HITRUST
6175 Main Street
Suite 400
Frisco, TX 75034

May 29, 2024

Thoropass, Inc.
228 Park Avenue South
PMB 41082
New York, NY 10003

Based upon representation from management as to the accuracy and completeness of information provided, the procedures performed by an Authorized External Assessor to validate such information, and HITRUST's independent confirmation that the work was performed in accordance with the HITRUST® Assurance Program requirements, the following platform, facilities, and supporting infrastructure of the Organization ("Scope") meet the HITRUST CSF® v11.3.0 Implemented, 1-year (i1) certification criteria:

Platform:

- Thoropass Application residing at Amazon Web Services (AWS – East and AWS – West)

Facilities:

- AWS - East (Data Center) managed by Amazon Web Services located in Virginia, United States of America
- AWS - West (Data Center) managed by Amazon Web Services located in Washington, United States of America

The certification is valid for a period of one year assuming the following occurs. If any of these criteria are not met, HITRUST will perform an investigation to determine ongoing validity of the certification and reserves the right to revoke the Organization's certification.

- No data security breach reportable to a federal or state agency by law or regulation has occurred within or affecting the assessed environment, and

- No significant changes in the business or security policies, practices, controls, and processes have occurred that might impact its ability to meet the HITRUST Implemented, 1-year (i1) certification criteria.

HITRUST has developed the HITRUST CSF, a certifiable framework that provides organizations with the needed structure, detail and clarity relating to information protection. With input from leading organizations, HITRUST identified a subset of the HITRUST CSF requirements that an organization must meet to be HITRUST Implemented, 1-year (i1) Certified. For certain

HITRUST CSF requirements that were not being met, the Organization developed a CAP that outlined its plans for meeting such requirements.

HITRUST performed a quality assurance review to ensure that the control maturity scores were consistent with the results of testing performed by the Authorized External Assessor. Users of this letter can refer to the document Leveraging HITRUST Assessment Reports: A Guide for New Users for questions on interpreting this letter and can contact HITRUST customer support at support@hitrustalliance.net. Users of this letter are assumed to be familiar with and understand the services provided by the organization listed above, and what specific services are being used by the user organization.

A full HITRUST Validated Assessment Report has also been issued by HITRUST which can also be requested from the organization listed above directly. Additional information on the HITRUST Assurance Program can be found at the HITRUST website at https://hitrustalliance.net.

HITRUST

Enclosures (2):

- Assessment Context
- Scope of Systems in the Assessment

HITRUST

Assessment Context

The HITRUST Implemented, 1-year (i1) Assessment is designed to address the need for a continuously-relevant cyber security assessment that incorporates best practices and leverages the latest threat intelligence to maintain applicability with information security risks and emerging cyber threats, such as ransomware and phishing. The i1 Assessment is intended for organizations needing a moderate level of assurance against HITRUST CSF framework that delivers full transparency, accuracy, consistency, and integrity.

HITRUST carefully curates the HITRUST CSF requirements in an i1 assessment to consider good security hygiene controls and cybersecurity best-practice controls. This design affords a high degree of coverage against authoritative sources generally viewed as security best practices. As a result, the HITRUST CSF requirements included in i1 Assessments provide a high degree of coverage against sources such as the HIPAA Security Rule; NIST SP 800-171; the NAIC Data Security Law; the FTC's GLBA Safeguards Rule (both the current version as well as the 2021 proposed update); NISTIR 7621: Small Business Information Security Fundamentals; the DOL's EBSA Cybersecurity Program Best Practices; and the HITRUST CSF requirements included in HITRUST's Essentials, 1-year (e1) assessment.

The i1 was also designed to be an evolving, threat-adaptive assessment and accompanying certification that leverages threat intelligence and best practice controls to deliver an assessment that addresses relevant practices and active cyber threats. In addition, HITRUST continually evaluates cybersecurity controls to identify those relevant to mitigating known risks using cyber threat intelligence data from leading threat intelligence providers. As a result, the i1 includes controls that were selected exclusively to address emerging cyber threats actively being targeted today.

HITRUST

Scope of the Assessment

Company Background

Thoropass Application is a compliance software-as-a-service centralized platform for building and automating your infosec and privacy compliance programs. The application provides for the implementation of controls, managing audits, responding to security questionnaires, and ensuring continuous compliance efforts. Thoropass developed the OrO Way: a first-of-its-kind approach to removing the friction and complexity associated with traditional infosec compliance processes and IT audits. Designed to maximize transparency and efficiency while ensuring the highest quality reports and attestations.

In-scope Platform

The following table describes the platform that was included in the scope of this assessment.

Thoropass Application	
Description	The application in scope is the Thoropass Application, which is a compliance software-as-a-service (SaaS) platform developed and managed by Thoropass and used by customers to build and automate compliance programs, implement controls, manage audits, respond to security questionnaires, and ensure continuous compliance efforts. The platform is a web application hosted entirely on Amazon Web Services (AWS) using primarily AWS native services for backend infrastructure including AWS Aurora and S3 buckets for databases and document storage, Lambda functions, ECS Fargate services, and EC2 virtual machines running Linux for backend compute infrastructure. The application is hosted in the AWS East region as the primary region with AWS West as the secondary region for data backups and redundancy. Users authenticate through Okta or AWS Cognito. Thoropass may contain details about their information security and compliance structure - except for business related names, emails, phone numbers, titles, etc. there is no other personally identifiable information outside of a business context.
Application(s)	Includes Polaris (construct) and Jarvis (audit) components
Database Type(s)	AWS Aurora
Operating System(s)	Linux

Thoropass Application	
Residing Facility	• AWS - East • AWS - West
Exclusion(s) from Scope	None

In-scope Facilities

The following table presents the facilities that were included in the scope of this assessment.

Facility Name	Type of Facility	Third-party Managed?	Third-party Provider	City	State	Country
AWS - East	Data Center	Yes	Amazon Web Services (AWS)		Virginia	United States of America
AWS - West	Data Center	Yes	Amazon Web Services (AWS)		Washington	United States of America

Services Outsourced

The following table presents outsourced services relevant to the scope of this assessment. The "Consideration in this Assessment" column of this table specifies the method utilized for each service provider relevant to the scope of this i1 assessment. Organizations undergoing i1 assessments have two options of how to address situations in which a HITRUST CSF requirement is fully or partially performed by a service provider (e.g., by a cloud service provider):

- The Inclusive method, whereby HITRUST CSF requirements performed by the service provider are included within the scope of the assessment and addressed through full or partial inheritance, reliance on third-party assurance reports, and/or direct testing by the external assessor, and

- The Exclusive (or Carve-out) method, whereby HITRUST CSF requirements performed by the service provider are excluded from the scope of the assessment and marked N/A with supporting commentary explaining that the HITRUST CSF requirement is fully

performed by a party other than the assessed entity (for fully outsourced controls) or through commentary explaining the excluded partial performance of the HITRUST CSF requirement (for partially outsourced controls).

Third-party Provider	Relevant Service(s) Provided	Consideration in this Assessment
Amazon Web Services (AWS)	Cloud hosting provider	Included
Google	Google Workspaces and G-Suite is used by Thoropass employees for email communications and internal collaboration. G-Suite Single Sign On (SSO) is used to manage Thoropass employee access to the AWS accounts used to host the Thoropass application.	Included
1Password	1Password is used as an internal tool for Thoropass engineers to securely manage authentication secrets for a limited number of Thoropass application system components.	Included
Rippling	Rippling is the mobile device management platform used to manage Thoropass employee workstations.	Included
Okta	Okta is used as the primary identity and access management system for managing customer identities in the Thoropass application.	Included

Overview of the Security Organization

Thoropass follows a holistic approach to information security combining several different security (and privacy) frameworks together such as the HITRUST CSF, ISO 27001, ISO 27701, ISO 9001, AICPA TSC's, GDPR, CCPA, EU-US DPF, and others. Thoropass's executive management has appointed a senior information (and privacy) official (i.e., the Data Protection Officer/CISO) with the mission and resources to coordinate, develop, implement, and maintain an information security and privacy program. The Data Protection Officer/CISO reports up through the VP of Engineering and co-chairs the Oversight and Risk Committee. The Oversight and Risk Committee is made up of senior leadership staff members who report to the Chief Operating Officer (COO)/Co-Founder and to the Board of Directors.

The information security/privacy team is led by the Data Protection Officer/CISO and one direct report with assistance to implement security (and privacy) controls from staff across engineering, product, operations, customer success, and others. The Data Protection Officer/CISO is responsible for the policies, procedures, and security/privacy controls required to comply with regulatory as well as contractual requirements. The Data Protection Officer/CISO manages and monitors the information security and privacy program.

The objectives of Thoropass's Information Security Management Program is to implement appropriate administrative, technical, and physical safeguards to provide for the confidentiality, integrity, and availability of Thoropass's information assets. Thoropass implements reasonable safeguards to protect information from unintentional/unauthorized use (or disclosure). Thoropass's Information Security Management Program covers the resources directly supporting Thoropass's software-as-a-service (SaaS) applications (and related services). Thoropass's goal is to mitigate, to the extent practicable, any harmful effect known to Thoropass of use/disclosure of information assets in violation of its policies/procedures, contractual obligations, or regulations. Thoropass maintains a risk management strategy implemented evenly across all facets of the organization to include identification, analysis, reporting, tracking, mitigation, and/or acceptance of risks.