

# Project Mercury

IT and cybersecurity due diligence report

**Reliance Restricted**

03 October 2018 | Version 1.0 (Draft)



**Ernst & Young LLP**  
**Transaction Advisory Services**  
5 Times Square  
New York, NY 10036  
**ey.com**

Aqua America Inc.  
726 West Lancaster Avenue  
Bryn Mawr, PA 19010

## **Project Mercury**

**3 October 2018**

Dear Sir / Madam,

At the request and direction of Aqua America Inc. (“Aqua” or “you”), we performed certain due diligence procedures in connection with your contemplated investment in Peoples Natural Gas (“the Transaction”). See Appendices C and D for a complete listing of scope and procedures performed. Any differences between the procedures set forth in this Report and those set forth in our Statement of Work dated September 14, 2018 under our Agreement reflect modifications that were made at your request or discussed with you during the course of the engagement.

The procedures that we performed do not constitute an audit of Peoples Natural Gas (“PNG”, “the Company” or “Target”) historical financial statements in accordance with generally accepted auditing standards, nor do they constitute an examination of prospective financial statements in accordance with standards established by the American Institute of Certified Public Accountants. Additionally, the procedures do not address the effectiveness of internal controls over financial reporting under Section 404 of the Sarbanes-Oxley Act. Also, we performed no procedures to evaluate the reliability or completeness of the information obtained. Accordingly, we express no opinion or any other form of assurance on the historical or prospective financial statements, management representations or other data of PNG included in or underlying the accompanying information. While we believe the information obtained is substantially responsive to your request, we are not in a position to assess its sufficiency for your purposes. In addition, we have no responsibility to update this report for events or circumstances occurring after the date of this Report.

In performing the due diligence procedures, we have accumulated data, written various memoranda for our own use and the use of other members of the due diligence team, and have had various meetings with representatives of Aqua and PNG. The procedures performed and related findings are presented in the attached Transaction Insights Report.

While we may provide advice and recommendations to Aqua, Aqua is solely responsible for any decision to execute or implement any such advice or recommendation, the actual execution or implementation of any thereof, and the results of such implementation. We make no representation, warranty or other statement as to whether its advice, recommendations or any strategies contained therein may be effectively or successfully implemented by Aqua, or with respect to any results thereof.

This report is intended for use solely by members of Aqua management, its board of directors and its legal advisors. Copies should not be made, nor should this report be distributed to others without our express permission.

Yours faithfully,

Ernst & Young LLP



**Dashboard**

Table of contents

- 1 Executive summary
- 2 Scope
- 3 IT observations
- 4 Cybersecurity observations
- 5 Next steps
- 6 Appendix

---

## Executive summary

1

Page 4

---

## Scope

2

Page 7

---

## IT observations

3

Page 11

---

## Cybersecurity observations

4

Page 32

---

## Next steps

5

Page 36

---

## Appendix

6

Page 43

# 1

## Executive summary

In this section	Page
Information technology and Cybersecurity	5



## 1 Executive summary

### Information technology and Cybersecurity

#### 1 Executive summary

- 2 Scope
- 3 IT observations
- 4 Cybersecurity observations
- 5 Next steps
- 6 Appendix

#### Major IT projects in-flight

- ▶ The Company has significant IT initiatives in-flight including IT integration of a recent acquisition, Delta Gas, customer service portal replacement, SAP upgrades, enhanced mobile connectivity, telecommunications upgrades, mobile device enablement, asset traceability, and business intelligence and analytics integration. These in-flight initiatives are relatively large and complex, impact core systems including SAP, and require a significant spend (budget of \$34.9M in FY18). Unless managed appropriately, there could be delays, cost overruns, potential business disruption, and customer impact. Aqua should factor in these initiatives as part of its IT integration roadmap.

#### Legacy applications

- ▶ Four out of 68 applications are no longer under active vendor maintenance and support contracts, thereby increasing operational risk.
- ▶ Additionally, documentation provided by the Company indicates that eight to ten compressor stations are controlled by an outdated program and hardware that is no longer supported by the vendor. Replacing the application requires the engine to be rewired with new sensors, remote terminal units, and possibly replacing the engine itself; the total cost would be \$500,000 or more per station. The IT Capex project list did not include upgrade of these systems.

#### SAP

- ▶ The Company leverages SAP as its core backbone enterprise resource planning (ERP) system. The Company also leverages SAP's customer relationship management (CRM) capabilities.
- ▶ Based on the SAP Early Watch report provided from the week of August 6, 2018, there appear to be no material issues with the Company's SAP environment.
- ▶ The Company has ensured that the SAP landscape is at the latest enhancement pack levels. SAP ECC 6.7 and CRM 7.3 provide robust functionality for a utility and are the minimum enhancement pack level necessary to upgrade to SAP Suite on HANA or S/4 HANA. SAP ECC and CRM will be out of support in 2025 and migration to HANA needs to be completed prior to this.
- ▶ Based on the information presented, the Company appears to be migrating to Suite on HANA, which entails replacing its current database with HANA. However, Management stated that the Company is migrating to S/4 which would require business process change driven by new SAP functionality. We recommend that the Company clarify its migration approach with SAP.
- ▶ The Company is planning to migrate Finance/Enterprise Asset Management (EAM) ECC to HANA first, followed by CRM. Doing so would have ECC and CRM on different support packs, which is not recommended.
- ▶ A full functional assessment should be conducted to understand business impact before migrating the Company to S/4 .

#### SAP (contd.)

- ▶ Based on timing of the start of the project in early 2019, Aqua should plan on executing a migration to HANA as part of the Company's migration onto the platform, so that the projects can be executed together. This assumes that Aqua does not want to wait for the Company's migration to S/4 HANA be completed, prior to integration. There is low incremental risk of executing both projects together but this would increase the current HANA migration budget by approximately \$1.5M to \$2.0M due to integration of Aqua.
- ▶ Due to the integrated nature of the Company's SAP system, Aqua may need to consider migrating finance and EAM together.

#### IT organization

- ▶ The Company has 69 IT resources, 14 of whom are contractors and 55 are full time employees. A third of the application development team is composed of contractors which could pose key person reliance risk for critical, application specific skills.
- ▶ The Company typically leverages outsourcing and consulting support to execute its discretionary projects. Approximately 10% of the internal IT team's effort is spent on capital projects.
- ▶ The IT Management team appears to be competent and knowledgeable about the Company's IT environment having built it ground up. Aqua should consider a retention strategy for IT Management.





## 1 Executive summary

### Information technology and Cybersecurity

#### 1 Executive summary

- 2 Scope
- 3 IT observations
- 4 Cybersecurity observations
- 5 Next steps
- 6 Appendix

#### Cybersecurity

- ▶ The Company has invested significantly in cybersecurity controls in order to protect both corporate data as well as the operational network used to deliver gas. A separate, firewalled operational network has been built in order to securely control the devices and controls necessary to operate and monitor pipelines. The operational network includes intrusion detection capabilities to identify potential attack.
- ▶ The Company conducts numerous annual security audits. Management reported the most recent audit by Deloitte had no adverse findings. The Company's cybersecurity insurer also requires an annual audit which is conducted by a different firm.
- ▶ The Company conducts annual penetration tests, and changes testing firms every few years to benefit from the different perspective and techniques different testers might bring.
- ▶ The Company also participates in industry working groups to share concerns regarding security as well as techniques to protect their environment. They are not required to be compliant with NERC-CIP, which applies to electric utilities, but do use the control framework published by that organization to govern the Company's control framework.
- ▶ Overall, the Company appears to have a well-documented security framework that is based on industry standard practices, and has a commitment to staying current on new threats that can affect its business and operations.

#### Other notables

- ▶ The Company's IT operating expenses are higher than industry benchmarks, most likely due to operational technology spend, which is included in the IT budget.
- ▶ The Company appears to be following appropriate practices for software asset tracking to monitor usage and compliance.
- ▶ The Company is not currently SOX compliant but performs ad hoc assessments in compliance with the Commonwealth of Pennsylvania law and follows the Cybersecurity Capability Maturity Model (C2M2) standards.
- ▶ The Company appears to have robust IT and OT (operational technology) disaster recovery capabilities which includes local and cross-site redundancy, rapid failover of critical applications, and multiple back-up and recovery options for systems.

# 2

## Scope

In this section	Page
Scope	8
Overview of the Company's application landscape	9



## 2 Scope

### Scope

1	Executive summary
<b>2</b>	<b>Scope</b>
3	IT observations
4	Cybersecurity observations
5	Next steps
6	Appendix

### Scope

Analyzed materials provided and conducted two discussions with Management to identify key IT transaction considerations.

This report summarizes our findings and observations regarding the Company's information technology (IT) and cybersecurity matters and is based on:

1. A two hour conference call led by Aqua's Chief Information Officer (CIO), Ms. Whitney Kellett, to discuss IT and cybersecurity matters with Management including:
  - ▶ Ms. Ruth Wylie, Senior Vice President and Chief Administrative Officer (CAO)
  - ▶ Mr. Nagy Nagiub, Senior Director, Corporate Services
  - ▶ Mr. Kevin Turkovich, Chief Cybersecurity Director
  - ▶ Mr. Joseph Brado, Chief Technical Director
2. A follow-up conference call with Management to discuss the Company's SAP environment;
3. Analysis of the materials provided by the Company; and
4. Research on vendors and technologies used by the Company.

We did not visit the Company's facilities and relied on Management's descriptions of the infrastructure and data centers. We did not witness any system or platform demonstrations.

We performed high level procedures as described in Appendices C and D focused on:

- ▶ The scalability and reliability of key software applications.
- ▶ Performance, reliability and security of the IT infrastructure.
- ▶ Organizational skillsets and capabilities to support the IT environment.
- ▶ The Company's cybersecurity posture.

We did not include comments in our discussions below for those procedures where we did not have significant findings. Information provided by the Company has not been independently verified. A more detailed assessment may reveal unidentified risks and additional opportunities for improvement.





## 2 Scope

### Overview of the Company's application landscape

1	Executive summary
<b>2</b>	<b>Scope</b>
3	IT observations
4	Cybersecurity observations
5	Next steps
6	Appendix

Function	Current system	Future disposition
Asset tracking, Spatial Modeling	ArcGIS	No planned change
Business Intelligence	SAP BW on Hana	No planned change
Call Center front-end	IC/Web	Replace with SAP Fiori Multi-Channel Functionality
Capital Assets	SAP ECC	Upgrade to S4/HANA
Compliance Work Management	GL/Essentials	Upgrade Essentials software to latest release
Compressor station operations	Siemens – Step 7 Legacy system inherited in prior acquisition. Installed version no longer supported by vendor. Requires new sensors, rewiring compressor engine to replace.	Replace obsolete M-Health system for tracking and reporting on compressor station operating data. New system will augment manual data collection with sensor-based data acquisition.
Consolidations, Financial Reporting	SAP ECC	Upgrade to S4/HANA
Customer Information System (CIS)	SAP ECC (on prem)	Upgrade to S4/HANA
Customer Portal	Avertra MiCustomer Portal	Replace with SEW/SAP Customer Portal
Document Management	Perceptive Content	No planned change
Environment, Health and Safety (EHS)	Zeraware – Job site safety observations (JSSO)	Legacy system brought over from Dominion. Targeted by Operations for replacement in 2019
Email	MS Exchange	Upgrade to Microsoft Exchange software to current release, 2016
Financial Information System (FIS)	SAP ECC	Upgrade to S4/HANA
Gas Management	Gastar – Ensyte	Upgrade Gastar software to current release
Gas Measurement	Aveva	Upgrade Gas Measurement software to current release, refresh hardware platform
HRIS	SAP ECC	Upgrade to S4/HANA, potentially deploy SuccessFactors in the future
Interactive Voice Response (IVR)	Genesys	Upgraded to Latest Software, Added Natural Voice capabilities, Redesigned the call Flow and Added more self service
Land Records	P2 Tobin	No planned change
Metering	M-Health	GE Intelligence Platform

\*This list includes key systems and does not cover all systems used by the Company



## 2 Scope

### Overview of the Company's application landscape

1	Executive summary
<b>2</b>	<b>Scope</b>
3	IT observations
4	Cybersecurity observations
5	Next steps
6	Appendix

Function	Current system	Future disposition
Middleware Integrations	SAP Process Integration (PI), vendor APIs, custom-developed programs, and scripts	No planned change, however, interfaces may get impacted due to upgrades planned
Mobile Map	Custom Developed	Replace the current Mobile Map application to improve usability and keep current with Esri technology evolution
Mobile Workforce Mgmt.	Ventyx/Service Suite	Upgrade Ventyx ServiceSuite software to version 9.6
Phones	Atos (Unify, Siemens).HiPath 4K PBX Platform	Upgrade recently completed
Supervisory control and data acquisition (SCADA)	Aveva	Upgrade SCADA software to current release, refresh hardware platform
Time tracking	Workforce Software (cloud)	Recently implemented, go live in June 2018
Training	TEDS – Legacy system brought over from Dominion	Operations is planning to transition to SkillSoft for training and OQ tracking by 1/1/2019

\*This list includes key systems and does not cover all systems used by the Company

# 3

## IT observations

In this section	Page
Key findings	12
Preliminary comparison of key IT systems	31



## 3 IT observations

### Key findings

1	Executive summary
2	Scope
<b>3</b>	<b>IT observations</b>
4	Cybersecurity observations
5	Next steps
6	Appendix

Item	Description	Actions / Next Steps
<b>Major IT transformation in-flight</b>	<ul style="list-style-type: none"> <li>▶ The Company has a well thought out Information Technology (IT) strategy that focuses on delivering business process optimization and cross functional integration. IT is focused on improving four key aspects – availability, security, reliability, and functionality of the underlying systems and infrastructure. These are being addressed through multiple capital projects aimed at upgrading IT applications and infrastructure. Key initiatives cover a wide set of areas, including IT integration of recent acquisition, Delta Gas, customer service portal replacement, SAP upgrades, enhanced mobile connectivity, telecommunications upgrades, mobile device enablement, asset traceability, and business intelligence and analytics integration. [Refer to next two pages for details of in-flight and planned projects].</li> <li>▶ These in-flight initiatives are relatively large and complex, impact core systems including SAP, customer facing portal and IVR, and require a significant spend (budget of \$34.9M in FY18). Unless managed appropriately, there could be delays, cost overruns, potential business disruption, and customer impact if system changes are not adequately tested prior to release.</li> <li>▶ The IT capex budget file indicates that the Company expects to spend \$21.6M for IT and telecom related projects in FY18.</li> <li>▶ The high-level project portfolio status provided by the Company indicates that there are no significant risks associated with any of the in-flight IT initiatives. However, no detailed plans or status reports have been provided as yet <b>[OPEN]</b>.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Further diligence is needed to understand the discrepancy between the IT project budget and the IT capex budget.</li> <li>▶ Aqua should closely monitor the status and progress of in-flight projects as such large scale implementations run the risk of delays, cost overruns and customer impact.</li> <li>▶ Aqua should monitor the post go-live period closely to ensure customer satisfaction metrics are maintained at their current levels.</li> <li>▶ Additionally, Aqua should analyze the portfolio of planned projects and make adjustments to meet its integration objectives.</li> </ul>
<b>IT strategy and governance</b>	<ul style="list-style-type: none"> <li>▶ The Company's IT governance and strategic decision making processes align with industry standards. The Company pursues innovation through various initiatives including regular meetings with vendors, conducting annual "Technology Day" with SAP, close partnership with Carnegie Mellon University, and membership in the Pittsburgh Technology Council Board.</li> <li>▶ The Company's executive team and their direct reports meet annually to compile a five year outlook and set the Company's business goals for the coming year. The identification, budgeting and prioritization of discretionary IT projects begins with IT communicating with the business groups to understand requirements; followed by creation of a business case and a capital plan. The Company's Capital Investment Committee (CIC) reviews and approves the capital plan, which forms the basis for funding capital projects.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Aqua should participate in the CIC reviews and make adjustments to meet its integration objectives.</li> </ul>



### 3 IT observations

#### Key findings

1	Executive summary
2	Scope
<b>3</b>	<b>IT observations</b>
4	Cybersecurity observations
5	Next steps
6	Appendix

IT Projects – Applications: The Company expects to spend approximately \$32.7M in FY18 on application-related capital projects.

Project	Objectives	2018 Budget	Timelines	Status
Smart Meter – Peoples & PTWP	Multi-year initiative to install automated meter reading capability on Peoples and PTWP meters	\$ 12,280,000	Yearly phases	On Track – no significant risks
SAP CRM Replacement and Portal Enhancements	Replace existing IC/Web CRM front-end with a new, more efficient Fiori user interface. Replace the existing Peoples e-Account portal with the SEW/SAP customer portal solution	\$ 4,750,000	Jan 2018 to May 2019	On Track – no significant risks
DELTA integration	Migrate Delta Gas to Peoples' IT applications	\$ 4,000,000	2018 to 2019	On Track – no significant risks
IT – As Built Data Collection (Bar Coding)	Implement a system to collect as-built data electronically in the field	\$ 3,000,000	Prototype to be complete by end of 2018	On Track – no significant risks
Construction Project Management System	Implement systems to better manage the increased level of construction activity due to the LTIP Pipe Replacement program	\$ 2,000,000	To be complete by end of 2018	On Track – no significant risks
Ops Workforce Optimization	Improve field workforce productivity through more optimizing task routing and dispatching	\$ 1,500,000	To be complete by end of 2018	On Track – no significant risks
Application Upgrades – SAP S/4 HANA	Migrate SAP system to S/4 HANA to stay current with SAP strategic direction	\$ 1,250,000	Mid 2018 to Dec 2019	Initial planning in process; Project schedule TBD
Application Upgrades – SCADA	Upgrade SCADA and Gas Measurement software to current release, refresh hardware platform	\$ 1,200,000	To be complete by Nov 2018	On Track – no significant risks
PowerTax Deferred Tax Planning Module	Implement PowerTax Deferred Tax Planning module to comply with new tax regulations	\$ 500,000	NA	On Track – no significant risks
Accelerated Supplier Switching	Implement SAP system configuration changes to reduce the lead time for customers	\$ 400,000	TBD	Not started; pending PUC action
HR – WorkForce System	Implement new cloud-based time and attendance system from WorkForce Software	\$ 300,000	2017 to June 2018	Project complete
M-Health Replacement	Replace obsolete M-Health system for tracking and reporting on compressor station operating data	\$ 300,000	2017 to Dec 2018	On Track – no significant risks
Application Upgrades – Email	Upgrade Microsoft Exchange software to current release	\$ 260,000	To be complete by end of 2018	On Track – no significant risks
Mobile Map Upgrade	Replace the current Mobile Map application to improve usability and keep current with Esri technology evolution	\$ 200,000	2017 to June 2018	Project complete
Application Upgrades – Ventyx	Upgrade Ventyx Service Suite software to v 9.6	\$ 200,000	2017 to June 2018	Project complete
UFG Reporting Improvements	Develop a more automated and efficient process for gathering data for UFG reporting	\$ 200,000	To be complete by end of 2018	On Track – no significant risks
Esri Licenses	Purchase Esri licenses to remain in compliance with user activity	\$ 131,000	License purchase	Purchase submitted in August
Application Upgrades – Ensyte (GASTAR)	Upgrade Gastar software to current release	\$ 100,000	TBD	Not started; may be deferred to 2019
Application Upgrades – Essentials	Upgrade Essentials software to latest release	\$ 100,000	TBD	Not started; may be deferred to 2019

Source: Based on information provided by the Company



### 3 IT observations

#### Key findings

1	Executive summary
2	Scope
<b>3</b>	<b>IT observations</b>
4	Cybersecurity observations
5	Next steps
6	Appendix

IT Projects – Infrastructure: The Company is expected to spend an additional \$2.2M on infrastructure related capital projects

Project	Objectives	Total Cost	Estimated to Complete	Timelines	Status
Replace 1500+ Windows 7 Machines with windows 10	Replace 1500+ Windows 7 Laptops/Pcs to window 10	\$ 3,000,000	\$ 1,800,000	3-year project	40% Complete
SCADA Modems Replacement	Replacement of old XT/LS300 3G cellular modems with new RV50 4G/LTE modems to operate under new cellular platform	\$ 600,000	-	7 months	Project Complete
Upgrade Data Network_ Replace Routers and switches	Replaced routers at 17 locations, Switches in 24 Locations and Upgraded 84 Router and switches to enhance its cybersecurity Posture	\$ 300,000	-	6 months	Project Complete
Microwave Radio Infrastructure Replacement	5 year replacement schedule (2018-2022): Pitt St to Calvary to Cyano to Ginger Hill Also Hopewell to Grove City links in 2018.	\$ 225,000	\$ 75,000	4 months	60% Complete
IVR System Upgrade	Upgrading the software on all servers to the latest release	\$ 200,000	\$ 170,000	6 months	50% Complete
MAS/SCADA Infrastructure Replacement	Replacement of 4 wire and modems at priority sites with private MAS radio systems	\$ 200,000	\$ 75,000	6 months	80% Complete
Call Centre Infrastructure Upgrade	Replaced the current servers	\$ 75,000	-	4 months	Project Complete
Phone System Upgrade	Two New PBX processor one at Peoples Centre and one at Pitt St.	\$ 50,000	-	5 months	Project Complete
Upgrade Wireless Network Infrastructure	Enterprise upgrade of wireless controllers and access points over 150 Access Points and 2 controllers	N/A	\$ 50,000	NA	20% Complete
Unified Communications System Upgrade	OSV/UC is what provides our internal audio conference bridges and web conferencing. Replaced Servers and upgraded Software.	\$ 46,000	-	3 months	Project Complete
Voice Mail System Upgrade	A redundant warm standby server configuration with servers at Peoples Centre and Pitt St For improved business continuity.	\$ 10,000	\$ 10,000	5 months	In Planning Phase

Source: Based on information provided by the Company





## 3 IT observations

### Key findings

1	Executive summary
2	Scope
<b>3</b>	<b>IT observations</b>
4	Cybersecurity observations
5	Next steps
6	Appendix

Item	Description	Actions / Next Steps
<b>Application landscape is focused on leveraging SAP as the backbone ERP</b>	<ul style="list-style-type: none"> <li>▶ The Company extensively uses the SAP platform with a moderate to high level of customization.</li> <li>▶ The following SAP ECC (version 6.7) modules are implemented: <ul style="list-style-type: none"> <li>▶ Finance</li> <li>▶ HR</li> <li>▶ Supply chain management</li> <li>▶ Enterprise asset management</li> <li>▶ SAP BW (business warehouse) for managing SAP and non-SAP data sources</li> </ul> </li> <li>▶ The SAP CRM module (version 7.3) with ICWeb is also implemented and tightly integrated with ECC.</li> <li>▶ The SAP CRM system has been customized to meet regulatory requirements in Pennsylvania. The Company has followed SAP recommended practices of using allowable user exits and configurations to make changes to the system.</li> <li>▶ The Company is currently in the second year of a thirty month project to migrate all current SAP modules to S/4 HANA. This is expected to complete by December 2019.</li> <li>▶ The Company is implementing its e-account customer self-service portal based on the cloud platform provided by Smart Energy Water (SEW), an SAP partner. This would replace their MiCustomer portal provided by Avertra with whom the Company has begun the process of terminating its contract.</li> <li>▶ Management indicated that it has no significant customizations in its IT landscape outside of SAP. However, some applications have been significantly configured to adequately align with the Company's business processes: <ul style="list-style-type: none"> <li>▶ ABB (Ventyx) ServiceSuite has over 200 work order types configured for data fields, screen layouts, and validation rules.</li> <li>▶ DNV-GL Essentials has been configured for scheduling rules and work flow processes.</li> </ul> </li> <li>▶ The Company has ensured that the SAP landscape is at the latest enhancement pack levels. SAP ECC 6.7 and CRM 7.3 provide robust functionality for a utility and are the minimum enhancement pack level necessary to upgrade to SAP Suite on HANA or S/4 HANA. No additional enhancement pack upgrades should be required. SAP ECC and CRM will be out of support in 2025 and migration to HANA needs to be completed prior to this.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Aqua should monitor the SEW implementation and other customer affecting initiatives (i.e., Fiori applications, IVR upgrades) to ensure customer satisfaction metrics are maintained after go-live.</li> </ul>



## 3 IT observations

### Key findings

1	Executive summary
2	Scope
<b>3</b>	<b>IT observations</b>
4	Cybersecurity observations
5	Next steps
6	Appendix

Item	Description	Actions / Next Steps
<b>SAP Migration to S/4 HANA</b>	<ul style="list-style-type: none"> <li>▶ Based on the information presented, the Company appears to be migrating to Suite on HANA, which entails replacing its current database with HANA. However, Management stated that the Company is migrating to S/4 which would require business process change driven by new SAP functionality. We recommend that the Company confirm with SAP that their migration approach is indeed to S/4 HANA and not Suite on HANA.</li> <li>▶ <b>Migration of ECC to HANA, followed by CRM:</b> The Company is planning to migrate Finance/Enterprise Asset Management (EAM) ECC to HANA first followed by CRM. Doing so would have ECC and CRM on different support packs, which is not recommended. ECC and CRM are tightly integrated so having ECC and CRM on different kernel and support packs could have functional implications, thereby increasing risk. EY recommends that the entire stack is upgraded at once for both ECC and CRM altering Mercury's plan.</li> <li>▶ <b>ECC finance functionality:</b> There is an option to implement enhanced business processes for finance with a Suite on HANA migration. However, it is recommended that the Company should not adjust finance business processes until after the Aqua migration. Leaving the finance functionality as-is eliminates business process changes which may introduce additional risk.</li> <li>▶ <b>Migration of Mercury to S/4:</b> EAM and finance functionality will be impacted in a full S/4 migration thus Aqua and the Company would want to know those impacts to the business before proceeding.</li> <li>▶ <b>Timing of upgrade:</b> Based on timing of the start of the project in early 2019, Aqua should plan on executing a migration to HANA as part of the Company's migration onto the platform, so that the projects can be executed together. This assumes that Aqua does not want to wait for the Company's migration to S/4 HANA be completed, prior to integration. There is low incremental risk of executing both projects together but this would increase the current HANA migration budget by approximately \$1.5M to \$2.0M due to integration of Aqua. These are preliminary top-down estimates based on discussion with Aqua Management and EY's SAP Advisory practice.</li> <li>▶ <b>Migration sequence:</b> The Company indicated they could not break up the functional areas of finance, EAM and CIS. CIS can typically be separated and implemented independently; however, finance and EAM are tightly integrated due its use of compatible units.</li> </ul>	<ul style="list-style-type: none"> <li>▶ The Company is working with SAP to define their migration approach. Aqua should confirm the Company's migration approach to better understand functionality, timeline and budget impacts.</li> <li>▶ A full functional assessment needs to be completed before migrating the Company to S/4.</li> <li>▶ Aqua should plan on executing a migration to HANA as part of the Company's migration onto the platform.</li> <li>▶ Further diligence is recommended to develop detailed S/4 HANA migration roadmap and cost estimates.</li> <li>▶ Due to the integrated nature of the Company's SAP system, Aqua may need to consider migrating finance and EAM together. A functional assessment needs to be completed to validate a finance only versus finance and EAM migration.</li> </ul>



### 3 IT observations

#### Key findings

- 1 Executive summary
- 2 Scope
- 3 IT observations**
- 4 Cybersecurity observations
- 5 Next steps
- 6 Appendix

Item	Description	Actions / Next Steps
<b>SAP contract analysis</b>	<ul style="list-style-type: none"><li>■ [Redacted]</li><li>■ [Redacted]</li><li>■ [Redacted]</li><li>■ [Redacted]</li><li>■ [Redacted]</li><li>■ [Redacted]</li><li>■ [Redacted]</li><li>■ [Redacted]</li><li>■ [Redacted]</li></ul>	<ul style="list-style-type: none"><li>■ [Redacted]</li></ul>



### 3 IT observations

#### Key findings

- 1 Executive summary
- 2 Scope
- 3 IT observations**
- 4 Cybersecurity observations
- 5 Next steps
- 6 Appendix

Item	Description	Actions / Next Steps
<b>SAP contract analysis (Contd.)</b>	<ul style="list-style-type: none"><li>■ [Redacted]</li><li>■ [Redacted]</li></ul>	



## 3 IT observations

### Key findings

1	Executive summary
2	Scope
<b>3</b>	<b>IT observations</b>
4	Cybersecurity observations
5	Next steps
6	Appendix

Item	Description	Actions / Next Steps
<b>SAP Early Watch report</b>	<ul style="list-style-type: none"> <li>▶ The SAP Early Watch Report provides a health check of an SAP environment. It checks for service preparation and data quality of enterprise cache protocol (ECP), system configuration, SAP program errors, security, data volume management (DVM), database performance, and database administration, and provides insights into potential issues.</li> <li>▶ The Company conducts a check on its SAP environment by executing and reviewing the SAP Early Watch report on a weekly cadence. Whenever there is a major project or upgrade software, or infrastructure is reconfigured, the Company reviews the Early Watch Report with SAP. In addition, an SAP Solutions Architect reviews the report in detail.</li> <li>▶ Based on the report provided from the week of August 6, 2018, there are no material concerns. The report flagged the following alerts:               <ul style="list-style-type: none"> <li>▶ <b>Based on the data size and growth rate, problems regarding Data Volume Management are expected.</b> However, the Company utilizes a completely virtualized environment with automatic extension of data files as necessary. This auto-extend technology is not recognized by the tool and is flagged as a Red item. This configuration for auto-extend has been approved by SAP multiple times and hence is not a reason for concern.</li> <li>▶ <b>More than 30 ABAP dumps in the system.</b> This is by design and due to the fact that jobs (e.g., long running reports) running in foreground are canceled after 10 minutes to prevent performance degradation, and hence not a reason for concern.</li> <li>▶ <b>Readiness of system for SAP Remote Service has not been verified by running report RTCCTOOL.</b> The report highlights that Servicetools for Applications Plug-In for NetWeaver as of 7.31 are several versions behind and need to be updated. Management has stated that these will be updated as part of SAP's quarterly update.</li> <li>▶ <b>A high number of users have critical authorizations.</b> The Company uses a three pronged approach towards monitoring authorizations which lowers material concerns.                   <ul style="list-style-type: none"> <li>▶ Security is reviewed for system accounts (non-human users) required for processes such as Batch, Workflow, and Remote Function Calls.</li> <li>▶ The Company uses the Governance, Risk, and Compliance Control (GRC) module from SAP to monitor access control.</li> </ul> </li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>▶ The Company should continue to run the SAP Early Watch report on a periodic basis, review the findings with SAP, and take remedial action where needed.</li> </ul>



## 3 IT observations

### Key findings

1	Executive summary
2	Scope
<b>3</b>	<b>IT observations</b>
4	Cybersecurity observations
5	Next steps
6	Appendix

Item	Description	Actions / Next Steps
<b>SAP Early Watch report (Contd.)</b>	<ul style="list-style-type: none"> <li>▶ Security authorizations are reviewed by the Company's external auditor (Deloitte) annually. They have approved these authorizations.</li> <li>▶ Some additional considerations include the following:               <ul style="list-style-type: none"> <li>▶ Microsoft SQL Server 2012 support ends 2022, requiring an upgrade to a higher release prior to that timeline.</li> <li>▶ Microsoft Windows Server 2012 support ends in 2023, requiring an upgrade to a higher release prior to that timeline.</li> <li>▶ The SAP Kernel release is out of date and may need to be upgraded as part of the S/4 HANA migration.</li> <li>▶ There were no major performance problems in the database system. However, wait statistics for SQL Server show long wait times for certain event(s) because the average wait time exceeds the system threshold.</li> <li>▶ Database consistency checker (DBCC) job is not scheduled upon the advice of the SAP Solutions Architect. The reasons provided are as follows:                   <ul style="list-style-type: none"> <li>▶ The Company runs SQL Server in a High-Availability (H-A) configuration, and as such the nodes communicate and repair any type of physical data corruption in the system.</li> <li>▶ Running DBCC Check on a production system external to the H-A setup would create unnecessary load on the system for an extended amount of time.</li> </ul> </li> </ul> </li> <li>▶ We noted certain industry recommended practices being followed by the Company. Specifically, these include:               <ul style="list-style-type: none"> <li>▶ Security patches are monitored on a periodic basis and are applied as appropriate.</li> <li>▶ An appropriate cadence is in place to run and review the SAP Early Watch report.</li> </ul> </li> </ul>	





### 3 IT observations

#### Key findings

- 1 Executive summary
- 2 Scope
- 3 IT observations**
- 4 Cybersecurity observations
- 5 Next steps
- 6 Appendix

Item	Description	Actions / Next Steps
------	-------------	----------------------

**Legacy systems**

- ▶ Based on our analysis of the application portfolio, four out of 68 applications appear to be no longer under active vendor maintenance and support contracts. These include the following:

Application Name	Vendor Name	Business Capabilities Supported
Zeraware	Zeraware	Job site safety observations (JSSO)
CorrMD	Diversified Computer Group	Manage and track specialized, low-volume corrosion management inspection and testing activities
Lotus Notes	IBM	Development environment for building collaborative database applications. Notes is a legacy tool that was used by Dominion. Most of the Notes applications have been replaced by other systems. A few minor applications are still in use by the Rates Department but are slated for replacement when time permits.
Step7	Siemens	Used to operate three compressor stations

Source: Based on information provided by the Company

- ▶ Additionally, documentation provided by the Company indicates that eight to ten compressor stations are controlled by an outdated program and hardware that is no longer supported by the vendor. Replacing the application requires the engine to be rewired with new sensors, remote terminal units, and possibly replacing the engine itself; the total cost would be \$500,000 or more per station. The IT Capex project list did not include upgrade of these systems.
- ▶ Legacy applications lack robust features and functionality required by the business and customers, introduce security risks, and may require significant costs to upgrade or replace.

- ▶ The Company should upgrade or replace the legacy systems at the earliest.
- ▶ The Company should align the upgrades from older systems to newer systems such that there is:
  - ▶ No loss in functionality
  - ▶ Continuity of IT support and maintenance
  - ▶ Appropriate training to operate the newer systems
- ▶ The Company should replace the out of support compressor station system to avoid operational and reputational damage from system failure.



## 3 IT observations

### Key findings

1	Executive summary
2	Scope
<b>3</b>	<b>IT observations</b>
4	Cybersecurity observations
5	Next steps
6	Appendix

Item	Description	Actions / Next Steps																				
<b>IT organization structure and staffing</b>	<ul style="list-style-type: none"> <li>▶ The IT organization appears to be structured appropriately. The Company's Senior Vice President, Ms. Ruth Delost-Wylie leads the IT and OT organization. Her direct reports include: <ul style="list-style-type: none"> <li>▶ Mr. Joseph Brado (Chief Technical Director), who leads the IT department responsible for supporting applications.</li> <li>▶ Mr. Nagy Nagiub (Senior Director), who leads the corporate services and telecommunication teams including telecom analysts responsible for supporting operational technology.</li> <li>▶ Mr. Kevin Turkovich (Chief Cybersecurity Director), who leads the teams supporting cybersecurity, infrastructure and SCADA applications.</li> </ul> </li> <li>▶ The table below indicates the breakdown of IT resources by function. <table border="1"> <thead> <tr> <th>IT Department</th> <th>Employees</th> <th>Contractors</th> <th>Total</th> </tr> </thead> <tbody> <tr> <td>Applications</td> <td>22</td> <td>10</td> <td>32</td> </tr> <tr> <td>Telecom and helpdesk</td> <td>20</td> <td>2</td> <td>22</td> </tr> <tr> <td>Cyber, Infrastructure and SCADA apps</td> <td>13</td> <td>2</td> <td>15</td> </tr> <tr> <td></td> <td><b>55</b></td> <td><b>14</b></td> <td><b>69</b></td> </tr> </tbody> </table> <p>Source: Based on information provided by the Company</p> </li> <li>▶ The Company relies on a significant number of independent contractors (approximately 31%) to support its IT environment, in comparison with industry benchmark median of 7.7% (source: Computer Economics benchmarks for Energy and Utilities, 2018-19). Operational risks of leveraging independent contractors include attrition of key resources, loss of intellectual property, lack of control over performance and quality of work delivered.</li> <li>▶ The IT and OT teams are closely integrated. Mr. Naquib's team includes a manager and six IT technicians who provide support for all SCADA network, fiber network, microwave network, MAS (multiple address) radio network and over 2000 field devices.</li> <li>▶ Management stated that the IT organization is adequately staffed and that there are no open positions.</li> </ul>	IT Department	Employees	Contractors	Total	Applications	22	10	32	Telecom and helpdesk	20	2	22	Cyber, Infrastructure and SCADA apps	13	2	15		<b>55</b>	<b>14</b>	<b>69</b>	<ul style="list-style-type: none"> <li>▶ The Company should re-assess its staffing mix to ensure an appropriate ratio of employees, outsourced providers, and independent contractors. Benefits may include: <ul style="list-style-type: none"> <li>▶ Greater accountability and oversight</li> <li>▶ Diversification of outsourced providers</li> <li>▶ Flexibility to expand and contract the team with economic conditions</li> <li>▶ Access to appropriate skill sets to manage the major transformation currently underway</li> </ul> </li> </ul>
IT Department	Employees	Contractors	Total																			
Applications	22	10	32																			
Telecom and helpdesk	20	2	22																			
Cyber, Infrastructure and SCADA apps	13	2	15																			
	<b>55</b>	<b>14</b>	<b>69</b>																			



## 3 IT observations

### Key findings

1	Executive summary
2	Scope
<b>3</b>	<b>IT observations</b>
4	Cybersecurity observations
5	Next steps
6	Appendix

Item	Description	Actions / Next Steps
<b>IT sourcing strategy</b>	<ul style="list-style-type: none"> <li>▶ Management stated that the Company's internal IT team is focused on "keeping the lights on" support and maintenance of the IT systems and infrastructure. Approximately 10% of the IT team's effort is spent on capital projects. The Company typically leverages outsourcing and consulting support to execute its discretionary projects.</li> <li>▶ Additionally, the Company leverages an outsourced program management office (PMO) model where the project managers (PMs) can be dynamically staffed based on project load. The PMs report to a PMO director, who reports to Mr. Brado.</li> <li>▶ While it is not uncommon for organizations to leverage consulting support to deliver discretionary projects, over reliance on vendors may lead to the following challenges and risks: <ul style="list-style-type: none"> <li>▶ The internal team will have limited opportunities to upskill themselves.</li> <li>▶ Additional effort and cost may be needed to transition knowledge from the consulting resources to employees at the end of discretionary projects.</li> <li>▶ Employees may be demotivated due to lack of opportunities to work on newer technologies and projects.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>▶ Aqua and the Company should collectively evaluate the IT sourcing strategy for the combined business.</li> </ul>
<b>Quality of IT leadership</b>	<ul style="list-style-type: none"> <li>▶ The IT Management team appears to be competent and knowledgeable about the Company's IT environment. Ms. Delost-Wylie and her team have had experience building out the Company's IT environment from the ground up, and have integrated three recent acquisitions. The IT Management team has a proven track record of bringing acquired companies into the SAP landscape seamlessly with minimal negative impact to customer satisfaction metrics. Additionally during the Management discussions they were able to sufficiently articulate their vision for continuing to align IT with business objectives.</li> <li>▶ Given that there are several large scale IT in-flight initiatives, it is critical that Ms. Delost-Wylie, Mr. Brado, Mr. Nagiub and Mr. Turkovich continue with the Company to prevent loss of knowledge and minimize disruption due to this transaction.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Aqua should consider a retention strategy for critical IT Management resources.</li> </ul>



## 3 IT observations

### Key findings

1	Executive summary
2	Scope
<b>3</b>	<b>IT observations</b>
4	Cybersecurity observations
5	Next steps
6	Appendix

Item	Description	Actions / Next Steps
<b>IT vendor relationships</b>	<ul style="list-style-type: none"> <li>▶ The Company leverages the services of reputable vendors such as SAP, Oracle, and Microsoft for applications; Cisco, GE, and Verizon for telecom; and Dell and VMWare for IT infrastructure.</li> <li>▶ Documentation provided by the Company indicates that there are no issues with any of its vendors other than dissatisfaction with MiCustomer ePortal from Avertra. The vendor continued to fall behind on delivery dates for system enhancements. The Company formally notified Avertra of termination of services, and is currently implementing SAP Hybris SS for Utilities by SEW (Smart Energy Water) Cloud. We have not been provided a detailed plan or roadmap which highlights that the replacement solution will be implemented prior to termination of the Avertra contract [OPEN].</li> </ul>	<ul style="list-style-type: none"> <li>▶ Aqua should monitor the replacement of MiCustomer ePortal with SAP Hybris SS for Utilities by SEW Cloud.</li> </ul>
<b>Software licensing compliance</b>	<ul style="list-style-type: none"> <li>▶ The Company appears to be following appropriate practices for software asset tracking for monitoring usage and license compliance: <ul style="list-style-type: none"> <li>▶ The Company tracks all software deployed with an automated software discovery tool that scans every computer on its network and builds a comprehensive inventory. At least annually, it compares the number of installed instances to license agreements and reconciles with the vendors if it is out of compliance.</li> <li>▶ Microsoft (MS) Operating Systems (OS) and MS products are tracked monthly using a software discovery tool (BMC-Numara). The inventory is checked against purchased licenses and adjustments are done on quarterly basis.</li> <li>▶ All network equipment licenses are perpetual and purchased when equipment is ordered.</li> <li>▶ SAP typically conducts an automated license audit every year and the Company works with them on the results to true up any exceptions.</li> </ul> </li> <li>▶ IT application owners monitor license usage for their assigned applications on an ongoing basis so that the Company can plan ahead for any required purchases and avoid situations where users cannot access systems due to license shortages. Licensing impacts are also assessed as part of projects that involve deployments of new software or deployments of existing software to new user groups.</li> </ul>	<ul style="list-style-type: none"> <li>▶ The Company should continue to perform licensing true-up exercises at the established cadence.</li> </ul>



## 3 IT observations

### Key findings

1	Executive summary
2	Scope
<b>3</b>	<b>IT observations</b>
4	Cybersecurity observations
5	Next steps
6	Appendix

Item	Description	Actions / Next Steps
<b>IT disaster recovery (DR) capabilities</b>	<ul style="list-style-type: none"> <li>▶ The Company appears to have robust IT and OT disaster recovery capabilities which includes local and cross-site redundancy, rapid failover of critical applications, and multiple back-up and recovery options for systems.               <ul style="list-style-type: none"> <li>▶ Applications: All application servers have redundancy depending on criticality and vendor supported technology. Redundancy is provided either through multiple active servers with nodes at both data centers, or through hot standby servers at the alternate data center (DC). All application servers are also backed up with copies at both DCs.</li> <li>▶ Databases (DB): 95% of all DBs are part of a SQL Server 'always-on' group with nodes at primary and alternate DCs. The other 5% have redundancy and backup currently provided for and are in the process of being moved to the main group.</li> <li>▶ Call center technologies: Applications, IVR, call routing, chat, email, call recording, workforce management and call backs are configured for hot standby, and are on active-active configuration.</li> <li>▶ Files: File servers have redundancy through hot standby servers at the alternate DC;</li> <li>▶ Infrastructure: All critical infrastructure servers have redundancy and are backed up with copies stored at both data centers.</li> <li>▶ Data network: All critical components are configured for automatic failover and redundancy;</li> <li>▶ SCADA: All application servers and databases have redundancy with hot standby nodes at the alternate data center that are kept in sync with proprietary technology that comes with the system. All workstations have redundancy with extra workstations at the primary site and the alternate site.</li> </ul> </li> <li>▶ It is to be noted that Compressor Control Workstations do not have redundancy; however, the Company regularly makes full system images and backs up the data to a local storage device on a daily basis. In the event of a workstation failure there may be a disruption to operations while a replacement workstation is set-up and data restored from back-ups.</li> <li>▶ Documentation provided indicates that the Company conducts DR testing annually; however, test results have not been provided as yet. <b>[OPEN]</b></li> </ul>	<ul style="list-style-type: none"> <li>▶ The Company should analyze the recovery time objective (RTO) and recovery point objectives (RPO) of Compressor Control Workstations and determine whether redundancy is required. It should maintain these devices under warranty support and perform periodic refresh as per industry standard practice.</li> </ul>



## 3 IT observations

### Key findings

1	Executive summary
2	Scope
<b>3</b>	<b>IT observations</b>
4	Cybersecurity observations
5	Next steps
6	Appendix

Item	Description	Actions / Next Steps
<b>IT internal controls</b>	<ul style="list-style-type: none"> <li>▶ The Company is not currently SOX compliant but performs ad hoc assessments in compliance with Commonwealth of Pennsylvania law such as the Cybersecurity Capability Maturity Model (C2M2). In addition, the Pennsylvania Public Utility Commission requires an annual submission of a Public Utility Security Planning and Readiness self-certification. As such, the Company is required to prepare, update and test their cybersecurity and business continuity plans each year.</li> <li>▶ The Company provided documentation for their IT internal control practices. The following processes and procedures were assessed in order to identify potential gaps:               <ul style="list-style-type: none"> <li>▶ Identity and Access Management Plan.</li> <li>▶ IT Incident Problem Change Management.</li> </ul> </li> <li>▶ Management stated that the Company maintains role based security within SAP, using the GRC module, and performs access certifications regularly. The Company performs much of its work with contracted employees. Upon reviewing the Company's policy documentation, it was noted that the documentation did not include specifications on particularly privileged users. This included the monitoring of user access granted to temporarily contracted employees and the utilization of SAP's Firefighter ID.</li> <li>▶ Overall, the IT control environment appears appropriate for a non-public company. However, there are certain key items to consider with regards to SOX compliance, as noted in the "Actions / Next Steps".</li> </ul>	<ul style="list-style-type: none"> <li>▶ If SOX requirements will be applicable the Company will need to:               <ul style="list-style-type: none"> <li>▶ Establish and enhance risk and control matrices.</li> <li>▶ Perform a controls readiness assessment.</li> <li>▶ Perform testing of their controls to support Management's opinion.</li> <li>▶ Perform training for key control owners to align upon additional documentation requirements and any required process adjustments identified in controls design assessment.</li> </ul> </li> <li>▶ It is suggested that the Company update their policies and procedures in order to provide more robust information regarding their processes and IT internal control practices. The Company should include specific control considerations in the following areas:               <ul style="list-style-type: none"> <li>▶ Temporarily contracted users should fall under specific policies within the Target's IT internal control framework so as to be able to adequately monitor their privileges within the system.</li> <li>▶ Privileged access to perform sensitive transactions.</li> <li>▶ Segregation of duties in the access administration process.</li> <li>▶ Segregation of duties in the change management process. If access to develop and promote changes to the production environment cannot be segregated, then guidance around change migration monitoring should be in place (e.g. firefighter process).</li> </ul> </li> </ul>





## 3 IT observations

### Key findings

1	Executive summary
2	Scope
<b>3</b>	<b>IT observations</b>
4	Cybersecurity observations
5	Next steps
6	Appendix

Item	Description	Actions / Next Steps																											
<b>Infrastructure refresh cycle</b>	<ul style="list-style-type: none"> <li>Documentation provided states that the Company follows a regular refresh cycle for its infrastructure assets and almost all IT and OT infrastructure is refreshed before it reaches end of vendor support.</li> <li>Analysis of the Company's refresh cycle indicates that it may be extending usage of certain infrastructure components beyond typical end of life. As an example, the Company is currently deploying Microsoft Windows 10 on new laptops, and desktops. The Company's hardware replacement guidelines and comparison with industry standards is summarized below: <table border="1"> <thead> <tr> <th>Hardware Assets</th> <th>Company</th> <th>Industry Standard</th> </tr> </thead> <tbody> <tr><td>Servers</td><td>4-6 years</td><td>4-6 years</td></tr> <tr><td>Storage devices</td><td>5-7 years</td><td>4-6 years</td></tr> <tr><td>Network devices</td><td>4-7 years</td><td>4-6 years</td></tr> <tr><td>Communication devices</td><td>4-7 years</td><td>4-6 years</td></tr> <tr><td>Laptops</td><td>4-5 years</td><td>3-4 years</td></tr> <tr><td>Desktops</td><td>5-6 years</td><td>3-4 years</td></tr> <tr><td>Printers</td><td>5-7 years</td><td>4-6 years</td></tr> <tr><td>Mobile phones</td><td>Every 3 years</td><td>2-3 years</td></tr> </tbody> </table> <p>Source: Based on information provided by the Company and EY analysis</p> </li> </ul>	Hardware Assets	Company	Industry Standard	Servers	4-6 years	4-6 years	Storage devices	5-7 years	4-6 years	Network devices	4-7 years	4-6 years	Communication devices	4-7 years	4-6 years	Laptops	4-5 years	3-4 years	Desktops	5-6 years	3-4 years	Printers	5-7 years	4-6 years	Mobile phones	Every 3 years	2-3 years	<ul style="list-style-type: none"> <li>The Company should refresh IT infrastructure as per industry standard practices and keep hardware under active warranty support.</li> <li>The Company should ensure that desktop applications are at the appropriate version to ensure smooth integration with the SAP S/4 HANA systems. Additional capital and operations and maintenance (O&amp;M) spending may be required.</li> </ul>
Hardware Assets	Company	Industry Standard																											
Servers	4-6 years	4-6 years																											
Storage devices	5-7 years	4-6 years																											
Network devices	4-7 years	4-6 years																											
Communication devices	4-7 years	4-6 years																											
Laptops	4-5 years	3-4 years																											
Desktops	5-6 years	3-4 years																											
Printers	5-7 years	4-6 years																											
Mobile phones	Every 3 years	2-3 years																											
	<ul style="list-style-type: none"> <li>We have not been provided the IT infrastructure inventory and hence have not been able to conduct a detailed assessment of the age, warranty and vendor support for infrastructure components. <b>[OPEN]</b></li> </ul>																												



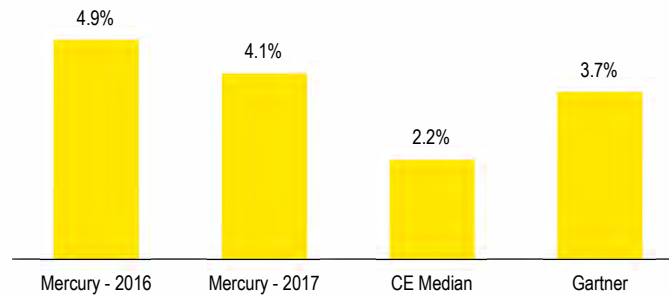
### 3 IT observations

#### Key findings

- 1 Executive summary
- 2 Scope
- 3 IT observations**
- 4 Cybersecurity observations
- 5 Next steps
- 6 Appendix

Item	Description	Actions / Next Steps
<b>IT and OT spending</b>	<ul style="list-style-type: none"> <li>▶ The Company's IT spending appears to be consistently above industry benchmarks. The spending in FY16 and FY17 is 4.9% and 4.1% of revenues, respectively as compared to industry benchmarks range of 2.2% to 3.2% percent. The IT spending is higher than benchmarks because operational technology costs are also included in the IT spend. This is as expected.</li> </ul>	<ul style="list-style-type: none"> <li>▶ The Company should evaluate its IT capital expenditure and overall IT spend, and identify opportunities to optimize while continuing to support business growth.</li> </ul>

IT spending as % of revenue



- ▶ The IT capex amounts show variability across the years. The \$10M increase in the budgeted IT capex costs for FY2018 is due to multiple upgrade projects that are already planned. These include SAP CRM enhancements, portal enhancements, and customer service and billing systems migration.

(000's)	2016	2017	2018	2019	2020	2021	2022	2023
Type	Actual	Actual	Budget	Forecast	Forecast	Forecast	Forecast	Forecast
IT Capex	11,562	10,455	21,515	21,585	15,899	13,187	27,260	18,360



## 3 IT observations

### Key findings

1	Executive summary
2	Scope
<b>3</b>	<b>IT observations</b>
4	Cybersecurity observations
5	Next steps
6	Appendix

Item	Description	Actions / Next Steps
<b>Software development lifecycle methodology</b>	<ul style="list-style-type: none"> <li>▶ The Company has traditionally followed a Waterfall based approach for software development. More recently, it has been using the more modern, Agile-type approach on certain development projects. Instead of organizing the work into Waterfall phases as above, it conducts requirements, design, development work in sprints and deploys the results to production incrementally. The Company has not yet adopted a full-scale Agile methodology because its project volume has not justified it, but will continue to assess its applicability moving forward.</li> <li>▶ As a result of two software development methodologies (Waterfall and Agile), the Company will need to contend with parallel processes to support each. Typically significant training effort and change management are required to drive the transition from Waterfall to Agile.</li> </ul>	<ul style="list-style-type: none"> <li>▶ The Company should ensure that its resources are adequately trained and its processes adaptable to support Agile delivery.</li> </ul>
<b>IT integration methodology</b>	<ul style="list-style-type: none"> <li>▶ The Company's integration philosophy is to rapidly merge any acquired entities while improving customer experience and closely aligning IT and Operations.</li> <li>▶ The Company has demonstrated a successful track record of integrating prior acquisitions such as Equitable Gas.</li> <li>▶ The Company leverages the following components for successful integrations: <ul style="list-style-type: none"> <li>▶ Strong program management office (PMO), with a knowledgeable and Agile team;</li> <li>▶ Industry leading frameworks (e.g. Zachman framework) to quickly understand business processes;</li> <li>▶ ASAP (Accelerated SAP) methodology to optimize time, resources, and quality;</li> <li>▶ Identification of key risks and customer support objectives;</li> <li>▶ Detailed planning and Agile execution; and</li> <li>▶ Leverage automated interfaces to connect systems.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>▶ Aqua should leverage the Company's integration methodology (where feasible) for this transaction.</li> </ul>



## 3 IT observations

### Key findings

1	Executive summary
2	Scope
<b>3</b>	<b>IT observations</b>
4	Cybersecurity observations
5	Next steps
6	Appendix

Item	Description	Actions / Next Steps
<b>IT integration of Aqua and Mercury</b>	<ul style="list-style-type: none"> <li>▶ Aqua is planning to acquire and merge Mercury's operations with itself. It intends to leverage a common set of IT systems and infrastructure where feasible.</li> <li>▶ If the transaction is successful, there would be certain business priorities for Day 1 that would need to be enabled by IT. Unless Day 1 readiness is adequately planned and executed, there could be challenges in meeting Day 1 requirements.</li> <li>▶ Preliminary analysis indicates that there is limited overlap between key systems used by Aqua and the Company [Refer to next page for details of key systems used by Aqua and the Company]. Additionally, as noted earlier, the Company is in the process of a major SAP upgrade program. Hence, IT integration will require greater effort and focus to avoid business disruption, cost overruns, delays and customer impact.</li> </ul>	<p><b>Sign-to-close:</b></p> <ul style="list-style-type: none"> <li>▶ Aqua should create a detailed plan for an accelerated integration. Below are a preliminary set of considerations: <ul style="list-style-type: none"> <li>▶ Understand Day 1 business imperatives and kick-off IT initiatives to achieve Day 1 priorities.</li> <li>▶ Establish guiding principles for IT integration.</li> <li>▶ Establish IT integration governance and reporting.</li> <li>▶ Develop IT integration plan, leveraging industry standard playbook: <ul style="list-style-type: none"> <li>▶ Assess overlapping capabilities between Aqua and the Company.</li> <li>▶ Develop the IT operating model (systems, infrastructure, vendors, organization and processes) for the combined businesses.</li> <li>▶ Assess and re-prioritize IT initiatives at Aqua and at the Company, where needed.</li> <li>▶ Sequence IT integration initiatives, develop cost estimates and timelines to achieve.</li> <li>▶ Publish request for proposals (RFP) where vendor support is needed.</li> <li>▶ Establish change management and communication procedures.</li> <li>▶ Identify key risks and develop mitigation measures.</li> </ul> </li> </ul> </li> </ul> <p><b>Post-close:</b></p> <ul style="list-style-type: none"> <li>▶ Review RFPs and select appropriate vendor partners for IT integration.</li> <li>▶ Continue to refine target IT operating model for the combined business.</li> <li>▶ Drive IT integration across key areas: <ul style="list-style-type: none"> <li>▶ The Company's SAP ERP system – finance and accounting, reporting, supply chain</li> <li>▶ Customer facing technologies</li> <li>▶ Customer service and CRM</li> <li>▶ HRIS and payroll</li> <li>▶ Enterprise work and asset management</li> <li>▶ SCADA systems</li> <li>▶ Document management</li> <li>▶ Environment, health and safety</li> <li>▶ Regulatory and compliance</li> <li>▶ Software tools and end user computing</li> <li>▶ Infrastructure hosting and networks</li> </ul> </li> <li>▶ Right-size and design the IT organization and outsourcing model to support the combined business.</li> </ul>



### 3 IT observations

#### Preliminary comparison of key IT systems

1	Executive summary
2	Scope
<b>3</b>	<b>IT observations</b>
4	Cybersecurity observations
5	Next steps
6	Appendix

Function	Aqua	Mercury
Phones	Avaya	Atos (Unify, Siemens).HiPath 4K PBX Platform
Email	Office 365 (cloud)	MS Exchange
Middleware Integrations	(In design to rebuild)	SAP Process Integration (PI), vendor APIs, custom-developed programs, and scripts
Business Intelligence	Qlik	SAP S/4HANA Toolset
Document Management	MHC and On Base	Preceptive Content
HRIS	Workday (cloud)	SAP ECC
Time tracking	Kronos (cloud)	Workforce Software (cloud)
CIS	Banner (on prem)	SAP ECC (on prem)
Website	(Building new site with Sitecore)	Avertra/SAP SEW for Utilities
Call Center front-end		SAP Fiori Multi-Channel Functionality
IVR	Nuance	Genesys
Other Customer Ops	Knowledge Owl,	SAP customer relationship management for utilities
FIS	Lawson (on prem)	SAP ECC
Capital Assets		Power plant (on prem)
Consolidations, Financial Rpting		Hyperion (on prem)
Asset Mgmt	Maintenance Connection (on prem)	SAP ECC
Workforce Mgmt	Service Link (on prem)	Ventyx/Service Suite
Compliance Work Management		GL/Essentials
Spatial Modeling		ESRI GIS (on prem)
EHS	Cority	Zeraware
Business Intelligence	Qlik?	SAP S/4 HANA
Meter Reading	AMR	
SCADA	Various	Telvent
Gas Management	N/A	Ensyte
Gas Measurement	N/A	Telvent
Land Records	N/A	P2 Tobin

Source: Based on information provided by Aqua and the Company

# 4

## Cybersecurity observations

In this section	Page
Key findings	33





## 4 Cybersecurity observations

### Key findings

- 1 Executive summary
- 2 Scope
- 3 IT observations
- 4 Cybersecurity observations**
- 5 Next steps
- 6 Appendix

Item	Description	Actions / Next Steps
<b>Data privacy program overview</b>	<ul style="list-style-type: none"> <li>▶ The Company stated that it possesses personally identifiable information (PII) and protected health information (PHI) for over 700,000 customers and 3,000 employees (including dependents and retirees). As a result, it is required to comply with federal laws such as the Federal Trade Commission (FTC) Act and the Health Information Portability and Accountability Act (HIPAA) as well as state privacy laws in Pennsylvania, West Virginia and Kentucky.</li> <li>▶ While the Company seems to have an understanding of its data privacy regulatory requirements and has designated the Chief Cybersecurity Director as its Data Privacy Officer, there does not appear to be a formal data privacy program in place. For instance, a formal privacy program would include a documented privacy strategy, privacy framework, concepts and procedures such as privacy by design, privacy impact assessments or third party privacy audits; none of which appear to be implemented. Management stated that the Cybersecurity team conducts biannual security assessment meetings with every business unit where the handling of sensitive PII is discussed, but there is no independent third party privacy audit.</li> <li>▶ Lack of compliance with data privacy regulatory requirements could lead to litigation, mandatory audits, monetary fines and reputational damage.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Post-close, develop a formal privacy program including but not limited to the following:               <ul style="list-style-type: none"> <li>▶ A formal privacy strategy</li> <li>▶ A privacy framework</li> <li>▶ Privacy concepts and procedures such as privacy by design, privacy impact assessments (PIAs) etc.</li> <li>▶ Third party privacy audits</li> <li>▶ Ongoing performance measurement.</li> </ul> </li> </ul>



## 4 Cybersecurity observations

### Key findings

- 1 Executive summary
- 2 Scope
- 3 IT observations
- 4 Cybersecurity observations**
- 5 Next steps
- 6 Appendix

Item	Description	Actions / Next Steps
<b>Website security</b>	<ul style="list-style-type: none"> <li>▶ Bitsight website scan reports were acquired on the Company's main website, peoples-gas.com, as well as their consumer portal, peopleseaccount.com. These reports identify certain potential security issues which the Company can validate and address to help protect the Company from a data breach.</li> </ul> <p><b>Peoples-gas.com:</b></p> <ul style="list-style-type: none"> <li>▶ While the Company implements the Sender Policy Framework (SPF) email protocol, it does not also implement the newer Domain Keys Identified Mail (DKIM) which would add an extra layer of reputational protection and reduce spam. Without these protocols, legitimate emails from the Company are more likely to be treated as junk email, or able to have a spammer send emails pretending to be from the Company, potentially damaging its reputation.</li> <li>▶ Websites were lacking security headers which can protect sensitive information in transit.</li> <li>▶ Certain instances were identified where websites allowed obsolete encryption (TLS 1.0) or hashing algorithms (SHA-1), or where certificates had expired.</li> <li>▶ Trackstar.peoples-gas.com has a certificate that the Chrome browser will not allow to be used, due to a compromise at the Symantec certificate authority. This certificate should be replaced with a new certificate.</li> </ul> <p><b>Peopleseaccount.com:</b></p> <ul style="list-style-type: none"> <li>▶ No SPF or DKIM implementations were identified for this domain. If the domain does not send email, this may not be a problem, but industry practice recommends implementing SPF and DKIM on all domains that are used by consumers.</li> <li>▶ The site allows the obsolete encryption algorithms SSLv3 and TLS 1.0.</li> <li>▶ A port used by Microsoft Remote Desktop was identified, which may indicate remote access to the web server is open to the Internet. This should be secured to allow access only from within the Company, or require multi-factor authentication if that is not feasible.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Post-close, the Company should validate and correct these issues.</li> </ul>



## 4 Cybersecurity observations

### Key findings

- 1 Executive summary
- 2 Scope
- 3 IT observations
- 4 Cybersecurity observations**
- 5 Next steps
- 6 Appendix

Item	Description	Actions / Next Steps
<b>Dark Web searches identified no Company-specific targeting</b>	<ul style="list-style-type: none"> <li>▶ EY conducted searches of the Dark Web for mentions about the Company, its principals, products and services. No mention of the Company was identified.</li> <li>▶ Searches were also conducted in relation to the gas delivery industry, which revealed some groups who vandalize equipment and also advocate hacking. There were no direct threats to the Company identified. Since the Company is a public utility, it is essential that the Company maintain vigorous threat intelligence gathering on these threats and conduct rigorous security testing on its systems reduce the chance of a hacking attempt being successful.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Post-close, the Company should continue to leverage industry groups and independent research to maintain awareness of threats targeting public utilities.</li> </ul>
<b>Cybersecurity Insurance needs to be evaluated in terms of regulation in Pennsylvania state</b>	<ul style="list-style-type: none"> <li>▶ The Company has a Critical Asset Protection insurance with a \$30 million per-claim coverage limit, but the insurer is not licensed by the Pennsylvania Insurance department, and is subject to limited regulation. The insurance is not covered by the Pennsylvania Property and Casualty Insurance Guaranty Association.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Post-close, the Company should assess the impact of limited regulation of the insurer.</li> </ul>
<b>Web Application vulnerability scan</b>	<ul style="list-style-type: none"> <li>▶ The Company is in the process of deploying Rapid7 AppSpider to perform application code scans to identify vulnerabilities. The frequency and deployment plan are being determined.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Post-close, Aqua should review the Company's deployment plans to determine if this should be accelerated.</li> </ul>

# 5

## Next steps

In this section	Page
Next steps	37



## 5 Next steps

### Next steps

- 1 Executive summary
- 2 Scope
- 3 IT observations
- 4 Cybersecurity observations
- 5 Next steps**
- 6 Appendix

## Pre-sign

1. Aqua's legal counsel should review the SAP and other key IT contracts to understand if there are any change of ownership limitations or additional cost.

Contract review

## Sign-to-close

1. Aqua should consider a retention strategy for the Company's IT Management resources.
2. Aqua should create a detailed plan for an accelerated integration. Below are a preliminary set of considerations:
  - a) Understand Day 1 business imperatives and kick-off IT initiatives to achieve Day 1 priorities
  - b) Establish guiding principles for IT integration
  - c) Establish IT integration governance and reporting
  - d) Develop IT integration plan, leveraging industry standard playbook:
    - I. Assess overlapping capabilities between Aqua and the Company.
    - II. Develop the IT operating model (systems, infrastructure, vendors, organization and processes) for the combined businesses.
    - III. Assess and re-prioritize IT initiatives at Aqua and at the Company, where needed.
    - IV. Sequence IT integration initiatives, develop cost estimates and timelines to achieve.
    - V. Publish request for proposals (RFP) where vendor support is needed.
    - VI. Establish change management and communication procedures.
    - VII. Identify key risks and develop mitigation measures.

Retention of IT Management

Day 1 readiness and integration planning



## 5 Next steps

### Next steps

- 1 Executive summary
- 2 Scope
- 3 IT observations
- 4 Cybersecurity observations
- 5 Next steps**
- 6 Appendix

## Post-close

1. Further diligence is needed to understand the discrepancy between the IT project budget and the IT capex budget.
2. Aqua should closely monitor the status and progress of in-flight projects as such large scale implementations run the risk of delays, cost overruns and customer impact.
3. Aqua should monitor the post go-live period closely to ensure customer satisfaction metrics are maintained at their current levels.
4. Additionally, Aqua should analyze the portfolio of planned projects and make adjustments to meet its integration objectives.
5. Aqua should monitor the SEW implementation and other customer affecting initiatives (i.e., Fiori applications, IVR upgrades) to ensure customer satisfaction metrics are maintained after go-live.
6. The Company is working with SAP to define their migration approach. Aqua should confirm the Company's migration approach to better understand functionality, timeline and budget impacts.
7. A full functional assessment needs to be completed before migrating the Company to S/4.
8. Aqua should plan on executing a migration to HANA as part of the Company's migration onto the platform.
9. Further diligence is recommended to develop detailed S/4 HANA migration roadmap and cost estimates.
10. Due to the integrated nature of the Company's SAP system, Aqua may need to consider migrating finance and EAM together. A functional assessment needs to be completed to validate a finance only versus finance and EAM migration.
11. The Company should continue to run the SAP Early Watch report on a periodic basis, review the findings with SAP, and take remedial action where needed.
10. The Company should upgrade or replace the legacy systems at the earliest.
11. The Company should align the upgrades from older systems to newer systems such that there is:
  - a) No loss in functionality;
  - b) Continuity of IT support and maintenance; and
  - c) Appropriate training to operate the newer systems.
12. The Company should replace the out of support compressor station system to avoid operational and reputational damage from system failure.

**IT projects  
in-flight**

**SAP**

**Legacy  
upgrade**



## 5 Next steps

### Next steps

- 1 Executive summary
- 2 Scope
- 3 IT observations
- 4 Cybersecurity observations
- 5 Next steps**
- 6 Appendix

## Post-close

13. Aqua should participate in the CIC reviews and make adjustments to meet its integration objectives.
14. The Company should re-assess its staffing mix to ensure an appropriate ratio of employees, outsourced providers, and independent contractors. Benefits include:
  - a) Greater accountability and oversight
  - b) Diversification of outsourced providers
  - c) Flexibility to expand and contract the team with economic conditions
  - d) Access to appropriate skill sets to manage the major transformation currently underway
15. Aqua and the Company should collectively evaluate the IT sourcing strategy for the combined business.
16. Aqua should monitor the replacement of MiCustomer ePortal with SAP Hybris SS for Utilities by SEW Cloud.
17. The Company should continue to perform licensing true-up exercises at the established cadence.
18. The Company should analyze the recovery time objective (RTO) and recovery point objectives (RPO) of Compressor Control Workstations and determine whether redundancy is required. It should maintain these devices under warranty support and perform periodic refresh as per industry standard practice.

IT strategy and governance

IT organization

IT sourcing strategy

IT vendor relationships

Software licensing compliance

IT disaster recovery (DR) capabilities



## 5 Next steps

### Next steps

1	Executive summary
2	Scope
3	IT observations
4	Cybersecurity observations
<b>5</b>	<b>Next steps</b>
6	Appendix

## Post-close

19. If SOX requirements will be applicable the Company will need to:
- Establish and enhance risk and control matrices.
  - Perform a controls readiness assessment.
  - Perform testing of their controls to support Management's opinion.
  - Perform training for key control owners to align upon additional documentation requirements and any required process adjustments identified in controls design assessment.
20. It is suggested that the Company update their policies and procedures in order to provide more robust information regarding their processes and IT internal control practices. The Company should include specific control considerations in the following areas:
- Temporarily contracted users should fall under specific policies within the Target's IT internal control framework so as to be able to adequately monitor their privileges within the system.
  - Privileged access to perform sensitive transactions.
  - Segregation of duties in the access administration process.
  - Segregation of duties in the change management process. If access to develop and promote changes to the production environment cannot be segregated, then guidance around change migration monitoring should be in place (e.g. firefighter process).
21. The Company should refresh IT infrastructure as per industry standard practices and keep hardware under active warranty support.
22. The Company should ensure that desktop applications are at the appropriate version to ensure smooth integration with the SAP S/4 HANA systems. Additional capital and operations and maintenance (O&M) spending may be required.

**IT internal  
controls**

**Infrastructure  
refresh cycle**





## 5 Next steps

### Next steps

- 1 Executive summary
- 2 Scope
- 3 IT observations
- 4 Cybersecurity observations
- 5 Next steps**
- 6 Appendix

## Post-close

23. The Company should evaluate its IT capital expenditure and overall IT spend, and identify opportunities to optimize while continuing to support business growth.
24. The Company should ensure that its resources are adequately trained and its processes adaptable to support Agile delivery.
25. Aqua should leverage the Company's integration methodology (where feasible) for this transaction.
26. Develop a formal privacy program including but not limited to the following:
  - a) A formal privacy strategy
  - b) A privacy framework
  - c) Privacy concepts and procedures such as privacy by design, privacy impact assessments (PIAs) etc.
  - d) Third party privacy audits
  - e) Ongoing performance measurement.
27. The Company should validate and correct these issues.
28. The Company should continue to leverage industry groups and independent research to maintain awareness of threats targeting public utilities.
29. The Company should assess the impact of limited regulation of the insurer.
30. Aqua should review the Company's deployment plans to determine if this should be accelerated.

IT and OT spending

Software development lifecycle methodology

IT integration methodology

Cyber



## 5 Next steps

### Next steps

- 1 Executive summary
- 2 Scope
- 3 IT observations
- 4 Cybersecurity observations
- 5 Next steps**
- 6 Appendix

## Post-close

30. Review RFPs and select appropriate vendor partners for IT integration.
31. Continue to refine target IT operating model for the combined business.
32. Drive IT integration across key areas:
  - a) The Company's SAP ERP system – finance and accounting, reporting, supply chain
  - b) Customer facing technologies
  - c) Customer service and CRM
  - d) HRIS and payroll
  - e) Enterprise work and asset management
  - f) SCADA systems
  - g) Document management
  - h) Environment, health and safety
  - i) Regulatory and compliance
  - j) Software tools and end user computing
  - k) Infrastructure hosting and networks
33. Right-size and design the IT organization and outsourcing model to support the combined business.

**IT integration  
execution**

# 6

## Appendix

In this section	Page
Appendix A: Definitions and abbreviations	44
Appendix B: Description of key systems	45
Appendix C: Procedures performed – IT	47
Appendix D: Procedures performed – Cyber	50
Appendix E: SAP licensing details	51
Appendix F: Cybersecurity open source findings (Peoples-gas.com)	55
Appendix F: Cybersecurity open source findings (Peopleseaccount.com)	56



## 6 Appendix

### Appendix A: Definitions and abbreviations

1	Executive summary
2	Scope
3	IT observations
4	Cybersecurity observations
5	Next steps
<b>6</b>	<b>Appendix</b>

ASAP	Accelerated SAP	HRIS	Human resource information system
BI	Business intelligence	H-A	High-Availability
C2M2	Cybersecurity capability maturity model	HIPAA	Health information portability and accountability act
CAO	Chief administrative Officer	IVR	Interactive voice response
CIC	Capital investment committee	IT	Information technology
CIO	Chief information officer	JSSO	Job site safety observation
CIS	Customer information system	LTIIP	Long-term infrastructure improvement plan
COTS	Commercial off-the-shelf	MAS	Multiple Address Systems
CRM	Customer relationship management	MS	Microsoft corporation
DB	Database	O&M	Operations and maintenance
DBCC	Database consistency checker	OS	Operating system
DC	Data center	OT	Operational technology
DVM	Data volume management	PBX	Private branch exchange
DKIM	Domain keys identified mail	PHI	Protected health Information
DR	Disaster recovery	PIA	Privacy impact assessment
EAM	Enterprise asset management	PI	Process integration
ECC	ERP central component	PII	Personally identifiable Information
ECP	Enterprise cache protocol	PM	Project manager
EHS	Environment, health and safety	PMO	Program management office
ERP	Enterprise resource planning system	PNG	Peoples Natural Gas
EY, US	Ernst & Young, LLP	PUC	Public utility certification
FIS	Financial information system	RPO	Recovery point objectives
FTC	Federal trade commission	RTO	Recovery time objectives
GE	General electric	SEW	Smart Energy Water
GRC	Governance, risk, and compliance control	SCADA	Supervisory control and data acquisition
GIS	Geospatial information system	SLA	Service level agreement
GL	General ledger	SOX	Sarbanes-Oxley act
GRC	Governance, risk and compliance	SPF	Sender policy framework



## 6 Appendix

### Appendix B: Description of key systems

- 1 Executive summary
- 2 Scope
- 3 IT observations
- 4 Cybersecurity observations
- 5 Next steps
- 6 Appendix**

System	Description
SAP ECC	Enterprise resource planning software (ERP) which consists in several modules – General Accounting, Financial Reporting, Fixed Assets, A/P, Billing, A/R, Human Resources, Supply Chain Management and Enterprise Asset Management that provide the organizations with great control over their key business processes.
SAP CRM	Integrated customer relationship management (CRM) software that manages customer accounts.
SAP BW	Data warehousing and reporting tool used company-wide for reporting on SAP and non-SAP data sources.
MiCustomer	Customer self-service portal and mobile app.
WorkForce Time & Attendance	Third-party system that enables the organization to collect, track, and manage employee Time and Attendance.
ClockView	Acumen's ClockView mobile APP allows employees to use phones, tablets and any smart device to manage Time and Attendance.
Service Suite	Mobile Workforce Management system which is used by field personnel to receive their assigned orders and enter relevant information as they complete each order.
Essentials	Scheduling system that does tracking of Operations compliance inspections, repairs, leak management, etc.
GasStar	Tracking software that tracks gas supplier delivery and consumption and calculates supplier charges and payments.
Primevera P6	Project management application that helps inside planning, managing and controlling project charges, activities & resources.
CorrMD	Manages corrosion management inspection and testing activities.
Epoch	System which tracks hazardous waste disposal.
ARCOS	Automated system for executing and tracking off-hours callouts for field personnel.
DigTrack	Ticket management software that manages PA One Call tickets and pipeline damage incidents.
ICAM	Governance control system.
Uptime	Suite of analytical tools for pipeline hydraulic modelling, risk ranking, etc.
ArcGIS	Tracking software that provides contextual tools for mapping and spatial reasoning so the firm can explore data and share location-based insights.
SmarCal	Calibration software that helps in gas detection device calibration tracking and compliance reporting.



## 6 Appendix

### Appendix B: Description of key systems

- 1 Executive summary
- 2 Scope
- 3 IT observations
- 4 Cybersecurity observations
- 5 Next steps
- 6 Appendix**

System	Description
iFix	GE Intelligent Platform's software used for machine control at 3 of the larger compressor stations.
Historian	GE Intelligent Platform's software used for data repository for plant/machine data.
Perceptive Content	Image and document management system used company-wide.
UCIS	Custom developed system that processes and tracks PUC complaints.
ODITIN	Workflow-based application for review and approval of engineering documents.
Protection Program Tracker	Tacking software that tracks and reports customer enrolments in Peoples Protection Programs and claims made under those programs.
Gas Forecasting/Reconciliation	In-house system that helps in forecasting of gas supply requirements and reconciliation of actual vs planned purchases.
SCADA	AVEVA's supervisory control and data acquisition (SCADA) system that helps in monitoring, management and control of gas flow through their pipelines
Gas Measurement and Analysis	AVEVA's system that helps in measurement of gas flow for large commercial and industrial customers, and at pipeline interconnects.
Step7	Siemen's system that is used to operate 3 compressor stations.



## 6 Appendix

### Appendix C: Procedures performed – IT

1	Executive summary
2	Scope
3	IT observations
4	Cybersecurity observations
5	Next steps
<b>6</b>	<b>Appendix</b>

#### IT strategy and governance

- ▶ Understood the Company's IT strategy and how it aligns with business goals for both regulated and non-regulated business segments.
- ▶ Understood the effectiveness of the Company's IT strategy to support gas distribution, storage and asset management operations.
- ▶ Understood technology oversight and strategic decision making processes.

#### IT systems and platforms

- ▶ Assessed the adequacy of IT systems, the level of investment that has been made, as well as the projected investment needed to scale for growth.
- ▶ Understood the performance, reliability, and scalability of the key software applications (e.g., SAP ERP) supporting gas distribution, and back-office functions including:
  - ▶ Field operations management: Scheduling, inventory, procurement, maintenance, repairs, safety and environmental compliance
  - ▶ Meter equipment and data management systems
  - ▶ Network operations: Monitoring, performance management, maintenance and incident response
  - ▶ Revenue management: Contracts management, billing and collection
  - ▶ Websites: External and internal websites (web layer, CMS, back-end integration)
  - ▶ Customer operations: Customer information system, billing systems and cash processing/collections systems
  - ▶ Finance and accounting: General ledger, accounts receivable, accounts payable, billing, procurement and tax management
  - ▶ Human Resources, Payroll, and Time and Attendance
- ▶ Understood business processes and associated systems to determine:
  - ▶ How effectively existing technology supports Target's business operations
  - ▶ The ability of Target's IT systems to adequately support business needs

- ▶ The scalability of Target's IT systems to accommodate future business requirements
- ▶ The degree to which Target's IT systems have been customized
- ▶ Opportunities for IT systems rationalization, especially in the case of the SAP ERP system
- ▶ Appropriateness of Internet presence including web sites and mobile applications

#### Data analytics and reporting

- ▶ Determined if the IT environment has the capability to provide the information needed to effectively manage the business, and if it is provided to the Target's leadership and to employees on a timely basis.
- ▶ Understood the financial and operational reporting platform capabilities.

#### IT Organization

- ▶ Understood the IT organization's ability to:
  - ▶ Accommodate current business needs
  - ▶ Support the Target through the next growth cycle
- ▶ Assessed the IT organization for size and structure appropriateness including:
  - ▶ Employee skills and experience profiles
  - ▶ Staffing by functional area
  - ▶ Extent of reliance on key staff
  - ▶ Details of any current contracting agreements to provide technical, operational or applications staff.
- ▶ Obtained an understanding of third-party IT providers' relationships and commitments (e.g., outsourcing, offshoring), including:
  - ▶ Technology services provided by any third-parties
  - ▶ Estimated ongoing costs of technology contract commitments



## 6 Appendix

### Appendix C: Procedures performed – IT

1	Executive summary
2	Scope
3	IT observations
4	Cybersecurity observations
5	Next steps
<b>6</b>	<b>Appendix</b>

#### IT projects

- ▶ Assessed the Target's IT projects portfolio, including current and future IT initiatives **[OPEN – Detailed project plans and status reports not provided]**
- ▶ For current and future IT projects, understood the one-time and recurring expenses, purpose, priority, timeline and resources required for execution.

#### IT spending

- ▶ Understood IT budgets including recurring IT spending, one-time IT spending and IT capital expenditures for:
  - ▶ The two previous fiscal year periods, including budgeted and actual spend
  - ▶ The current fiscal year period, including budgeted and actual spend
  - ▶ The next fiscal year
- ▶ Identified potential IT spend optimization opportunities, as well as areas of under or over investment.
- ▶ Compared IT spending levels to the industry benchmarks, if available.

#### IT processes and operations

- ▶ Understood software development processes and methodologies (e.g., Waterfall, Agile) used to develop proprietary software applications including:
  - ▶ Adequacy of tools and utilities available
  - ▶ Technology change management processes, documentation and tools
  - ▶ Program and project management methodology
  - ▶ Methods used for version control, code documentation and defect tracking
  - ▶ Testing and quality assurance approaches
- ▶ Understood the ability to manage the delivery of IT services to end-users (e.g., IT service desk).
- ▶ Understood software licenses management and tracking to ensure compliance with software licensing requirements.

- ▶ Understood the maturity of IT services management processes such as incident management, problem management, change management, configuration management, and release management.

#### Infrastructure and disaster recovery

- ▶ Understood the reliability of the Company's data centers and IT networks to support short and long term goals.
- ▶ **[OPEN – Detailed inventory not provided]** - Obtain and analyze the technology inventory, including:
  - ▶ Hardware (e.g. PCs, business systems platforms)
  - ▶ Desktop software applications
  - ▶ Network (LAN, WAN, Internet, Intranet) infrastructure
  - ▶ Back office software
  - ▶ Telephony infrastructure
- ▶ Understood the Company's disaster recovery capabilities including:
  - ▶ Plans for restoring IT systems, personal computers, and voice and data communications
  - ▶ Data center location strategy for the Company
- ▶ Understood the Company's data backup, rotation and offsite storage provisions.
- ▶ Understand results of the Company's disaster recovery testing procedures.**[OPEN]**

#### OT (Operational Technology) systems and support

- ▶ Inquired about the organizational structure supporting the OT assets -- who manages the assets at the Target, how are they supported (e.g. employees, third party integrators).
- ▶ Inquired and understood the reliability of the Target's operational technology systems including communications (modems, wireless, etc.), automation (SCADA, other platforms), cybersecurity governance, controls and monitoring, and data collection and analysis.





## 6 Appendix

### Appendix C: Procedures performed – IT

- 1 Executive summary
- 2 Scope
- 3 IT observations
- 4 Cybersecurity observations
- 5 Next steps
- 6 Appendix**

- ▶ Inquired about the obsolescence and appropriateness of OT assets, including:
  - ▶ Hardware
  - ▶ Software
  - ▶ Network infrastructure
- ▶ Understood the Target's disaster recovery capabilities including:
  - ▶ Data backup schemes (e.g., backup media rotation and retention, offsite storage provisions)
  - ▶ Plans for restoring OT systems, personal computers, and voice and data communications



## 6 Appendix

### Appendix D: Procedures performed – Cyber

1	Executive summary
2	Scope
3	IT observations
4	Cybersecurity observations
5	Next steps
<b>6</b>	<b>Appendix</b>

- ▶ Conducted a two hour risk assessment interviews of key personnel to understand:
  - ▶ Volume and sensitivity of, and Company protection of, personally identifiable information, and risk of compromise of such information
  - ▶ Company preparedness for cyber-attacks which disrupt its operations (e.g. denial of service, ransomware)
  - ▶ Approach to compliance with applicable cybersecurity and data privacy laws
  - ▶ Company protections of confidential Intellectual Property (IP)
  - ▶ Compliance with Payment Card Industry (PCI) standards
  - ▶ Whether the Company has been the recent victim of a data breach or has any pending or contemplated litigation or regulatory action related to information security
- ▶ Analyzed written representations made by the Company about its information security to customers, employees and other third parties.
- ▶ Assessed scope and depth of the Company cybersecurity liability insurance.
- ▶ Analyzed available information about vulnerabilities and indicators of compromise in the Company (e.g. Company computers that are infected with malware or weak encryption that could be exploited by hackers).
- ▶ Conducted dark web research into compromised employee credentials, stolen Company or customer property being sold in criminal forums, such as source code, customer credit card data and hacker conversations about the Company and its products.
- ▶ Provided observations including:
  - ▶ Observations on cybersecurity risks to the business based on the diligence procedures performed
  - ▶ Assess historical, current and planned levels of information security capital expenditures and operating expenses to identify potential deferred investments
  - ▶ Examples of leading practices in addressing security gaps similar to those identified during diligence



## 6 Appendix

### Appendix E: SAP licensing details

- 1 Executive summary
- 2 Scope
- 3 IT observations
- 4 Cybersecurity observations
- 5 Next steps
- 6 Appendix**

Product / License type	Metric	Blocks of units	Original # of units	Change	Current # of units	Maintenance base	Annual support costs	Document Reference
SAP Application Professional	Named User		430	170	600			Net changes as per form #7
SAP Application Limited Professional	Named User		75	-65	10			
SAP Application Business Expert	Named User		75	-70	5			
SAP Application employee self-service (ESS)	Named User		300					
SAP application developer	Named User		20	4				
<b>Subtotal: All named user licenses Appendix 1</b>						<b>\$ 162,494.00</b>	<b>\$ 35,748.68</b>	1. SAP invoice as of 12/2/2017 2. Initial contract from 2/5/2010 3. SAP form #7
<b>SAP ERP</b>								
SAP Financial supply chain management	Number of active customers	1000	400	-112	288			
SAP treasury and risk management	Annual revenue	100 M	10					
SAP real estate management - Land management	Number of parcels of land	1000	10					
SAP environment health and safety (EH&S) management	Number of employees	100	6					
SAP work clearance management (WCM)	Number of WCM plants	1	5					
<b>SAP Utilities</b>								
SAP customer relationship & billing for utilities	Number of active contracts	1000	400					
SAP customer financial management for utilities	Number of contract accounts	1000	400					
SAP collaborative services management for utilities	Number of points of deliveries (PODs)	1000	100					
SAP resources and supplier management for utilities	Spend volume	\$1M	400					
SAP energy data management for utilities	Number of points of deliveries (PODs)	1000	425					
<b>SAP for Oil and GAS</b>								
SAP supply chain management for Oil and GAS	Number of barrels of oil equivalent per day scheduled/planed	25,000	2					
<b>Supplementary software licensed</b>								
SAP contract lifecycle management (SAP CLM)	Number of contracts	500	8					
SAP test data migration (TDSM)	Database size of the productive system	1GB	800					
SAP Netweaver process integration	Number of OPUs	1	4					
<b>Support related software</b>								
SAP solution manager extended service desk	Number of service requests	1	1000					
<b>Subtotal: Appendix 2</b>						<b>\$ 1,354,061.36</b>	<b>\$ 297,893.50</b>	1. SAP invoice as of 12/2/2017 2. Termination amendment effective 6/30/2016
<b>Appendix 3: SAP Business Objects BI Package</b>								
	CPUs	1	2			<b>\$ 43,254.00</b>	<b>\$ 9,515.88</b>	1. SAP invoice as of 12/2/2017 2. Initial contract from 2/5/2010



## 6 Appendix

### Appendix E: SAP licensing details

- 1 Executive summary
- 2 Scope
- 3 IT observations
- 4 Cybersecurity observations
- 5 Next steps
- 6 Appendix**

Product / License type	Metric	Blocks of units	Original # of units	Change	Current # of units	Maintenance base	Annual support costs	Document Reference
SAP interactive forms by Adobe, Enable the enterprise (includes 40 interactive forms)	# of SAP Named Users	1	575		575			
SAP central process scheduling by Redwood	# of Process Servers	1	2		2			
SAP productivity park by RWD	# of Users	1	575		575			
SAP Productivity pak help launchpad by RWD	# of Users	1	575		575			
SAP productivity composer by RWD	# of Users	1	575		575			
SAP productivity composer help launchpad by RWD	# of Users	1	575		575			
<b>Appendix 4: Subtotal: Redwood and Adobe</b>						<b>\$ 78,556.00</b>	<b>\$ 17,282.32</b>	1. SAP invoice as of 12/2/2017. 2. Initial contract from 2/5/2010, appendix 4
SAP application employee self-service user	SAP application employee self-service user		450		450	\$ 84,600.00	\$ 18,612.00	1. SAP order form 5
Database	MS SQL server enterprise edition		1		1	\$ 6,768.00	\$ 1,488.96	
<b>Subtotal: Software order form #5</b>						<b>\$ 91,368.00</b>	<b>\$ 20,100.96</b>	
SAP linear asset management	Users	1	150		150	\$ 26,478.00	\$ 5,825.16	1. SAP order form 6 2. Termination amendment from Jun 2016
BA&T SAP access control	Users, monitored for SAP access control	1000	2		2	\$ 20,388.06	\$ 4,485.37	
SAP enterprise integration for work manager mobile app	Users	1	20		20	\$ 29,125.00	\$ 6,407.50	
BA&T SAP data services	Cores	1	13		13	\$ 478,075.00	\$ 105,176.50	
SAP HANA runtime edition for SAP BW	SMBV	1	1		1	\$ 177,343.00	\$ 39,015.46	
SAP mobile platform developer	Users	1	1		1	\$ 441.30	\$ 97.09	
Database	MS SQL server enterprise edition	1	1		1	\$ 58,548.09	\$ 12,880.58	
Reduction as per Termination amendment as of Jun 30, 2016						\$ (79,667.79)	\$ (17,526.91)	
<b>Subtotal: Software order form #6</b>						<b>\$ 710,730.66</b>	<b>\$ 156,360.75</b>	
SAP developer user	SAP developer user	1	6		6	\$ 9,995.40	\$ 2,198.99	1. Order form 7 2. Termination amendment from Jun 2016
SAP financial supply chain management	Active customers / Vendors	1000	228	-228	0	\$ -	\$ -	
SAP customer relationship management for utilities	Active contractors	1000	228		228	\$ 126,608.40	\$ 27,853.85	
SAP customer financial management for utilities	Contractor accounts	1000	228		228	\$ 158,260.50	\$ 34,817.31	
SAP HANA, enterprise edition, up to 10 units	GB of memory	64	2		2	\$ 320,000.00	\$ 70,400.00	
SAP HANA, runtime edition for SAP BW – New/subsequent	HSAV	1	1		1	\$ 57,229.22	\$ 12,590.43	
SAP infinite insight modeler	Users	1	5		5	\$ 55,530.00	\$ 12,216.60	
SAP HANA predictive option, up to 10 units	GB of memory	64	2		2	\$ 50,000.00	\$ 11,000.00	
SAP business objects BI suite (user)	Users	1	50		50	\$ 26,608.00	\$ 5,853.76	
SAP business objects BI suite (CS)	Concurrent sessions	25	2		2	\$ 85,146.00	\$ 18,732.12	
Database	MS SQL server enterprise edition	1	1		1	\$ 91,407.56	\$ 20,109.66	
<b>Subtotal: Software order form #7</b>						<b>\$ 980,785.08</b>	<b>\$ 215,772.72</b>	



## 6 Appendix

### Appendix E: SAP licensing details

- 1 Executive summary
- 2 Scope
- 3 IT observations
- 4 Cybersecurity observations
- 5 Next steps
- 6 Appendix**

Product / License type	Metric	Blocks of units	Original # of units	Change	Current # of units	Maintenance base	Annual support costs	Document Reference
SAP professional user	SAP professional user	1	100		100	\$ 232,944.00	\$ 51,247.68	1. SAP order form 8 2. SAP invoice as of 12/2/2017, Supersedes invoice #6008427566
SAP HANA, runtime edition for SAP BW – New / Subsequent	HSAV	1	1		1	\$ 30,236.13	\$ 6,651.95	
SAP access control	Users, monitored for SAP access control	100	8		8	\$ 145,007.64	\$ 31,901.68	
SAP HANA enterprise information management option, up to 10 units	GB of memory	64	2		2	\$ 60,000.00	\$ 13,200.00	
SAP HANA smart data tiering option, up to 40 units	Gigabyte	256	1		1	\$ 5,000.00	\$ 1,100.00	
Database	MS SQL server enterprise edition	1	1		1	\$ 37,855.02	\$ 8,328.10	
<b>Subtotal: SAP Order form 8</b>						<b>\$ 511,042.79</b>	<b>\$ 112,429.41</b>	
SAP HANA, runtime edition for SAP BW – New/subsequent	HSAV	1	1		1	\$ 12,960.00	\$ 2,851.20	1. SAP order form 9 2. SAP invoice as of 12/2/2017, Supersedes invoice #6008427567
Database	MS SQL Server enterprise edition	1	1		1	\$ 13,996.80	\$ 3,079.30	
<b>Subtotal: SAP Order form 9</b>						<b>\$ 26,956.80</b>	<b>\$ 5,930.50</b>	
SAP Customer relationship management and billing for utilities		1000	72	113	185	\$ 169,500.00	\$ 37,290.00	1. SAP order form 7 and 10 2. SAP invoice as of 12/2/2017, Supersedes invoice #6008427568
SAP customer financial management for utilities		1000	72	10	82	\$ 18,750.00	\$ 4,125.00	
SAP HANA, Runtime edition for SAP BW – New/subsequent		1	1		1	\$ 36,835.00	\$ 8,103.70	
SAP Netweaver application server, add-on for code vulnerability analysis		500	3		3	\$ 56,250.00	\$ 12,375.00	
SAP worker user		1	400		400	\$ 180,000.00	\$ 39,600.00	
SAP business Objects BI Suite (user)		1	25		25	\$ 35,937.00	\$ 7,906.14	
Database		1	1		1	\$ 39,781.00	\$ 8,751.82	
<b>Subtotal: SAP Order form 10</b>						<b>\$ 537,053.00</b>	<b>\$ 118,151.66</b>	
SAP meter administration and operations for energy utilities	Points of delivery	1000	730		730	\$ 284,371.50	\$ 62,561.73	1. SAP order form 11.
SAP HANA, runtime edition for applications & SAP BW – install base	HSAV	1	1		1	\$ 520,213.62	\$ 114,447.00	
SAP HANA, runtime edition for Applications & SAP BW – New/subsequent	HSAV	1	1		1	\$ 43,407.00	\$ 9,549.54	
SAP S/4 HANA enterprise management for ERP customers	Flat fee	1	1		1	\$ 5,008.50	\$ 1,101.87	
Database	MS SQL Server Enterprise Edition	1	1		1	\$ 67,839.37	\$ 14,924.66	
<b>Subtotal: SAP Order form 11</b>						<b>\$ 920,839.99</b>	<b>\$ 202,584.80</b>	



## 6 Appendix

### Appendix E: SAP licensing details

- 1 Executive summary
- 2 Scope
- 3 IT observations
- 4 Cybersecurity observations
- 5 Next steps
- 6 Appendix**

Product / License type	Metric	Blocks of units	Original # of units	Change	Current # of units	Maintenance base	Annual support costs	Document Reference
SAP Multichannel foundation for utilities	Active user	1000	750		750	\$ 292,500.00	\$ 64,350.00	1. SAP order form # 12 from May 31, 2018
SAP HANA, Runtime edition for applications and SAP BW – New/Subsequent Database	HSAV	1	1		1	\$ 43,875.00	\$ 9,652.50	
	MS SQL server enterprise edition	1	1		1	\$ 26,910.00	\$ 5,920.20	
<b>Subtotal: SAP Order form 12</b>						<b>\$ 363,285.00</b>	<b>\$ 79,922.70</b>	
<b>Total</b>						<b>\$ 5,780,426.68</b>	<b>\$ 1,271,693.87</b>	



## 6 Appendix

### Appendix F: Cybersecurity open source findings (Peoples-gas.com)

- 1 Executive summary
- 2 Scope
- 3 IT observations
- 4 Cybersecurity observations
- 5 Next steps
- 6 Appendix**



#### Mail Services

No DKIM record found but SPF domain is properly configured



#### Message transfer security

3 records where the SSL certificate had expired or was using an algorithm that is no longer supported



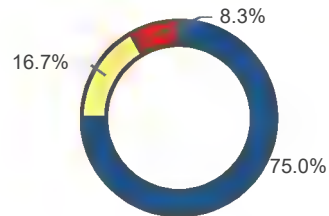
#### Web Application headers

No security headers are set

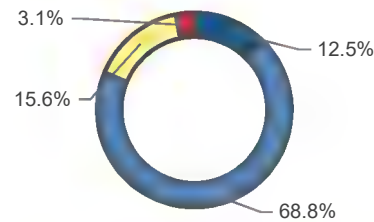
#### DKIM

No Records

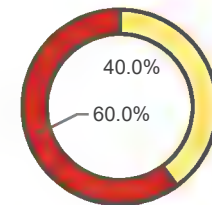
#### TLS/SSL Certificates



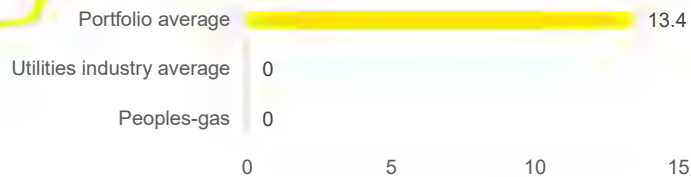
#### TLS/SSL Configuration



#### Web Headers



#### Compromised system

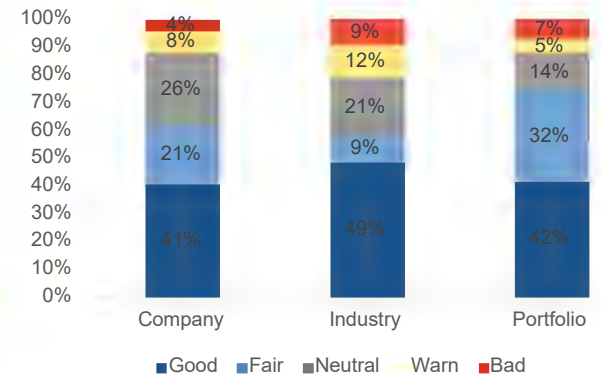


Average amount of time between first time an event was observed and the last time it was seen. For peoples it is 0.

■ Good ■ Fair ■ Neutral ■ Warn ■ Bad

#### Diligence Summary

Only 12% of the company's items are in Warn/bad stage compared to Industry average of 21%



Note: Source taken from Bitsight report as of 21<sup>st</sup> September 2018



## 6 Appendix

### Appendix F: Cybersecurity open source findings (Peopleseaccount.com)

- 1 Executive summary
- 2 Scope
- 3 IT observations
- 4 Cybersecurity observations
- 5 Next steps
- 6 Appendix



#### Mail Services

No DKIM record and SPF domain found



#### Message transfer security

No SSL certificates found and all the 3 instances appear to have been configured as bad for security protocol libraries (TLS/SSL).



#### Open Ports

There was 1 instance found that had potentially insecure ports open (remote access)

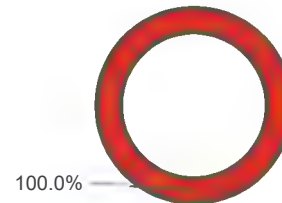
#### No DKIM and SPF

No Records

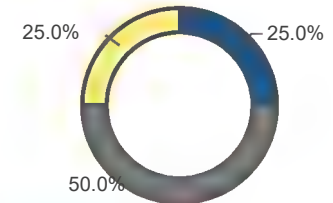
#### TLS/SSL Certificates

No Records

#### TLS/SSL Configuration



#### Open Ports



#### Compromised system

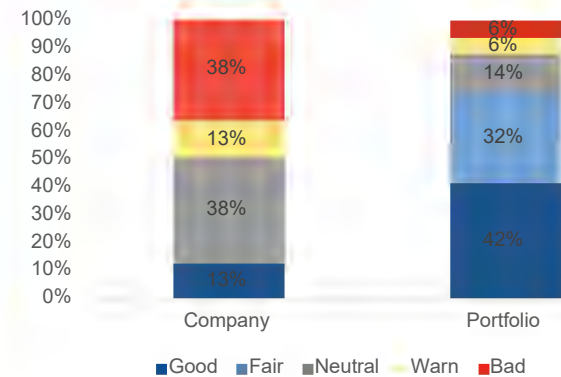


Average amount of time between first time an event was observed and the last time it was seen. For peoples it is 0



#### Diligence Summary

More than 40% of the company's diligence items were found to be in Warn/bad stage compared to 12% of industry's average



Note: Source taken from Bitsight report as of 21<sup>st</sup> September 2018



## EY | Assurance | Tax | Transactions | Advisory

### **About EY**

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit [ey.com](http://ey.com).

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2018 Ernst & Young LLP.  
All Rights Reserved.

1810-2904761