Point-In-Time Cybersecurity Assessment

IT Cloud Provider | Cloud Hosting System

vendiligence™

Vendor Profile

IT Cloud Provider

Product
Cloud Hosting System

Assessment Date
09/28/2023

Service Description
The Vendor was noted as providing the following service(s): IT Cloud Provider-Cloud Hosting System

Domain URL
itcloudprovider.com

Vendor Type/Industry
Cloud Hosting Infrastructure

Vendiligence™ Overall Rating

SATISFACTORY

Vendor appears to maintain a partially well-formed control environment. Unanswered, unchecked, and unmitigated items should be internally assessed, then accepted or mitigated. Responses appear satisfactory.

Section Rating Summary

Security Testing	Information Security Governance	Sensitive Data Security
LOW	MEDIUM	MEDIUM

Report Comments and Recommendations

Vendor stated that Personally Identifiable Information (PII), Card Holder Data (CHD) and Protected Health Information (ePHI) is involved in the use of this product/service. Client is encouraged to request evidence that Vendor has a documented Third-Party Vendor Management/Due Diligence program in place. Client is encouraged to request evidence that Vendor has a documented PII Retention Policy in place as well as someone in leadership acting in the capacity of a Chief Information Security Officer. Vendor did not provide adequate evidence that data is encrypted in transit or at rest. Client is encouraged to request documentation surrounding current encryption methods. Client is encouraged to request information surrounding the following data security controls we would expect to see: DDoS Mitigation, Wireless Access Controls, Data Classification, Media Sanitization, Breach Notification, Environment Segmentation, and MFA for administrative access. Client is encouraged to request evidence that environmental equipment is properly maintained and serviced regularly

Legend

	A positive or affirmative response to the control category was provided by the vendor.	N/P	A response was not provided to the control category by the vendor.
	A negative or insufficient response to the control category was provided by the vendor.	N/A	The control category is not applicable to the scope of the assessment.

Assessment Of Controls

This assessment identifies key risks to your organization's operations, assets, and customers, posed by current and potential vendors. Each control within this assessment ties back to relevant industry guidance and standards addressing vendor risk, allowing key decision makers to confidently weigh vulnerabilities introduced by vendors and respond to the resulting risks.

Security Testing

Regulation Mapping | LOW

NO Penetration tests are performed by internal staff	YES Vulnerability scans/tests are performed by internal staff	YES Social engineering or phishing performed
YES Penetration tests are performed by a third party	YES Vulnerability scans/tests are performed by a third party	Frequency of social engineering tests: Monthly
Date of most recent penetration test: 2/1/2023	Frequency of vulnerability scans/tests: Daily	Frequency of social engineering tests (other): NA
Frequency of penetration testing: Quarterly	Frequency of vulnerability scans/tests (other): NA	
YES Any Medium or higher findings identified during the penetration tests are remediated timely	YES Any Medium or higher findings identified during the vulnerability tests are remediated timely	
Scope of penetration testing: Core Network		
Frequency of penetration testing (other): NA		

Security Testing Comments:

Vendor provided a third party penetration test executive summary documenting the most recent penetration test to include findings and remediation steps if applicable.

Provided report demonstrated a live test was performed within the last calendar year.

Vendor's penetration test summary notated that the scope of the testing including their full Core network.

Provided report noted that test performed was for the 1st quarter and indicated subsequent quarter testing was scheduled.

Provided report included managements response and a documented POA for remediation of any findings.

Vendor states that Internal staff performs active monitoring of vulnerability scanning.

Vendor states they also use a third party scanning tool that is monitored internally.

Vendor has a documented remediation plan for addressing medium or higher findings during vulnerability tests.

Vendor states they perform regular social engineering/phishing tests that includes follow up training and additional testing for failures as needed.

Information Security Governance

Regulation Mapping | MEDIUM

Formal Programs or Policies

- YES Information Security
- YES Incident Management
- YES Change Management
- YES Mobile Device/BYOD
- N/P Cybersecurity Insurance
- YES Asset Management - Hardware
- YES Asset Management - Software
- NO Vendor Management/Due Diligence

Represented Practices

- YES Employee/Contractor Security Training
- YES Board/Executive/Senior Management Involvement
- NO Designated Chief Information Security Officer (CISO)
- YES Patch Management

Information Security Governance Comments:

Vendor provided a documented Information Security plan that included evidence of recent review and updates.

Vendor provided a documented Incident Management plan that included evidence of recent review and updates as well as a documented incident response plan.

Vendor provided a documented Change Management plan that included evidence of recent review and updates as well as clear segregation of environments and duties of review and approval.

Vendor did not provide evidence of any cyber related insurance coverages.

Vendor states they do not have a formal Third Party Risk Management program in place.

Vendor states that Employees and contractors are required to undergo security training during onboarding as well as annually thereafter.

Vendor's notates that the development of information security policies and procedures include the involvement of senior leadership.

Vendor states that they do not currently have a CISO, but do have a senior information security professional with the CISSP and CISA certifications acting within that capacity.

Vendor provided documented evidence of a Patch Management program that included regular interval patching and remediation.

Sensitive Data Security

Regulation Mapping | MEDIUM

N/P Encryption at Rest	YES Secure Device Baselining	NO Media Sanitization
N/P Encryption in Transit	YES Remote Access Requires Multifactor Authentication	YES Principle of Least Privilege
YES Logical Access Management	NO Data Classification	YES Separation of Duties

Incident Detection and Response

YES IDS/IPS	NO Breach Notification
YES Event Log Correlation and Analysis	YES Periodic Logical Access Review/Termination
YES Network Segmentation	
YES Antimalware	

Password Policy For Employee Access

YES Does vendor require appropriate complexity/length/unpredictability for employee passwords?	NO Multifactor authentication for administrative access

Sensitive Data Security Comments:

Information regarding Encryption at Rest was not provided for review.

Information regarding Encryption in Transit was not provided for review.

Vendor provided evidence that they have adequate Logical Access Management.

Vendor provided evidence of a secure device baselining process in place for all servers and workstations to include remote devices and laptops.

Vendor has a documented remote access policy that includes the requirement for multifactor authentication.

Vendor states they do not have a process or policy surrounding Data Classification.

Vendor states they do not have a process or policy surrounding Media Sanitization.

Vendor states they incorporate Principle of Least Privilege in account provisioning.

Vendor states they incorporate Principle of Separation of Duties in account provisioning.

Vendor provided evidence of IDS/IPS.

Vendor provided evidence of regular event log correlation and analysis with a written procedural document provided to the appropriate personnel upon hire and annually thereafter.

Vendor's documentation regarding network segmentation did not provide satisfactory evidence that the production environment was properly segmented from a testing environment.

Vendor provided evidence that antimalware was in use. Vendor's SOC 2 report also demonstrated that this control was tested by a third party auditor and no exception was found.

Vendor states they do not have a Breach Notification policy in place.

Vendor provided evidence that they do quarterly access reviews and access termination verifications.

Vendor's password policy follows NIST guidelines for proper password parameters.

Vendor does not require MFA for administrator access.

Disclaimer

It should be noted that it is the responsibility of the Board of Directors to determine whether the organization agrees with the opinion-based risk level expressed in this report.

All information contained in this assessment is the work product of the Venminder, Inc. Information Security Operations Team. Documents listed as Resources Utilized have been reviewed and assessed by an Information Security Subject Matter Expert and this assessment has been reviewed and approved for distribution. For more information on Venminder's Subject Matter Experts, please click here.

The objective of this Assessment is to assess a third party's general controls relating to their ongoing ability to protect data and deliver the products and services for which you have contracted. This assessment is not intended for, nor should it be used for, the purpose of assessing the third party's likelihood of suffering a data breach, attack, or other business impacting event causing the inability to provide contracted services, nor as a guarantee the vendor will follow any assessed plan or meet specified objectives. This Assessment is intended solely for the information and use by the client and is not intended to be and should not be used by anyone else other than the objectives listed herein.

Rating Explanation

LOW	Vendor appears to maintain a well-formed control environment. Unanswered, unchecked, and unmitigated items should be internally assessed, then accepted or mitigated. Responses appear appropriate.
MEDIUM	Vendor appears to maintain a partially well-formed control environment. Unanswered, unchecked, and unmitigated items should be internally assessed, then accepted or mitigated. Responses appear satisfactory.
HIGH	Vendor does not appear to maintain, or has provided insufficient evidence of, a well-formed control environment. Unanswered, unchecked, and unmitigated items should be internally assessed, then accepted or mitigated. Responses appear insufficient and/or introduce a cautionary level of risk.
SEVERE	Vendor does not appear to maintain, or has provided insufficient evidence of, a well-formed control environment. Unanswered, unchecked, and unmitigated items should be internally assessed, then accepted or mitigated. Responses appear insufficient and/or introduce a severe level of risk.

Industry Guidance and Standards Utilized

This assessment was developed using the following industry guidance and standards.

INDUSTRY GUIDANCE AND STANDARDS	MAPPING REFERENCE
AICPA Trust Services Criteria	TSC-*
California Consumer Privacy Act	CCPA-*
California Privacy Rights Act	CPRA.**
Canadian Personal Information Protection and Electronic Documents Act	PIPEDA.*
Center for Internet Security - Critical Security Controls v8	CSC-*
China Personal Information Protection Law	PIPL.*
Colorado Privacy Act	CPA.**
Connecticut Data Privacy Act	CTDPA.**
EU General Data Protection Regulation	GDPR-*
FFIEC IT Examination Handbook - Wholesale Payment Systems Booklet	WPS.**
FFIEC IT Examination Handbook - Audit Booklet	AUD.**
FFIEC IT Examination Handbook - Business Continuity Booklet	BCP.**
FFIEC IT Examination Handbook - Information Security Booklet	IS.**
FFIEC IT Examination Handbook - Management Booklet	MGT.**
FFIEC IT Examination Handbook - Operations Booklet	OP.**
FFIEC IT Examination Handbook - Outsourcing Technology Services	OT.**
FINRA Report on Cybersecurity Practices	FINRA-pg*
Health Insurance Portability and Accountability Act	HIPAA-*
Interagency Guidelines Establishing Information Security Standards	12CFR-**
Interagency Guidance on Third-Party Relationships (Board, FDIC, & OCC) 06.2023	TPRM.*
ISO/IEC 27001:2022	ISO.*
New York Department of Financial Services - 23 NYCRR 500	NYCRR-*
NIST Framework for Improving Critical Infrastructure Cybersecurity version 1.1	CSF.*
NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations	800-53-r5-**
NIST SP 800-63b Digital Identity Guidelines	800-63b.**
OCC 2021-36	OCC20**-**
SEC Regulation SCI reference to NIST 800-53 Rev. 4	800-53-**