Liquid Web, LLC

Data Center, Virtual Private Hosting, Dedicated Hosting, and Cloud Sites Services

SOC 3®

November 1, 2023 - October 31, 2024

UHY LLP
www.uhy-us.com

Table of Contents

Section 1:

Independent Service Auditor's Report

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of:
Liquid Web, LLC
2703 Ena Dr.
Lansing, MI 48917

Scope

We have examined Liquid Web, LLC's ("Liquid Web") accompanying assertion titled "Liquid Web Management's Assertion" (assertion) that the controls within the Liquid Web system were effective throughout the period November 1, 2023 to October 31, 2024, to provide reasonable assurance that Liquid Web's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (applicable trust services criteria) set forth in *TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (trust services criteria).*

Service Organization's Responsibilities

Liquid Web 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 Liquid Web's service commitments and system requirements were achieved. Liquid Web has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Liquid Web is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's 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.

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

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Liquid Web'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 Liquid Web's service commitments and system requirements based the applicable trust services criteria.

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

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 risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Basis for Qualified Opinion

During the period June 10, 2024 to June 11, 2024 Liquid Web detected and responded to a security incident. Controls failed to prevent the unauthorized access to and the installation of malware on internal hosting systems supporting the Cloud Sites services resulting in an extended downtime for Cloud Sites services customers. Consequently, controls did not operate effectively to provide reasonable assurance that Liquid Web's service commitments and system requirements were achieved based on the trust service criterion CC6.6 - *The entity implements logical access security measures to protect against threats from sources outside its system and boundaries*

Opinion

In our opinion, except for the effects of the matter giving rise to the modification described in the preceding paragraph, management's assertion that the controls within Liquid Web, LLC's Data Center, Virtual Private Hosting, Dedicated Hosting, and Cloud Sites services system were effective throughout the period November 1, 2023 to October 31, 2024 to provide reasonable assurance that Liquid Web service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Farmington Hills, MI
March 28, 2025

Section 2:

Liquid Web Management's Assertion

Liquid Web Management's Assertion:

We are responsible for designing, implementing, operating, and maintaining effective controls within Liquid Web, LLC's ("Liquid Web") Data Center, Virtual Private Hosting, Dedicated Hosting, and Cloud Sites services system (system) throughout the period November 1, 2023, to October 31, 2024, to provide reasonable assurance that Liquid Web's service commitments and system requirements relevant to Security and Availability were achieved. Our description of the boundaries of the system is presented in Section 3 and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period November 1, 2023, to October 31, 2024, to provide reasonable assurance that Liquid Web's service commitments and system requirements were achieved based on the trust services criteria relevant to the Security 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). Liquid Web'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 included in Section 3 of the report.

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.

Except for the matter described in the following paragraph, we assert that the controls within the system were effective throughout the period November 1, 2023, to October 31, 2024, to provide reasonable assurance that Liquid Web, LLC's service commitments and system requirements were achieved based on the applicable trust services criteria.

Unauthorized inbound traffic was not restricted from the internet resulting in Cloud Sites services systems being down for an extended period of time during the period June 10, 2024 to June 11, 2024. Consequently, controls did not operate effectively during the period to provide reasonable assurance that Liquid Web's service commitments and system requirements were achieved based on the trust service criterion CC6.6 - *The entity implements logical access security measures to protect against threats from sources outside its system and boundaries*

Scott Arlen
Director, Network & Security Operations
Liquid Web, LLC

Section 3:

Liquid Web's Description of the Boundaries of its Data Center, Virtual Private Hosting, Dedicated Hosting, and Cloud Sites Services System

Overview

Liquid Web, LLC ("Liquid Web") was founded in 1997 as a privately held managed co-location, web hosting, and network and infrastructure services company and was acquired in 2015 by the private equity firm, Madison Dearborn Partners. Liquid Web is now a multi-brand, multi-service data center, web hosting, and managed services provider. Liquid Web has over 30,000 clients served in over 150 countries.

Description of the Service Offerings Provided

The organization provides a variety of services to customers. The in-scope services include:

Data Center Services

Data center services are provided at facilities owned and operated by the organization. This service provides for the physical and environmentally secure data centers used by the organization to provide colocation and hosted services to clients. Key features of this service include physical access restrictions, video surveillance, fire detection and suppression systems, heating, ventilation, and air conditioning (HVAC) systems, automatic transfer switches (ATS), uninterruptible power supply (UPS), generators, and redundant internet and power feeds.

Virtual Private Hosting

The Virtual Private Hosting service offering provides customers clients virtual private servers (Windows and Linux) in a shared hosting environment. The service offering is provided through a tiered approach and includes the Self-Managed, Core Managed, and Fully Managed tiers. Key features of all tiers include data center services (described above), logical and network security around the hosting infrastructure, infrastructure management, 100% uptime, and 24/7 support. The Core Managed tier includes additional support services and operational and security patching services. The Fully Manage tier includes all services included in the previous tiers and add antimalware protection and Control Panel updates and patching.

Dedicated Hosting

The Dedicated Hosting service offering provides customers dedicated physical servers (Windows and Linux). The service offering is provided through a tiered approach and includes the Self-Managed, Core Managed, and Fully Managed tiers. Key features of all tiers include data center services (described above), logical and network security around the hosting infrastructure, infrastructure management, 100% uptime, and 24/7 support. The Core Managed tier includes additional support services and operational and security patching services. The Fully Manage tier includes all services included in the previous tiers and add antimalware protection and Control Panel updates and patching.

Cloud Sites

The Cloud Sites service offering provides a platform for customers to host websites through. Key features of this service offering data center services (described above), logical and network security around the hosting platform, infrastructure management, security and operating systems patching, backups, 100% uptime, and 24/7 support.

Principal Service Commitments and System Requirements

The organization designs its processes and procedures related its Data Center, Virtual Private Hosting, Dedicated Hosting, and Cloud Sites services to meet its objectives. Those objectives are based on the service commitments that the organization's management makes to user entities, the laws, and regulations that govern the provision of the colocation services system, and the financial, operational, and compliance requirements that the organization has established for the services.

Security commitments to user entities are documented and communicated in Terms of Service (TOS) and Service Level Agreements (SLAs) that have been established for each service. Security and availability commitments are standardized and include, but are not limited to, the following principal service commitments and system requirements:

- Providing physically secure data centers and restricting access to authorized personnel.
- Providing environmentally secure data centers with uninterruptible power and redundant internet connections.
- Providing network and logical security safeguards around infrastructure and systems used to provided services to customers.
- Providing 24/7 support for resolving customer questions and issues in accordance with TOS and SLAs.
- Ensuring networks and systems are available for use by customer in accordance with TOS and SLAs.

The organization's management establishes operational requirements that support the achievement of security and availability commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated via the organization's system policies and procedures and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the system.

Components of the System

System Boundaries

The boundaries of the system include the products and services related to the Data Center, Virtual Private Hosting, Dedicated Hosting, and Cloud Sites service offerings that are provided to customers out of its two Lansing, MI data centers and third-party data centers in Phoenix, AZ and Amsterdam, Netherlands.

Infrastructure

The organization's data centers are designed with redundancy installed at every level, ensuring that a failure at any level will not affect customer servers. Data center power is conditioned and reliable through the use of centralized Uninterruptible Power Supplies (UPS) solutions backed by generators. Data centers exclusively utilize premium bandwidth providers, ensuring minimal latency and fast connections to all points of the global internet.

The physical machines that provide hosting services for clients may be either dedicated (private servers wholly allocated to the customer) or virtual (share services between several customers). In addition, redundant network firewalls, routers and servers are installed to ensure network equipment failures do not impact customers' availability to their servers.

Servers can only be accessed via the internal network or via our VPN. There is no direct outside access to the servers in our Data Centers. Our Company also has limitations in place as to who can access the servers physically and virtually.

The network has been designed to accommodate clients demanding the highest quality network performance. There is a central focus on redundancy allowing our network to rapidly self-heal failures without interruptions to connectivity. Our redundancy is multi-tiered with N+1 internal device elements as well as entirely redundant chassis allowing any routing device to fail without interrupting client data connectivity. All core routing and switching equipment is obtained from industry leaders.

Software

The following systems comprise the Data Center, Virtual Private Hosting, Dedicated Hosting, and Cloud Sites services system:

- Identity Management System for Network and VPN access
- Wordpress for content management
- Security monitoring software including a portfolio of network and system security tools and applications
- Availability monitoring software including a robust set of proprietary system level health and service monitoring tools

People

The organization has defined how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. The organization is structured in distinct operating units which are listed below and further defined in the Organizational Structure section below:

- Executive Management
- Operations Control Center
- Security Team
- Support Team
- Platform Team
- Systems Restore and Data Operations Team
- Advance Services Team
- Purchasing Team

Executive Management: The Executive Management team is responsible for monitoring trends in the hosting services industry and identifying risks internally and externally. Executive management constantly considers new technology trends, risks, and opportunities as well as the impact of any applicable regulation or legislation on the security or availability of services provided. Executive Management is responsible for implementing appropriate measures to monitor and manage these risks. Appropriate measures may include the addition or revision of control procedures, conducting specific investigations, or any other means necessary to provide adequate control.

Operations Control Center: OCC consists of the network team and the monitoring team, to include security monitoring. The OCC teams utilize a robust set of proprietary system level health and service monitoring tools to constantly ensure server's optimal performance through early detection of problems. In the event that an issue is identified, the team responds immediately, reducing downtime and repairing any issues proactively, in many cases before the client is even aware of the problem. Server failure monitoring, disk space monitoring, load monitoring, and memory available monitoring is performed by the Monitoring Team. Alerts are tracked to resolution within the ticketing system. The OCC is following the NIST feed, US Cert Feed, and monitors for severe environmental conditions. An email notification would be sent out if there is something that needs to be documented as far as regulatory or environmental trends.

Security Team: The Security Team consists of security engineers, operators, and quality control/assurance personnel. The Security Team also oversees/manages compliance components. The Security Team continuously monitors the entire network for possible intrusions and attacks. The team investigates any issues and takes appropriate action. Real-time monitoring activity is presented in dashboards within the OCC. The network monitoring dashboard graphic displays potential attack signature messages detected by perimeter firewalls and reports the activity back to the Security team.

Support Team: The organization has established a 24/7/365 Support team that is professionally educated and available on-site at each data center 24 hours per day. The organization currently employs 320+ Support engineers with specialties in Technical Support, Service Delivery, Networking, Security and more.

Platform Team: The Platform team is responsible for keeping and maintaining our platforms that we offer to our customers. This group is responsible for but not limited to Maintaining all systems from both hardware and software perspective, Monitor and remediation of any system issues that could become customer impacting, Coordinate and execute maintenances, Handle escalations from our support escalation points via both Slack and tickets, Works on projects that are both proactive and reactive to solve any problems that arise in the environment and building tools to automate routine processes.

Systems Restore Team and Data Operation: The system restore team is responsible for the restoring failed systems for customer with the defined SLA's and relies on alerts from the monitoring team. The System Setup team configures the hardware and deploys customer devices into the datacenter as requested. The training team handles all aspects of training, including technical, security, and compliance related training.

Advance Services Team: The Advanced Services team is responsible for the service delivery, system restores, training and monitoring.

Purchasing Team: The Purchasing team is responsible for the tracking of and approval of new procurements, add-ons to existing assets, and renewals.

Processes and Procedures

The organization has implemented policies and procedures related to the in-scope services. These policies and procedures are available to applicable personnel, customers, and third parties and includes controls over all critical aspects of the system. The control within the system includes both automated and manual procedures which are described in the Control Actives section below. The key process and procedures include the following areas:

- Logical Security
- Physical Security
- Environmental Security
- Network Security
- Data Security and Disposal
- System Operations Monitoring
- Security Violation Reporting and Monitoring
- Change Management
- Business Continuity and Recovery

Data

The organization does not manage, access, transfer, or move client data or content.

Audit Logs and System Log Files - The system and network user activity, system activity, and systems diagnostics are captured in audit logs and system logs that are retained within the system and/or forwarded to monitoring and reporting tools for analysis.

Support Tickets – Data related to customer requests and support activities are retained within the ticketing system.

Client Accounts – Client account information is retained within the client portal for the management of the client subscription with the organization.