

Vendor Name: Powerhouse Group

Tracking

- Submitting to: *Mr Smith*
 - Date: *09/12/2020*
 - Tier: 2
 - Status: *Complete*
-

Assessment Summary

Assessment Description

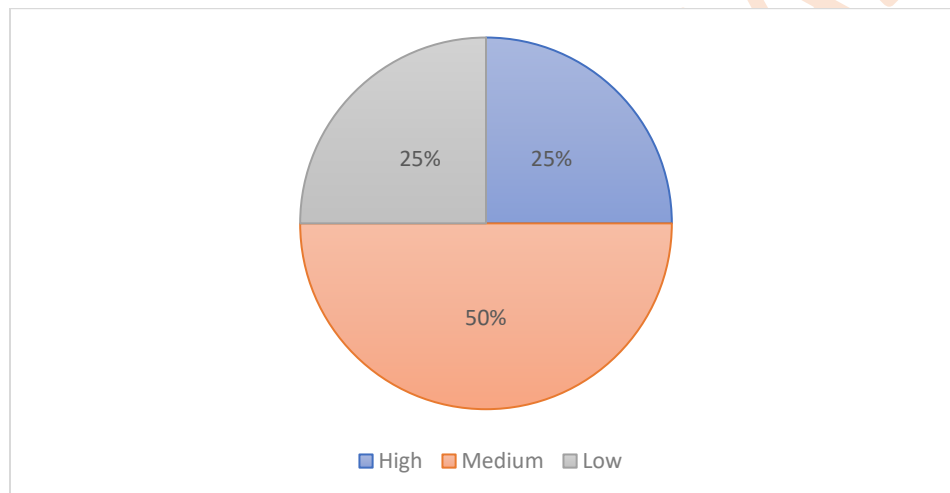
Powerhouse Group is providing an investment tool that will be used by *(client name)* for designing email messages, template sharing, tracking, and monitoring investment efficiency through analytics. The SaaS solution will be used by *(client name)* employees and contractors and expected to go live by Q4 2020.

Vendor Description

Powerhouse Group Ltd was founded in 1998. The company's line of business includes investing in commodity contracts, tax liens, venture capital companies, or other miscellaneous investing.

Findings Summary

Count of Unremediated Findings	Risk Rating
1	High
2	Medium
1	Low
4	Total



Findings by Category

Access Control (AC)

1. Vendor has no formal identity and access management program – **High**

Awareness and Training (AT)

2. Unable to validate if a formal security awareness training program has been established for vendor' employees – **Medium**

I. SRA Summary

The Security Risk Assessment (SRA) process is designed to document the risks identified in vendor systems, applications and platforms that process and/or store company data. This document provides an evaluation of the identified findings and the recommendations for management consideration.

ES Consult provides this information to the project manager, Information Technology (IT) owners and relevant stakeholders, as appropriate, to allow them to make well-informed decisions regarding risks that may impact the confidentiality, integrity and availability of the company environment. It is ultimately the responsibility of management to determine risk tolerance and to implement measures to reduce risk exposure to an acceptable level.

II. Engagement Characteristics

Question	Response
Availability: What is the maximum amount of time this application/service can be unavailable before causing serious impact to the business?	4 – week(s)
Information Classification: What type(s) of sensitive company data does/will this product/service store, transmit, receive and/or process?	Other Company Internal Information
Will this service or application connect with any critical internal systems?	No
Hosting Options: Where will this application and/or service be hosted?	Vendor site/ Cloud
User Identification: Number of employees/contractors/vendors that will access this application/service/information	Less than 100
User Identification: Who are the users of this application/service	Employees / Contractors
Endpoint Usage: What type of devices can be used to access the system?	Only (<i>client name</i>) managed computer/laptop/mobile device
How will this application/service be accessed?	Within (<i>client name</i>) internal networks only
Service Framing: Will this product/service store, transmit, receive and/or process sensitive data?	Yes
SDLC: How is/will this application/service be developed?	COTS

III. SRA Evidence Review Scope

The following evidence was provided during the assessment period:

Evidence type	Comments
Information Security Policy	
Vulnerability Scan Report	

IV. Information Security SRA Findings

Control Family: Access Control (AC)	Finding: Vendor has no formal identity and access management program
<p>Findings Description: Vendor has not formal identity and access management program. Additionally, there is no documented process for access review. An access management policy provides an overview of the safeguards in place to manage user access provisioning, user access re-certifications, and user access terminations. An access management policy may include safeguards to facilitate access authorizations and acceptable usages of the information system. Access control limits access to a system or to physical or virtual resources. It is a process by which users are granted access and certain privileges to systems, resources, or information.</p> <p>Risk Statement: The lack of an access management policy may allow for organizational personnel with information security responsibility to improperly provide access to an unauthorized user. The principle of least privilege may not be followed by organizational personnel when granting access and privilege to employees into information systems and scoped data. Not having a proper Access Control policy may result in the increase of incidents. Access Control standards force users, both client and customer, to adhere and follow mandated configurations such as password requirement and session inactivity controls. If controls are not communicated, then the organization may experience non-compliance to internal organizational requirements.</p> <p>Analyst Comments: ES Consult communicated the findings to vendor on 09/01/2020. Vendor responded on 09/12/2020 stating 'We currently do not have the policy in place. We have plans of completing one in the next few months.' Based on vendor's response, this finding will remain open.</p> <p>Evidence Reference: SRA AC.001</p>	
Risk Rating: High	Finding Status: Pending Remediation



V. Observations

Appendix

LIKELIHOOD	DESCRIPTION
Certain	There is a high chance that a threat could exploit a vulnerability and cause a loss to a system or its data. (On Average, more than 1 operational risk event per month)
Likely	It is probable that a threat could exploit a vulnerability and cause loss to a system or its data. (On Average, more than 1 operational risk event per month)
Possible	There is a possibility that a threat could exploit a vulnerability and cause loss to a system or its data. (Operational risk event estimated to occur within 1 year)
Unlikely	There is a little to no chance that a threat could exploit a vulnerability and cause loss to a system or its data. (Operational risk event estimated not to occur within 1 year)

IMPACT	DESCRIPTION
Critical	If vulnerabilities are exploited by threats, severe loss to the system, networks and data could occur.
High	If vulnerabilities are exploited by threats, a significant loss to the system, networks and data could occur.
Medium	If vulnerabilities are exploited by threats, a moderate loss to the system, networks and data could occur.
Low	If vulnerabilities are exploited by threats, little to no loss to the system, networks and data could occur.

LIKELIHOOD	IMPACT			
	Low	Medium	High	Critical
Certain	Medium	High	Critical	Critical
Likely	Low	Medium	High	Critical
Possible	Low	Medium	Medium	High
Unlikely	Low	Low	Low	Medium