PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

REPORT ON

VENDOR DUE DILIGENCE ASSESSMENT

PRESENTED TO

Waterfront Warehouse Local 1429 Pension Plan

July 10th, 2024

Submitted by:
Thomas J. DeMayo, CISSP, CISA, CRISC, CIPP/US, MCSE, CEH, CCFE, CHFI, CPT
Partner, Cybersecurity and Privacy Advisory
Cyber Risk Management Group
tdemayo@pkfod.com

KNOW GREATER VALUE®

July 10th, 2024

To the Trustees of the Waterfront Warehouse Local 1429 Pension Plan.

Dear Trustees:

PKF O'Connor Davies Advisory, LLC has completed the performance of Vendor Due Diligence on behalf of the Waterfront Warehouse Local 1429 Pension Plan ("Local 1429"). The objective of the study was to review the alignment of the utilized vendors' cybersecurity programs with the cybersecurity guidance issued by the Department of Labor.

Any procedures that were performed by us in connection with this assignment did not constitute an audit and were not designed to provide, and we will not express, any assurance on internal control.

Our findings are summarized within this report.

This report is intended solely for the information and use of Local 1429.

We wish to thank you and your staff for the courtesy and cooperation extended to us.

Very truly yours,

PKF O'Connor Davies Advisory, LLC

PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS
ESTABLISHED IN 1891

Table of Contents

Vendor Due Diligence Assessment

RISK RANKING DEFINITION

Based on the responses provided, the below rating system was applied to the Vendors in relation to their Cybersecurity Maturity level.

1. **No Response or Response Refused** – The Vendor has not provided any information for the assessment, stopped responding for follow-up information, or never responded to the initial requests.

2. **Low Maturity** – The Vendor has not implemented many of the minimum-security controls specified by the Department of Labor.

3. **Moderate-Low Maturity** – The Vendor has implemented basic security controls but are still missing key controls indicated by the Department of Labor.

4. **Moderate Maturity –** The Vendor meets the majority of the security controls specified by the Department of Labor.

5. **Moderate-High Maturity** – The Vendor meets almost all of the security controls specified by the Department of Labor with minor deviations.

6. **High Maturity** – The Vendor meets all the security requirements specified by the Department of Labor.

CYBERSECURITY ASSESSMENT RISK BREAKDOWN

During this assessment, we reviewed specific security controls for each vendor in accordance with the controls specified by the Department of Labor. The individual control areas assessed were:

- **A Well Documented Cybersecurity Program** – The Vendor should have a formalized and well-documented Information Security Program.

- **Annual Risk Assessments** – The Vendor performs an annual risk assessment to assist in determining any security gaps within the multiple areas within their Organization.

- **Reliable Third-Party Audit of Controls** – The Vendor performs Vulnerability scanning, Penetration Testing, or any other type of Security Testing by a reliable Outsourced company.

- **Clearly Defined Information Security Roles and Responsibilities** – The Vendor has specified employees which are placed in charge of handling Cybersecurity for their Organization and those employees understand their job responsibilities.

- **Strong Access Control Procedures**– The Vendor has implemented Two Factor

authentication for any remote access into their environment and has implemented the principle of least privilege.

- **Vendor Due Diligence** – The Vendor is utilizing a third-party cloud service provider and is performing their vendor due diligence by annually reviewing their security controls by asking for an SOC 2 type II report or sending out a questionnaire verifying they are following security best practices.

- **Annual Cybersecurity Awareness Training** – The Vendor is enforcing annual Cybersecurity Awareness training for all employees. The training includes anything new on the annual Risk Assessment report and a periodic Phishing test.

- **A Software Development Lifecycle** – The Vendor has a Software Development Lifecycle for their custom developed Software, or they do not have one because they do not custom develop software. In which case, this requirement cannot be applicable.

- **Disaster Recovery and Business Continuity Plans** – The Vendor has formalized Disaster Recovery and Business Continuity Plans in the event of a disaster event.

- **Encryption of Sensitive Data at Rest and in Transit** – The Vendor is properly encrypting all sensitive data stored on systems and being sent over a network connection**.**

- **Security Best Practices and Technical Controls** – The Vendor is implementing security configuration best practices (Password controls, proper access controls, etc.) and proper security appliances (firewalls with IDS/IPS, web content filter, Antivirus/EDR, etc.).

- **Formal IR Plan for breach events –** The Vendor has a formally documented IR plan specific to breach events and tabletop exercises are performed on a periodic basis.

- **Cybersecurity Insurance –** The Vendor has procured Cybersecurity insurance, and the amounts are reasonable.

- **Cybersecurity Breaches –** Verification that the Vendor has not had a breach within the past 5 years that impacted Plan data.

- **Background Checks –** The Vendor performs different types of background checks on their employees, at least on hire.

METHODOLOGY

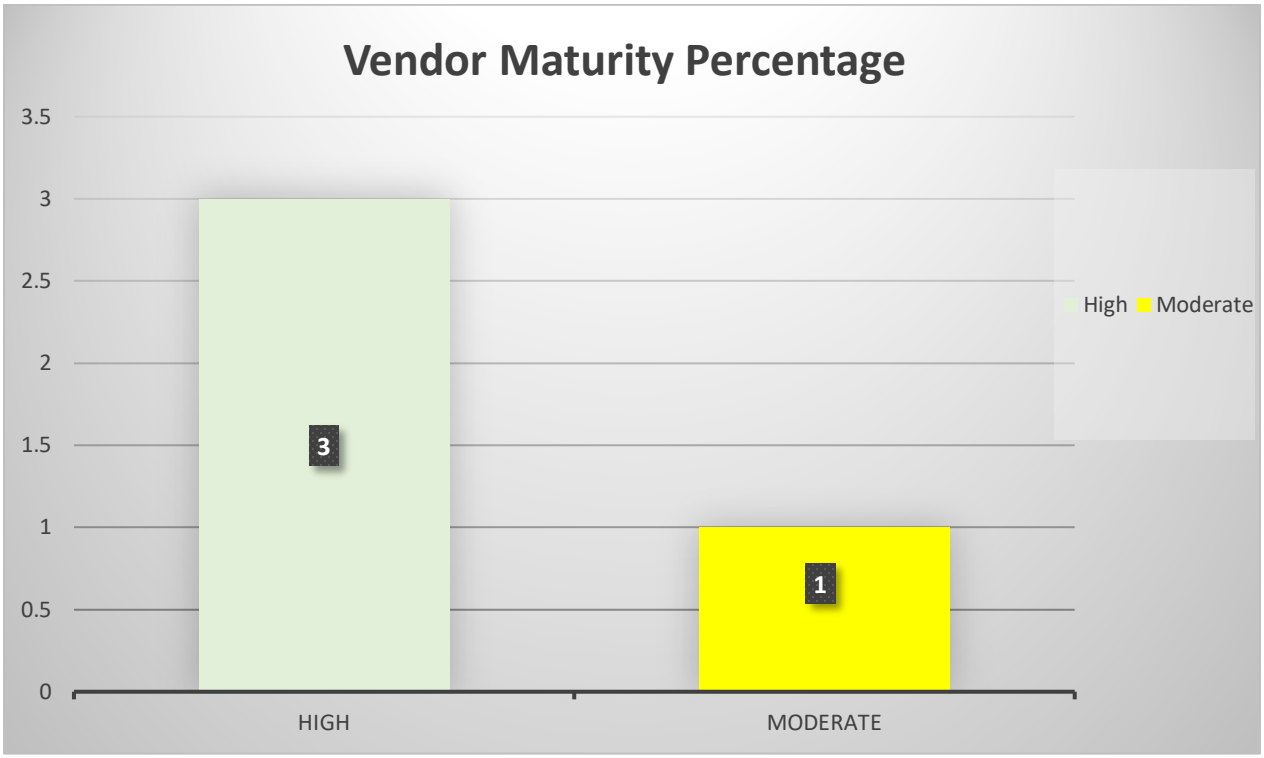
We reviewed the Vendors for Local 1429 by first determining the inherent risk the Vendor presents to Local 1429. The inherent risk is the risk of the Vendor based on the services provided to Local 1429 independent of the controls established by the Vendor to mitigate that risk. For example, the Audit firm has a high inherent risk given the extent of sensitive data they are entrusted with. We then reviewed the security controls implemented by each of the Vendors in relation to the cybersecurity guidance issued by the DOL. Utilizing this combined data, the assessment team was able to provide a qualitative measurement of the maturity level of the Vendor's cybersecurity program and a determination if the program was Satisfactory or Not satisfactory relative to the inherent risk of the Vendor. The maturity level assigned is independent of the inherent risk, as such, any vendor with a maturity level greater than moderate was deemed satisfactory. Should a Vendor receive a maturity ranking moderate or below, we factored in the inherent risk to better inform the Trustees if any remedial actions would need to be taken. For example, a Vendor that has low inherent risk based on the services provided and has an overall lower maturity cybersecurity program, could very well be satisfactory based on the risk and nature of the services.

EXECUTIVE SUMMARY

In total, we reviewed **4** Vendors. Each vendor was given a qualitative maturity risk ranking of High, Moderate-High, Moderate, Moderate-Low, or Low. The number of vendors for each risk ranking is as follows:

Maturity Level	Total
High	**3**
Moderate	**1**

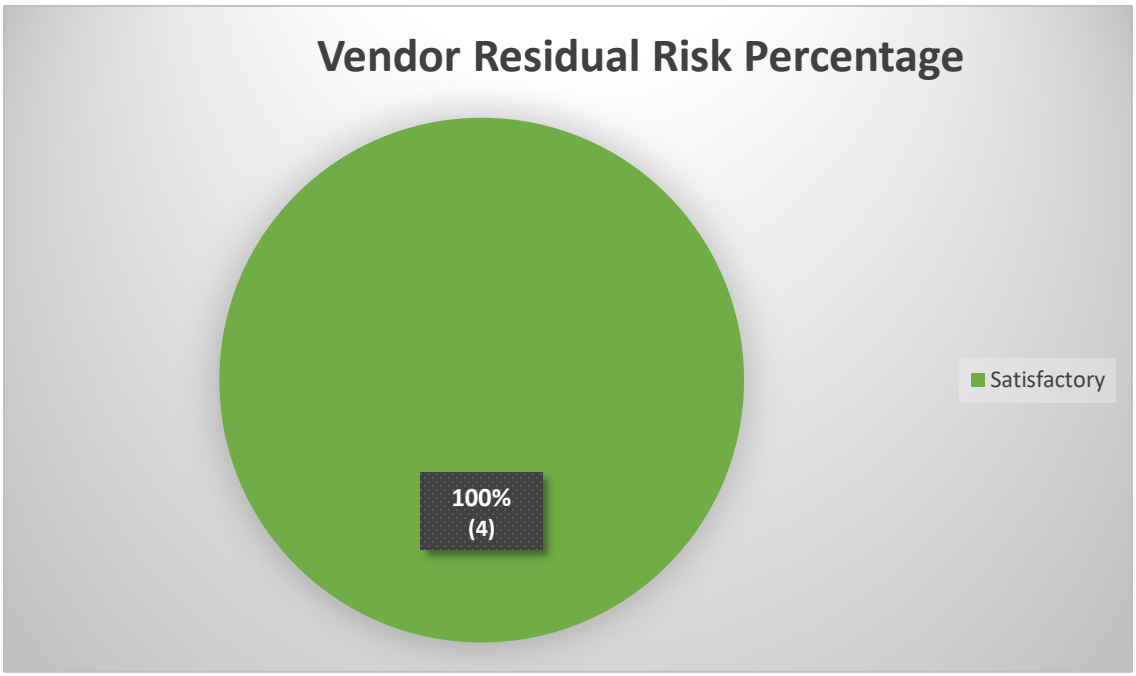
The chart below represents the total maturity percentage of the vendors assessed.



Based on the chart above, the majority of the Organization's vendors are at a High level of Cybersecurity Maturity. Any Vendor ranked Moderate or lower, the Organization should follow up with the Vendor and request the missing information to finalize their review or advise them to enhance their cybersecurity program.

VENDOR RESIDUAL RISK ANALYSIS

The following chart illustrates the overall risk percentages for the assessed vendors categorized based on the risk to Local 1429. The vendors were given a final residual risk of either Satisfactory, Unsatisfactory, and Pending.



Each assessed vendor has achieved the status of a Satisfactory risk to Local 1429.

VENDORS WITH MODERATE TO LOW CYBER MATURITY AND/OR OTHER CONSIDERATIONS

Below is a breakdown to assist Local 1429 in identifying vendors which did not respond, have Moderate to Low Cyber Maturity levels, or could have additional considerations that may pose risks to Local 1429. For the Vendors ranked Satisfactory with a low maturity rating and a low inherent risk, Local 1429 may choose to not take any additional action for those Vendors; however, should Local 1429 want, we have provided a set of considerations that can be conveyed to the Vendors.

Abato Rubenstein and Abato, P.A

Inherent Risk: ***Low Risk***
Vendor Type: Attorney
Overall Cyber Maturity Level After Assessment: ***Moderate***
Overall Vendor Risk: ***Low Risk: Satisfactory***
Periodic Follow-up Recommendation: *Every 3 years*

Vendor Review:

Abato Rubenstein and Abato, P.A provides attorney services to Waterfront Warehouse Local 1429 Pension Plans. This is a small operation consisting of roughly 11 employees. While it would be difficult for this Vendor to meet all the requirements set forth by the DOL, key controls should

still be implemented.

The Vendor is missing the following Security Controls:

- A formal Cybersecurity and IT Program.
- Phishing Tests are not performed on a periodic basis.
- Does not have a Third-Party Due Diligence program.
- A formal and documented Disaster Recovery and Business Continuity Plan.
- A formal Incident Response Plan.
- Data at rest and in Transit is not encrypted.
- Does not perform Annual Prudent Risk Assessments.
- Does not perform a third-party audit of Security Controls.
- Employees are not subject to background checks.

Client Follow-up Considerations for the Vendor:

As noted, highly robust controls may not be practical for the risk and size of the Vendor; however, the following should be considered for implementation by the Vendor.

- Implement a formalized documented Cybersecurity program with policies and procedures which follow Cybersecurity best practices.
- Perform periodic phishing tests on a periodic basis for all employees.
- Adopt a Third-Party Due Diligence program which is to be enacted at the time of vendor acquisition and reviewed periodically based on risk.
- Construct and implement a formalized Disaster Recovery and Business Continuity Plan.
- Create an Incident Response Plan which contains aspects of breach management protocols and perform tabletop exercises annually.
- Implement an email encryption mechanism for all data outbound.
- Enforce encryption on all laptop devices such as Microsoft BitLocker and File vault for any MAC Devices.
- Perform annual risk assessments to detect security gaps within their environment and implement security measures to remediate the gaps discovered.
- Hire a third party to perform an assessment of their security controls to be sure that they are functioning effectively.
- At a minimum perform a background check for all employees at hire.

Bolton USA

Inherent Risk: ***Moderate***
Vendor Type: Consulting Actuary
Overall Cyber Maturity Level After Assessment: ***High***
Overall Vendor Risk: ***Low Risk: Satisfactory***
Vendor Consideration: Cybersecurity Incident

During PKF O'Connor Davies review of Bolton USA, we noted that there was a cybersecurity incident that took place on October 7th, 2021. Details of the incident were not disclosed despite our further inquiries. We noted that at the time of the incident, Bolton USA's Cybersecurity Insurance Company provided them with a Cybersecurity Forensics Investigation Team. The team performed their forensic investigations and provided a report to Bolton USA based on their findings. However, Bolton USA has advised that the investigation is still ongoing.

Client Considerations for the Vendor:

- The Client should reach out to the Vendor to identify if any of their Data was part of the cybersecurity incident which is still being investigated.

ONGOING APPROACH

The initial year review as designed was sufficient to establish a baseline of maturity and risk across the Vendors in relation to the DOL Cybersecurity Guidance. The limitations of strictly going by the DOL Guidance, as we have learned, is that it has a tendency to be broad and the vendor responses reflected that. We believe this methodology is only effective for year one to establish the general baseline and also make the Vendors accustomed to the process and expectations. For many of the Vendors, it took a lot of back and forth to make them understand a generic and limited answer was not going to be sufficient for us and the expectations were higher than they perceived. We recognize Local 1429 may not want to do this every year, as such, the following proposed approach for subsequent years is as follows:

- Each Vendor is formally risk assessed to determine the risk of the Vendor to Local 1429. The risk assessment should factor in the overall results of this assessment, their size, and maturity. Any Vendor identified as having Low or Moderate maturity based on this assessment will automatically be considered a High risk vendor and be reassessed in the subsequent year to identify remediation progress. Vendors with Low or Moderate maturity will be reassessed annually until their ranking changes to Moderate-High or High.

- Any Vendor identified as a Moderate-High or High maturity must be reassessed at a frequency of every other year or once every three years.

- Any Vendor that experiences a breach that materially impacts Local 1429, and their members will be deemed a High risk vendor for a period of three years and will be reassessed annually during that period.

- A detailed questionnaire should be created that lists very specific controls that should be implemented. Controls will be weighted based on criticality. Such a method will allow us to generate a quantitative scoring process for the Vendors. In addition, it will help advise Vendors of controls that we believe are critical and need to be implemented if not. We will provide a suggested form to use going forward for any new Vendor and subsequent assessments.

The above is a risk-based approach to the Vendors. Should Local 1429 desire a full review every year or have a different proposed method, we will accommodate accordingly, should we continue to assist the Fun

VENDOR EVALUATION OVERVIEW

Below is a chart summarizing the overall breakdown of the vendors assessed for Local 1429.

Vendor	Vendor Type	Inherent Risk	Security Controls Status	Number of Deficiencies Discovered	Maturity Level	Unsatisfactory / Satisfactory
AALLC	Fund Administrators	High	Fully Implemented	0	High	Satisfactory
Abato, Rubenstein and Abato, P.A	Attorney	Low	Partially Implemented	9	Moderate	Satisfactory
Bolton	Consulting Actuary	Moderate	Fully Implemented	0	High	Satisfactory
The Houser-Ford Group	Investment Consulting	Low	Fully Implemented	0	High	Satisfactory