SOC 3 Report

Liquidware

August 1, 2024 to August 1, 2025

A Type 2 Independent Service Auditor's Report on Controls Relevant to Security, Confidentiality and Availability



AUDIT AND ATTESTATION BY

PRESCIENT ASSURANCE

CPA

Prescient Assurance LLC.
1100 Market Street Suite 600
Chattanooga, TN 37402

www.prescientassurance.com
info@prescientassurance.com
+1 646 209 7319



AICPA NOTICE:

You may use the SOC for Service Organizations - Service Organizations Logo only for a period of twelve (12) months following the date of the SOC report issued by a licensed CPA. If after twelve months a new report is not issued, you must immediately cease use of the SOC for Service Organizations - Logo.

Table of Contents

Management's Assertion 5
Independent Service Auditor's Report 8
Scope 8
Service Organization's Responsibilities 8
Service Auditors' Responsibilities 8
Inherent Limitations 9
Opinion 10
System Description 11
Attachment A 12
The Principal Service Commitments and System Requirements 13
The Components of the System Used to Provide the Services 14
People 14
Data 15
Security Processes and procedures 16
Physical security 16
Logical access 16
Computer operations - backups 16
Computer operations - availability 17
Change management 17
Data communications 17
Boundaries of the system 18
The Applicable Trust Services Criteria and the Related Controls Designed to Provide Reasonable Assurance that the Service Organization's Service Commitments and System Requirements were Achieved 19
Integrity and Ethical values 19
Commitment to competence 19
Management's philosophy and operating style 20
Organizational structure and assignment of authority and responsibility 20
Human Resource policies and practices 21
Risk assessment process 21
Integration with risk assessment 21
Information and communication systems 21
Monitoring controls 22
On-going monitoring 22
Reporting deficiencies 22
Complementary Subservice Organization Controls (CSOCs) 23

SECTION 1

Management's Assertion



Management's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Liquidware's IT System throughout the period August 1, 2024 to August 1, 2025 to provide reasonable assurance that Liquidware's service commitments and system requirements relevant to Security were achieved. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of controls within the system throughout the period August 1, 2024 to August 1, 2025, to provide reasonable assurance that Liquidware's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality and Availability (applicable trust services criteria) set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). Liquidware's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment A.

Liquidware uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Liquidware, to achieve Liquidware's service commitments and system requirements based on the applicable trust services criteria. The description presents Liquidware's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Liquidware's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Liquidware, to achieve Liquidware's service commitments and system requirements based on the applicable trust services criteria. The description presents Liquidware's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Liquidware's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period August 1, 2024 to August 1, 2025, to provide reasonable assurance that Liquidware's service commitments and system requirements were achieved based on the applicable trust services criteria.

Signed by:
Kameran Sarlati
EBDD2FDB81BE4B3...

Kameran Sarlati
Director of IT
Liquidware

SECTION 2

Independent Service Auditor's Report



Independent Service Auditor's Report

To: Liquidware

Scope

We have examined Liquidware's ("Liquidware") accompanying assertion in Section I, titled "Management's Assertion" (the assertion) that the controls within Liquidware's Filespaces system (the system) were effective throughout the period August 1, 2024 to August 1, 2025, to provide reasonable assurance that Liquidware's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality, and Availability (applicable trust services criteria) set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Service Organization's Responsibilities

Liquidware is responsible for its service commitments and system requirements and for designing, implementing and operating effective controls within the system to provide reasonable assurance that Liquidware's service commitments and system requirements were achieved. In Section I, Liquidware has provided the accompanying assertion about the effectiveness of the controls within the system. When preparing its assertion, Liquidware is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Liquidware uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Liquidware, to achieve its service commitments and system requirements based on the applicable trust services criteria. The description presents Liquidware's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Liquidware's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Liquidware, to achieve Liquidware's service commitments and system requirements based on the applicable trust services criteria. The description presents Liquidware's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Liquidware's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Auditors' Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved

based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the controls are not effective to achieve Liquidware's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Liquidware's service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risks that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

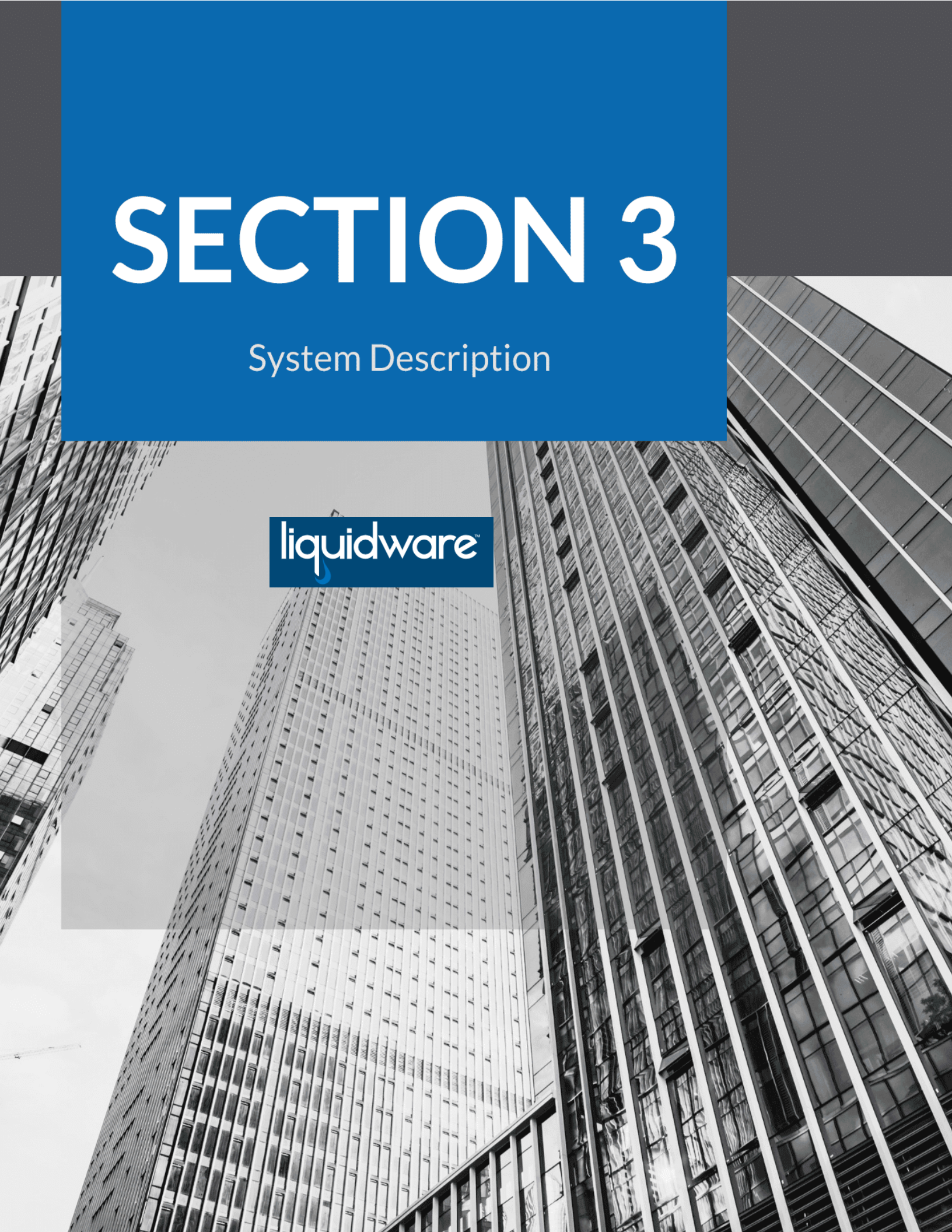
In our opinion, management's assertion that the controls within Liquidware's IT System were effective throughout the period August 1, 2024 to August 1, 2025 to provide reasonable assurance that Liquidware's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Signed by:
Prescient Assurance
B87FF418D4104D5...

Prescient Assurance LLC.
October 16, 2025

SECTION 3

System Description



Attachment A

Company Overview and Types of Products and Services Provided

Company Background

Liquidware is the leader in digital workspace management solutions. Our offerings encompass all facets of digital workspace management to ensure a consistent quality user experience across all Windows desktops, including physical, virtual, DaaS or in the cloud.

Description of services overview or services provided

Liquidware is the leader in Digital Workspace Management solutions that go beyond Digital Employee Experience (DEX). The company's solutions provide comprehensive DEX coverage by encompassing four key areas – managing, delivering, monitoring, and controlling DEX across physical, virtual, DaaS, or in the cloud. Globally, numerous enterprises leverage Liquidware's offerings to significantly reduce the time and effort involved in digital workspace management, while also enhancing security, flexibility, and scalability. Supported platforms include Microsoft physical, Azure Virtual Desktop (AVD), Windows 365, Citrix®, Omnissa Horizon, Amazon® WorkSpaces, and Dizzion® Frame. Liquidware products are available through a global network of partners.

About ProfileUnity - ProfileUnity transforms user environment management with advanced access control, granular context-aware filters, universal profiles and efficient application management, ensuring rapid logins and overcoming traditional Active Directory limitations.

About FlexApp - FlexApp revolutionizes application delivery by seamlessly providing applications from any location on various platforms, including cloud storage and traditional network shares, enhancing user experience with adaptability and offline functionality, and positioning organizations at the forefront of application lifecycle management.

About Stratusphere UX - With comprehensive data that outpaces other monitoring solutions Stratusphere UX provides unique features including process optimization, UX scoring, user-sentiment feedback, and security, machine health and resource metrics ensuring seamless deployments and migrations that align with user expectations for a frustration-free digital experience.

About CommandCTRL - CommandCTRL redefines workspace management with real-time insights, comprehensive desktop control, and award-winning monitoring, featuring intuitive diagnostics and the innovative Switch feature for proactive, non-intrusive troubleshooting, ensuring a secure, compliant, and highly responsive digital environment.

The Principal Service Commitments and System Requirements

Liquidware Labs, Inc. designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Liquidware Labs, Inc. makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Liquidware Labs, Inc. has established for the services. The system services are subject to the Security, Confidentiality, and Availability commitments established internally for its services.

Security commitments

Security commitments include, but are not limited to, the following:

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system
- Regular vulnerability scans over the system and network, and penetration tests over the production environment
- Operational procedures for managing security incidents and breaches, including notification procedures
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal

Confidentiality commitments

Confidentiality commitments include, but are not limited to, the following:

- The use of encryption technologies to protect system data both at rest and in transit
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties
- Confidential information must be used only for the purposes explicitly stated in agreements between The Company and user entities

Availability commitments

Availability commitments include, but are not limited to, the following:

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components
- Responding to customer requests in a reasonably timely manner
- Business continuity and disaster recovery plans that include detailed instructions, recovery point objectives (RPOs), recovery time objectives (RTOs), roles, and responsibilities
- Operational procedures supporting the achievement of availability commitments to user entities

The Components of the System Used to Provide the Services

The System is comprised of the following components:

- Software - The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.
- People - The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- Data - The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- Procedures - The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

People

The company employs dedicated team members to handle major product functions, including operations, and support. The IT/Engineering Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the company and its data secure.

Liquidware Labs, Inc. has a staff of approximately 1 organized in the following functional areas:

Management: Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.

This includes:
CEO - David Bieneman
COO - Chris Akerberg
CTO - Jason Mattox

Operations: Responsible for maintaining the availability of production infrastructure, and managing access and security for production infrastructure. Only members of the Operations team have access to the production environment. Members of the Operations team may also be members of the Engineering team.

Information Technology: Responsible for managing laptops, software, and other technology involved in employee productivity and business operations.

Product Development: Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality.

Data

Data as defined by Liquidware Labs, Inc., constitutes the following:

User and account data - this includes Personally Identifiable Information (PII) and other data from employees, customers, users (customers' employees), and other third parties such as suppliers, vendors, business partners, and contractors. This collection is permitted under the Terms of Service and Privacy Policy (as well as other separate agreements with vendors, partners, suppliers, and other relevant third parties). Access to PII is controlled through processes for provisioning system permissions, as well as ongoing monitoring activities, to ensure that sensitive data is restricted to employees based on job function.

Data is categorized in the following major types of data used by Liquidware Labs, Inc.

Category	Description	Examples
Public	Public information is not confidential and can be made public without any implications for Liquidware Labs, Inc..	• Press releases • Public website
Internal	Access to internal information is approved by management and is protected from external access.	• Internal memos • Design documents • Product specifications • Correspondences
Customer data	Information received from customers for processing or storage by Liquidware Labs, Inc.. Liquidware Labs, Inc. must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Customer operating data • Customer PII • Customers' customers' PII • Anything subject to a confidentiality agreement with a customer
Company data	Information collected and used by Liquidware Labs, Inc. to operate the business. Liquidware Labs, Inc. must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Legal documents • Contractual agreements • Employee PII • Employee salaries

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements, if any. Customer data is captured which is utilized by the company in delivering its services.

All personnel and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, Liquidware Labs, Inc. has policies and procedures in place to proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

Security Processes and procedures

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by management, the executive team, and control owners. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

Physical security

Liquidware Labs, Inc.'s production servers are maintained by Microsoft Azure, AWS, and Google Cloud Platform. The physical and environmental security protections are the responsibility of Microsoft Azure, AWS, and Google Cloud Platform. Liquidware Labs, Inc. reviews the attestation reports and performs a risk analysis of Microsoft Azure, AWS, and Google Cloud Platform on at least an annual basis.

Logical access

Liquidware Labs, Inc. provides employees and contracts access to infrastructure via a role-based access control system, to ensure uniform, least privilege access to identified users and to maintain simple and repeatable user provisioning and deprovisioning processes.

Access to these systems are split into admin roles, user roles, and no access roles. User access and roles are reviewed on an annual basis to ensure least privilege access.

The Internal Information Technology team is responsible for provision access to the system based on the employee's role and HR ms has a background check completed. The employee is responsible for reviewing Liquidware Labs, Inc.'s policies, completing security training. These steps must be completed within 14 days of hire.

When an employee is terminated, The Internal Information Technology team's Senior Support Technologist with their team's support is responsible for deprovisioning access to all in scope systems within 72 hours for that employee's termination.

Computer operations - backups

Customer provided support log data is automatically deleted with IT team confirmation every 90 days. If there is an exception, the internal IT team will perform troubleshooting to identify the root cause of the failure of the data's deletion and will manually delete the data if necessary.

Backup infrastructure is maintained in Microsoft Azure, AWS, and Google Cloud Platform with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

Computer operations - availability

Liquidware Labs, Inc. maintains an incident response plan to guide employees on reporting and responding to any information security or data privacy events or incidents. Procedures are in place for identifying, reporting and acting upon breaches or other incidents.

Liquidware Labs, Inc. internally monitors all applications, including the web UI, databases, and cloud storage to ensure that service delivery matches SLA requirements.

Liquidware Labs, Inc. utilizes vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open source dependencies and maintains an internal SLA for responding to those issues.

Change management

Liquidware Labs, Inc. maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Data communications

Liquidware Labs, Inc. has elected to use a platform-as-a-service (PaaS) to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. The PaaS simplifies our logical network configuration by providing an effective firewall around all the Liquidware Labs, Inc. application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints.

The PaaS provider also automates the provisioning and deprovisioning of containers to match the desired configuration; if an application container fails, it will be automatically replaced, regardless of whether that failure is in the application or on underlying hardware.

Liquidware Labs, Inc. uses an automated monitoring service to perform regular vulnerability scans and engages an external firm to perform annual penetration testing to look for unidentified vulnerabilities, and the product team responds to any issues identified via the regular incident response and change management process.

Boundaries of the system

The boundaries are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries.

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities. This report does not include the Cloud Hosting Services provided by Azure at multiple facilities. This report does not include the Cloud Hosting Services provided by GCP at multiple facilities.

The Applicable Trust Services Criteria and the Related Controls Designed to Provide Reasonable Assurance that the Service Organization's Service Commitments and System Requirements were Achieved

Integrity and Ethical values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Liquidware Labs, Inc.'s control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Liquidware Labs, Inc.'s ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

Commitment to competence

Liquidware Labs, Inc.'s management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Security Training is provided to maintain the skill level of personnel in certain positions.

Management's philosophy and operating style

The Liquidware Labs, Inc. management team must balance two competing interests: continuing to grow and develop in a cutting edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly-sensitive data and workflows our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way Liquidware Labs, Inc. can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally any regulatory changes that may require Liquidware Labs, Inc. to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business.

Organizational structure and assignment of authority and responsibility

Liquidware Labs, Inc.'s organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Liquidware Labs, Inc.'s assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.

Human Resource policies and practices

Liquidware Labs, Inc.'s success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Liquidware Labs, Inc.'s human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation during their onboarding.
- Evaluations for each employee are performed on an annual basis.
- Personnel termination procedures are in place to guide the termination process and are documented in a termination checklist.

Risk assessment process

Liquidware Labs, Inc.'s risk assessment process identifies and manages risks that could potentially affect Liquidware Labs, Inc.'s ability to provide reliable and secure services to our customers. As part of this process, Liquidware Labs, Inc. maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular Liquidware Labs, Inc. product development process so they can be dealt with predictably and iteratively.

Integration with risk assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Liquidware Labs, Inc.'s system; as well as the nature of the components of the system result in risks that the criteria will not be met. Liquidware Labs, Inc. addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Liquidware Labs, Inc.'s management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and communication systems

Information and communication are an integral component of Liquidware Labs, Inc.'s internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

Liquidware Labs, Inc. uses several information and communication channels internally to share information with management, employees, contractors, and customers. Liquidware Labs, Inc. uses chat systems and email as the primary internal and external communications channels.

Structured data is communicated internally via SaaS applications and project management tools. Finally, Liquidware Labs, Inc. uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

Monitoring controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Liquidware Labs, Inc.'s management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-going monitoring

Liquidware Labs, Inc.'s management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Liquidware Labs, Inc.'s operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Liquidware Labs, Inc.'s personnel.

Reporting deficiencies

Our internal risk management tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Complementary Subservice Organization Controls (CSOCs)

Liquidware Labs, Inc.'s services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Liquidware Labs, Inc.'s services to be solely achieved by Liquidware Labs, Inc. control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Liquidware Labs, Inc..

The following subservice organization controls have been implemented by Microsoft Azure, AWS, and Google Cloud Platform and included in this report to provide additional assurance that the trust services criteria are met.

AWS

Category	Criteria	Control
Security	CC 6.4	Physical access to data centers is approved by an authorised individual.
Security	CC 6.4	Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
Security	CC 6.4	Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
Security	CC 6.4	Closed circuit television camera (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
Security	CC 6.4	Access to server locations is managed by electronic access control devices.
Security	CC 7.2	AWS is responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers.
Security	CC 7.2	AWS is responsible for protecting data centers against disruption in power supply to the processing environment by an uninterruptible power supply.
Security	CC 7.2	AWS is responsible for overseeing the regular maintenance of environmental protections at data centers.
Availability	A 1.2	AWS maintains formal policies that provide guidance for information security within the organisation and the supporting IT environment.
Availability	A 1.2	AWS has a process in place to review environmental and geo-political risks before launching a new region.

Availability	A 1.2	Amazon-owned data centers are protected by fire detection and suppression systems.
Availability	A 1.2	Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
Availability	A 1.2	Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon owned data centers
Availability	A 1.2	Amazon-owned data centers have generators to provide backup power in case of electrical failure.
Availability	A 1.2	Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies. Contracts also include provisions requiring communication of incidents or events that impact Amazon assets and/or customers to AWS.

Azure

Category	Criteria	Control
Security	CC 6.4	Procedures to restrict physical access to the data center to authorised employees, vendors, contractors, and visitors, have been established.
Security	CC 6.4	Security verification and check-in for personnel requiring temporary access to the interior of the data center facility, including tour groups or visitors, are required.
Security	CC 6.4	Physical access to the data center is reviewed quarterly and verified by the Data center Management team.
Security	CC 6.4	Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorised individuals.
Security	CC 6.4	The data center facility is monitored 24x7 by security personnel.
Availability	A 1.2	Data center Management team maintains, and tests data center managed environmental equipment within the facility according to documented policy and maintenance procedures.
Availability	A 1.2	Environmental controls have been implemented to protect systems

		inside data center facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.

Google Cloud Platform (GCP)

Category	Criteria	Control
Security	CC 6.4	Data center server floors, network rooms and security systems are physically isolated from public spaces and/or delivery areas.
Security	CC 6.4	Access to sensitive data center zones requires approval from authorized personnel and is controlled via badge access readers, biometric identification mechanism, and/or physical locks.
Security	CC 6.4	Data center perimeters are defined and secured via physical barriers.
Security	CC 6.4	Access lists to high security areas in data centers are reviewed on a defined basis and inappropriate access is removed in a timely manner.
Security	CC 6.4	Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of the visit.
Security	CC 6.4	Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.
Security	CC 6.4	Data centers are continuously staffed and monitored by security personnel using real time video surveillance and/or alerts generated by security systems.
Availability	A 1.2	Critical power and telecommunications equipment in data centers is physically protected from disruption and damage.
Availability	A 1.2	Redundant power is utilized to support the continued operation of critical data center equipment in the event of a loss of the primary power source(s).
Availability	A 1.2	Data centers are equipped with fire detection alarms and protection equipment.
Availability	A 1.2	The organization's information processing resources are distributed across distinct, geographically dispersed processing facilities to support service redundancy, and availability.

Availability	A 1.2	The organization conducts disaster resiliency testing (DiRT) which covers reliability, survivability, and recovery on an ongoing basis (and at least annually).

Liquidware Labs, Inc. management, along with the subservice provider, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Liquidware Labs, Inc. performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling output reports
- Holding periodic discussions with vendors and subservice organization(s)
- Making regular site visits to vendor and subservice organization(s') facilities
- Testing controls performed by vendors and subservice organization(s)
- Reviewing attestation reports over services provided by vendors and subservice organization(s)
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

Any Specific Criterion of the Applicable Trust Services Criteria That is Not Relevant to the System and the Reasons it is Not Relevant

All Common Criteria/Security, Availability and Confidentiality criteria were applicable to Liquidware Labs, Inc.'s system.