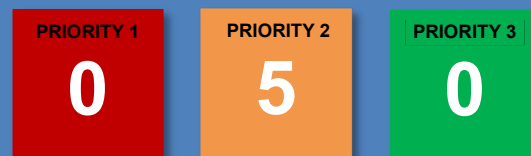


Report #2023-09

INSIGHT PUBLIC SECTOR INC CONTRACT AUDIT

NUMBER OF RECOMMENDATIONS



*City of Glendale
Internal Audit*

06.28.2023



Contents:

A. Overview..... 3

B. Action Plan and Target Completion Dates..... 4

C. Background 4

D. Objective, Scope and Methodology 6

E. Observations, Recommendations, & Management Responses Matrix..... 7

Appendix 1: Definitions of Priority Rankings and Value-Added Categories..... 12

Distribution List:

For action: Michelle Nall, Utility Business System Support Administrator

For information: Jason Bradford, Director of Finance/Information Technology
 Roubik Golanian, City Manager
 Scott Mellon, Assistant General Manager/Power Management
 Jason Miller, Assistant Chief Information Officer - Infrastructure
 John Takhtalian, Assistant City Manager
 Mark Young, General Manager of Glendale Water & Power
 Audit Committee
 City Council

Acknowledgment

We would like to thank staff from Insight Public Sector Inc, Glendale Water & Power, and Information Technology for the assistance provided to us throughout this project.

For questions regarding the contents of this report, please contact the lead auditor, Ani Antanesyan, Sr. Internal Auditor, or Jessie Zhang, Internal Audit Manager at InternalAudit@glendaleca.gov

This report is also available online at <https://www.glendaleca.gov>

A. Overview

Key Outcomes

The City is contracted with the Insight Public Sector Inc (Vendor) to provide infrastructure and security monitoring and Information Technology support for the Glendale Water & Power (GWP). The agreement is under the administration of GWP, which oversees the Vendor’s daily activities and performance. Although Vendor invoices are reviewed and approved by GWP, they are processed for payment by the Information Technology Department (ITD). Internal Audit reviewed the agreement’s statement of work and the current contract administration controls and noted that monitoring controls over Vendor deliverables and performance can be strengthened. Internal Audit identified five improvement opportunities related to establishing and monitoring a detailed list of deliverables by Vendor, clarifying areas of responsibilities between ITD/GWP and Vendor related to deliverables, clarifying and documenting response targets and deliverable task tracking methods, improving invoicing review, and ensuring that Vendor is compliant with all contractual data security requirements.

Impact Dashboard

This table summarizes the applicable value-added categories (total 15) for the five recommendations based on their priority rankings.¹

	Value Added Categories			
	Compliance	Cost Saving	Efficiency	Risk Reduction
Priority 1 0	0	0	0	0
Priority 2 5	5	1	4	5
Priority 3 0	0	0	0	0

¹ Each audit recommendation may have more than one value-added category. The Definitions of Priority Rankings and Value-Added Categories are located at Appendix 1.

B. Action Plan and Target Completion Dates

The action plan and target completion dates are summarized in the table below. Internal Audit will perform quarterly status follow-up to provide assurance that management is taking appropriate and timely corrective action to address audit recommendations.

Ref.	Management Action Plan	Completion Date
Priority 2		
1.	Establish and monitor a list of deliverables that reference the PSA statement of work and assign performance frequency for each deliverable. <i>Value added:</i> Compliance , Efficiency , Risk Reduction	12/31/2023
2.	Clarify, document, and communicate PSA deliverable areas that may require collaboration with ITD/GWP. <i>Value added:</i> Compliance , Efficiency , Risk Reduction	12/31/2023
3.	Clarify and document response time targets and task tracking methods for PSA deliverables including ticketing system usage. <i>Value added:</i> Compliance , Efficiency , Risk Reduction	12/31/2023
4.	Ensure that invoices have adequate support for all charges and ad-hoc hour invoices do not have in-scope charges. <i>Value added:</i> Compliance , Cost Saving , Risk Reduction	12/31/2023
5.	Obtain and review Vendor PSA required service organization control reports and ensure that any subcontractors employed by Vendor are approved by City prior to executing any PSA obligated activity. <i>Value added:</i> Compliance , Efficiency , Risk Reduction	12/31/2023

C. Background

Internal Audit has completed a compliance audit of an agreement with Insight Public Sector, Inc. The agreement is under the administration of GWP, which oversees the Vendor's daily activities and performance. The invoices are reviewed and approved by GWP, but they are processed by the ITD. This audit focused on determining whether the City has established controls to ensure that the contract provisions are being appropriately followed by the Vendor and the contract is appropriately administered by City staff.

Contract Overview

A professional services agreement (PSA) between the City and Insight Public Sector, Inc. was executed on July 1, 2022 to provide the City with remote infrastructure and security monitoring, managed and professional services and additional direct IT support in the amount of \$1,495,300, plus an additional \$40,000 for 200 hours of direct

information technology support and advanced specialized service for GWP per year.²
The key provisions from the PSA related to this audit include the following:

- **Scope of Work:** the contract details over 100 deliverables that are broadly categorized into the five areas below:
 - Monitoring and Notification
 - Network and Server Monitoring
 - Network and Server Problem Management and Maintenance
 - Security Management
 - Database Administration

Only the Security Management area has a specified monitoring method in the PSA, which uses Vendor's Security Incident Event Management (SIEM) ticketing software to create Security Incidents, Support Tickets and Change Requests. The table below provides response time targets for these tickets. The priority levels are determined based on a combination of predefined impact and severity.

Priority	Incident Response	Incident Update	Incident Resolution Target
Priority 1	15 minutes	1 hour	4 hours
Priority 2	1 hour	4 hours	8 hours
Priority 3	4 hours	24 hours	72 hours
Priority 4	24 hours	72 hours	120 hours

- **Invoicing:** deliverables are invoiced as follows:
 - **Monthly Fixed Price Managed Services Invoice** – payments are made for services such as VMware environment, backup and restore, network environment, windows/server environment, SQL DBA services and monitoring tools and ticket response.
 - **Monthly Per Unit Managed Security Invoice** – security monitoring and management of network devices, servers, and firewalls.
 - **Out of Scope Engineering Hours Invoice** – out of scope engineering hours are capped at 200 per fiscal year and are subject to a not-to-exceed amount.
- **Data Security Requirements:** the PSA also requires several data security elements to be presented by Vendor, such as limiting access of City information to authorized persons, implementing network, application, database and platform security, provide oversight of security compliance by periodically having third parties perform network-level vulnerability assessments over information technology and information security controls for all facilities used in complying with its obligations under the agreement.

² Cost to be reviewed every 12 months to determine if a decrease can be recognized due to service efficiencies resulting in a reduction of service hours utilized or removal of certain components of the infrastructure that no longer require Vendor support.

D. Objective, Scope and Methodology

The objective of this audit is to determine whether the City has established adequate controls to ensure that the contract provisions are being appropriately followed by the Vendor and the contract is appropriately administered by City staff.

The scope of the audit covers July 1, 2022 to April 11, 2023.

To accomplish the audit objective, Internal Audit performed the following:

- Interviewed City and Vendor personnel regarding the PSA and corresponding processes;
- Reviewed the contract terms and deliverables;
- Conducted detailed review of contract deliverables by obtaining samples of completed tasks and supporting documents;
- Conducted detailed testing of closed tickets from July 1, 2022 to April 11, 2023 based on a Vendor's ticketing system report;
- Conducted detailed review of Vendor invoices from July 31, 2022 to February 18, 2023;
- Reviewed the data security requirements in detail and obtained supporting documentation.

As a result of these audit procedures performed, five observations were identified and are detailed in the Observations, Recommendations, and Management Responses Matrix beginning on the following page.

E. Observations, Recommendations, & Management Responses Matrix

Ref	Observation	Recommendation	Management Response
1.	Service Delivery		
Priority 2	<p>Internal Audit reviewed the PSA statement of work and noted the following:</p> <ul style="list-style-type: none"> a. GWP has not established specific and measurable deliverables based on the broad PSA statement of work. For instance, services to be provided such as proactive detection or prediction of failure or threats, problem isolation and diagnosis, compliance requirements monitoring, or change management do not have specific measurable tasks. b. The frequency of performing deliverables is not consistently documented. 	<p>GWP management perform the following:</p> <ul style="list-style-type: none"> a. Establish and periodically monitor a list of deliverables that reference the PSA obligated statement of work. Clarify any tasks to be performed by Vendor that may be too broad to enable clear tracking of deliverables and performance. One method is to utilize and incorporate the recommended changes into the Vendor’s existing tracking tool. b. Review the list of deliverables and attach a frequency for executing deliverable, as applicable. 	<p>Agreed and will implement by December 31, 2023.</p>

Ref	Observation	Recommendation	Management Response
2.	ITD/GWP vs Vendor Responsibilities		
Priority 2	<p>Internal Audit reviewed the PSA statement of work and noted that five areas of the statement of work reviewed had unclear responsibilities between Vendor and ITD/GWP. These areas have been communicated to management.</p>	<p>GWP management review all PSA deliverables and reference tasks where ITD/GWP and Vendor staff may need to collaborate, and ensure that the responsibilities of Vendor and/or ITD/GWP staff are clearly defined and communicated to all parties.</p>	<p>Agreed and will implement by December 31, 2023.</p>

Ref	Observation	Recommendation	Management Response
3.	Service Delivery Tracking Method		
Priority 2	<p>Based upon review of 373 closed SIEM tickets created from July 1, 2022 to April 11, 2023, Internal Audit noted the following:</p> <ul style="list-style-type: none"> a. 281 (or 75%) tickets did not meet response time targets for incident resolution. Per GWP, the reason behind the target not being met is due to the ticket not being closed on time although the work is being performed, and/or the priority level not being assigned appropriately based on impact and severity. b. There is no documented method for tracking all PSA deliverables based on different tasks. Tasks can be tracked via email, Vendor ticketing system, ITD’s Help system, Vendor Excel tracking sheets, the weekly status reports, or a phone call. c. It is unclear whether and when Vendor and/or City’s IT ticketing systems should be used. d. It is unclear whether City staff consistently resolve tickets in “Waiting for Customer” status and whether any response times are applicable. 	<p>GWP management perform the following:</p> <ul style="list-style-type: none"> a. Evaluate and revise as appropriate, the PSA response level targets including priority levels and response times to either enforce or revise them based on different ticket types, and periodically monitor meeting performance targets. b. Clarify and document tracking method(s) for PSA deliverables including a specific method based on task type, for instance, by issuing tickets or by another tracking method. c. Clarify and document in policies and procedures whether Vendor and/or City’s ticketing system can be used and criteria for their usage. d. Establish policies and procedures for ticket status "Waiting for Customer", to clarify staff responsibilities and any response time targets, if applicable. 	<p>Agreed and will implement by December 31, 2023.</p>

Ref	Observation	Recommendation	Management Response
4. Invoicing			
Priority 2	<p>Internal Audit reviewed Vendor invoices from July 1, 2022 to February 18, 2023 and noted the following:</p> <ul style="list-style-type: none"> a. The recurring invoices, both for managed infrastructure and for managed security do not have accompanying task deliverable reports and/or managed device listings to enable verification of the invoiced charges by both GWP and ITD. b. 1 (or 1%) ad-hoc hour out of 140 hours billed, in the amount of \$200 related to a GWP firewall request was an in-scope deliverable per the PSA and should not have been invoiced separately as an ad-hoc hour. 	<p>GWP management perform the following:</p> <ul style="list-style-type: none"> a. Ensure that City staff that review and approve invoices have adequate support for services delivered based on the PSA. One method is to provide a detailed listing of devices and tasks performed and/or performance reports with the invoices. b. Review the ad-hoc hour charged for in-scope work and work with the Vendor to ensure that the City is appropriately credited back. To ensure ad-hoc hours are charged for out-of-scope services only, one method is to reference a PSA designated ad-hoc hour category to the invoice support. 	<p>Agreed and will implement by December 31, 2023.</p>

Ref	Observation	Recommendation	Management Response
5. Data Security Requirements			
Priority 2	<p>Internal Audit reviewed the Data Security Requirements in the PSA and noted the following:</p> <ul style="list-style-type: none"> a. Upon request, the City has not been able to obtain Vendor's SOC 1 or similar report. Additionally, per GWP staff, the existing SOC 2 report User Entity Responsibility controls have not been communicated to GWP by Vendor. b. Per the PSA, Vendor may not subcontract any part of the services without the prior written consent of the City. However, it was noted that the Vendor has not timely notified and has not obtained the written consent of the City prior to subcontracting. 	<p>GWP management perform the following:</p> <ul style="list-style-type: none"> a. Obtain and review a SOC 1 report, or similar report. Ensure that Vendor staff communicate any user entity responsibilities to City staff. b. Review all subcontractors involved with the PSA and document City's consent of the use of subcontractors by Vendor and update the contract. 	<p>Agreed and will implement by December 31, 2023.</p>

Appendix 1: Definitions of Priority Rankings and Value-Added Categories

Definitions of Priority Rankings

The priority rankings are assigned by internal auditors based on their professional judgment. They are also agreed to by management based on their evaluation of the alignment with the strategic goals, priorities and available resources. A timeline has been established based on each priority ranking:

- a. **PRIORITY 1** - Critical control weakness that exposes the City to a high degree of combined risks. Priority 1 recommendations should be implemented within **3 months** from the first day of the month following report issuance or sooner if so directed.
- b. **PRIORITY 2** - Less than critical control weakness that exposes the City to a moderate degree of combined risks. Priority 2 recommendations should be implemented within **6 months** from the first day of the month following the report issuance or sooner if so directed.
- c. **PRIORITY 3** - Opportunity for good or better practice for improved efficiency or reduce exposure to combined risks. Priority 3 recommendations should be implemented within **9 months** from the first day of the month following the report issuance or sooner if so directed.

Definitions of Value-Added Categories

The four value-added impact categories are defined based on their impact from the audit recommendations:

- a. **COMPLIANCE** - adherence to laws, regulations, policies, procedures, contracts, or other requirements.
- b. **COST SAVING** - lower the costs related to conducting City business.
- c. **EFFICIENCY** - ability to avoid wasting resources (money or time) in achieving goals.
- d. **RISK REDUCTION** - lower the risks related to strategic, financial, operations and compliance.