting them.

It is important to distinguish vulnerability scanning from penetration testing. Vulnerability scanning only reports known vulnerabilities that exist within systems.

Penetration testing

Penetration testing is an authorised simulated attack on a computer system. The penetration tester is given a defined scope and a particular goal. The primary goal of penetration tests is to find vulnerabilities that an adversarial attacker can exploit, and to recommend mitigation strategies.

Reports from this type of test include potential impacts of the vulnerabilities and entities can use these to inform the business security risk assessment. This type of testing shows the risk of not fixing security issues. These are more expensive and riskier than evaluating information technology controls and can affect system availability and data integrity.

Penetration testing consultant

The quality of the penetration test is directly proportional to the kind of expertise that the penetration testing consultants have. Figure D1 includes key questions that entities can consider when selecting a penetration tester.

Figure D1
Selecting a penetration tester

Questions to consider when selecting a penetration tester
Does the supplier's methodology follow or exceed guidelines of the National Institute of Standards and Technology, Open Web Application Security Project, Open Source Security Testing Methodology Manual, and Penetration Testing Execution Standards?
Are the supplier's staff experienced security professionals? Do they hold recognised certifications for penetration testing?
Does the supplier have sufficient technical consultants that work on the security assessments?
How does the supplier present the deliverables? Do they include detailed findings and recommendations for addressing security issues?
Is the supplier a recognised contributor within the security industry?
Has the lead penetration tester done any of the following? ▪ positively demonstrated a clear track record or performance ▪ published research papers ▪ made presentations at various local and international conferences ▪ gained relevant certifications.

Source: Queensland Audit Office.

Red teaming

A red team differs from a penetration test. The red team performs a controlled, simulated attack on an entire organisation. It uses all resources available to gain complete control of an entity's systems.

The objective of the test is to assess the ease with which an entity can be compromised. Unlike a penetration test, the single purpose of red teaming is to gain compromise. To achieve this, the team will attempt but not be limited to the following:

- masquerade as the entity's staff members to obtain or tamper with physical systems
- produce malicious systems that mimic those of the entity to convince employees to use them
- attack external systems to bypass weak security controls

Results and reports of red teaming provide information on the impacts of a compromise. Entities can use it to evaluate the security of people, process and technology of the business. However, as the red team uses the path of least resistance, the results may not provide the breadth and depth of coverage.

Entities can design this exercise so that the red teams can work with an internal team that would defend the red team's attempts to compromise the system. In this scenario, we refer to the internal team as the blue team. A new approach is also emerging, whereby entities can establish a purple team to enhance the collaboration between the red and blue teams. Figure D2 describes each team's characteristics.

Figure D2
Team compositions for penetration tests

Team Name	Description of their function
Red team	An external entity brought in to test the effectiveness of a security program. The entity emulates the behaviours and techniques of likely realistic attackers. This is similar, but not identical to penetration testing.
Blue team	This is the internal security team. Its primary objective is to defend against attempts to compromise the organisation. This is distinguished from security and operations teams as blue teams have a mentality of constant vigilance.
Purple team	The primary goal of this team is to facilitate integration between the red and blue teams and to provide feedback for improving their respective processes. This also assists the blue team to address the security gaps that the red team identifies.

Source: Daniel Miessler, Information Security Practitioner—The difference between red and blue teams.

Auditor-General reports to parliament

Reports tabled in 2016–17

Number	Title	Date tabled in Legislative Assembly
1.	Strategic procurement	September 2016
2.	Forecasting long-term sustainability of local government	October 2016
3.	Follow-up: Monitoring and reporting performance	November 2016
4.	Criminal justice system—prison sentences	November 2016
5.	Energy: 2015–16 results of financial audits	December 2016
6.	Rail and ports: 2015–16 results of financial audits	December 2016
7.	Water: 2015–16 results of financial audits	December 2016
8.	Queensland state government: 2015–16 results of financial audits	December 2016
9.	Hospital and Health Services: 2015–16 results of financial audits	January 2017
10.	Effective and efficient use of high value medical equipment	February 2017
11.	Audit of Aurukun school partnership arrangement	February 2017
12.	Biosecurity Queensland's management of agricultural pests and diseases	March 2017
13.	Local government entities: 2015–16 results of financial audits	April 2017
14.	Criminal justice system—reliability and integration of data	April 2017
15.	Managing performance of teachers in Queensland state schools	April 2017
16.	Government advertising	May 2017
17.	Organisational structure and accountability	May 2017
18.	Universities and grammar schools: 2016 results of financial audits	June 2017
19.	Security of critical water infrastructure	June 2017

www.qao.qld.gov.au/reports-resources/parliament

SCADA UPGRADE AT FITZROY RIVER WATER FOR IMPROVED SECURITY AND FUNCTIONALITY

FRW SCADA Risk Assessment Summary Report

Meeting Date: 15 August 2017

Attachment No: 2

KJ Khoo

13th March 2017

FITZROY RIVER WATER

Risk Assessment Report: Prioritized Remediations R0

Honeywell

Recommended Remediation (Prioritized)

Immediately to 3 months time:-

Current Network Architecture

- Application of two-factor authentication for client based VPN access into RRC/FRW
- To undertake an end-to-end Cyber Security Vulnerability Assessment for FRW's SCADA infrastructure

Proposed SCADA Upgrade Network Architecture

- Introduction of redundant Domain Controllers in Level 2 and Level 2.5
- All nodes to join the new domain
- Personal account for each engineer
- Operator based single sign-on
- Password and Account Policy
- Scheduled offsite backup to RRC IT

Honeywell

Recommended Remediation (Prioritized)

Immediately to 3 months time:-

SCADA Cisco Switch Review

- Catalog configurations, IOS versions and equipment into a list for SNR proposal
- Configuration hardening

Check Point Firewall Review

- Apply recommended changes to rules number 2, 5, 6, 9 and 10
- Engage administrator of public FTP server to support SFTP instead

Physical Security

- Establish local security policy to limit control area access to operators or other relevant personnel only
- Access to PLC room and alternate passage to control area should remain locked at all times

Recommended Remediation (Prioritized)

In 3 to 6 months:-

Network Segregation

- Removal of peering uplinks between IT and SCADA switches

Ubiquiti Stations & Access Point

- Replacement PSK with RADIUS authentication
- Configuration hardening

Proposed Cyber Security Lifecycle

- Antivirus, Operating System and Software Patch Management with Honeywell Industrial Managed Security Services
- Cyber Security Training Workshop for FRW both engineers and managers

Recommended Remediation (Prioritized)

In 6 to 12 months:-

EMClarity Microwave Modem

- Introduction of peering routers to establish a secured VPN tunnel from FRW to Mt. Archer

Physical Security

- Enclose control area with access card system

Proposed Cyber Security Lifecycle

- Development of an Incident Response Procedure
- Development of Access Control elements to be considered for FRW’s IACS-SMS policy
- Monitoring the SCADA Network with H-ICS Risk Manager for anomalies

8.5 SOLAR FARM AT THE GLENMORE WATER TREATMENT PLANT FOR SOCIAL, ENVIRONMENTAL AND ECONOMIC OUTCOMES

File No:	**1466**
Attachments:	**Nil**
Authorising Officer:	**Peter Kofod - General Manager Regional Services**
Author:	**Jason Plumb - Manager Fitzroy River Water**

SUMMARY

Sources of renewable energy such as solar farms are increasingly being seen as the means by which private and public entities can secure cost-effective electricity supplies that provide clear environmental outcomes through the reduction in greenhouse gas emissions. Fitzroy River Water has identified that the Glenmore Water Treatment Plant is highly suited to the construction of a solar farm that has great potential to provide environmental, social and economic benefits for FRW and the community. This report provides information as to the details of this opportunity and seeks endorsement of a capital budget allocation towards completion of this project within the next couple of years.

OFFICER'S RECOMMENDATION

THAT the development of a solar farm at the Glenmore Water Treatment Plant be considered for inclusion in the 2018/19 capital program.

COMMENTARY

The transition from traditional sources of electricity such as centralised power generation using coal or other fossil fuels, to de-centralised power generation using renewable energy sources such as solar is rapidly gaining momentum in Australia. The rapid increase in the development of solar power generation has led to a significant reduction in the cost of small and large-scale solar power. As a result, solar farm projects are being embraced by many different industry sectors including both private and publicly funded organisations. In Australia, a number of regional Councils are either commencing or considering the development of solar farms for their community. In Queensland, the Sunshine Coast, Fraser Coast and Mackay Regional Councils have confirmed investments in this initiative.

The development of solar power generation has a clear environmental benefit through the reduction in the reliance on fossil fuels and an associated reduction in the release of greenhouse gases such as carbon dioxide. It is important to understand that solar energy generation has the potential to deliver significant economic and social benefits also. These additional benefits are realised through the reduction or elimination of electricity bills that in recent years have seen annual increases in excess of 15% p.a. If this achieved, this reduced operating expenditure translates into increased revenue which could then be used to fund capital projects to improve service levels or achieve other community benefits. The social benefit is also achieved through an improved perception amongst the community that improved environmental and social outcomes are achieved at no additional cost. This opportunity to achieve triple bottom line outcomes to such an extent is usually very rare!

BACKGROUND

Fitzroy River Water (FRW) is a large user of electricity compared to Council's other sections. Primarily, this high electricity usage occurs when pumping large volumes of water or sewage from one location to another. Sewage treatment processes such as aeration also use significant amounts of electricity. Each year FRW incurs approximately $3 million in electricity costs, with the Glenmore WTP and associated water pump stations comprising close to a third of this total cost. With each capital upgrade opportunity FRW seeks to maximise the energy efficiency improvements that are possible through the use of new equipment or improved operating control systems, and at best these efficiency gains have occasionally offset the typical electricity price increases of 15% p.a. in recent years.

FRW has for some time been looking at the opportunities for investing in renewable energy generation as a means of reducing operating costs. In recent months, the completion of the SCADA upgrade project led FRW to commence initial discussions about solar energy generation with the company delivering this project due to their partnership with a global leader in solar energy generation projects. To date, these discussions have advanced as far as the completion of some pre-feasibility concept level analysis. The outcomes of this work indicate that FRW's Glenmore Water Treatment Plant site is well-suited to the development of solar farm for the following reasons:

- There is sufficient vacant land that is well suited for construction of a solar farm of up to at least 2 MW with sufficient space for vegetation buffers and maintenance access
- The Glenmore WTP currently has two 11 kV power feeds into the site that provide good access to the electricity network to either import or export power accordingly
- The recently completed electrical upgrade means that little to no work is required to upgrade existing electrical switching and associated infrastructure
- An existing diesel generator is already in place to provide additional back-up
- The FRW SCADA system can be used to ensure the most efficient mix of power sources is used to maximise the benefit of the solar power generation

Because of the inherent advantages of the FRW site, the estimated capital cost for the development of a solar farm is lower than what might be possible in other locations. Initial analysis completed for the construction of a 1.5 MW solar farm indicates that based on a total capital cost of $3 million, the electricity generated from such a facility could achieve a return on capital investment within 5-6 years. This analysis has been checked by Council's accountants and been shown to be sound. It is important to note also that the partial or complete reduction in electricity costs incurred at the Glenmore Water Treatment Plant through the use of available solar power would be achieved immediately upon commencement of operation.

Based on the work done to date, it is clear that this opportunity warrants further investigation to confirm the specific details required to finalise a decision on the merits of this project. FRW is currently ready to take the next step in this feasibility assessment to development the project specification and likely commercial arrangements with an energy retailer. Based on similar projects being developed in other locations and the specific advantages that the FRW site possesses, there is little doubt that this project will prove feasible.

BUDGET IMPLICATIONS

Currently there is no capital budget allocation to progress this project, with a proposed project allocation excluded from the 2017/18 Council budget. No significant expenditure has been incurred up until now on this project, however, the next step in investigating this opportunity will require approximately $20,000 for further feasibility work.

In the absence of any significant budget allocation, it is very difficult for Council to seek grant funding where matching funding from Council is a pre-requisite for grant funding. An alternative option is to prioritise this project for inclusion in any funding opportunities that do not require Council co-funding (e.g. Works For Queensland Program).

LEGISLATIVE CONTEXT

The construction of a solar farm at the Glenmore Water Treatment Plant site is likely to be subject to development assessment, although given that the vacant land was always intended for use in relation to waterworks, development approval appears likely to be granted with conditions to ensure adequate vegetation buffers are included in the design. FRW is not aware of any other legislative requirements or implications for this project opportunity.

CORPORATE/OPERATIONAL PLAN

This project opportunity is directly relevant to Operational Plan actions No. 3.2.1.1 Develop a Renewable Energy Program for Fitzroy River Water, and No. 5.3.2.1 Continually Review Operational Expenditure in order to identify operational cost savings.

CONCLUSION

An excellent opportunity exists for Council to make a capital investment in a renewable energy project by constructing a solar farm at the Glenmore Water Treatment Plant site in Parkhurst. The Glenmore Water Treatment Plant site is well suited to this type of project due to the available land, the recently completed electrical upgrades and access to the high voltage electricity network. The completion of this project would provide significant environmental, social and economic benefits for FRW and the community.

9 NOTICES OF MOTION

Nil

10 URGENT BUSINESS/QUESTIONS

Urgent Business is a provision in the Agenda for members to raise questions or matters of a genuinely urgent or emergent nature, that are not a change to Council Policy and can not be delayed until the next scheduled Council or Committee Meeting.

11 CLOSURE OF MEETING