



Proprietary & Confidential



Fraud Dispute Offerings

SOC 2

Report on Quavo's System and Organization Controls
Relevant to Security



OCTOBER 1, 2021 TO SEPTEMBER 30, 2022



Table of Contents

I. Independent Service Auditor’s Report	1
II. Quavo’s Assertion	5
III. Quavo’s Description of Its Fraud Dispute Offerings	6
A. Services Provided	6
B. Principal Service Commitments and System Requirements	7
C. Components of the System Used to Provide the Services	7
1. Infrastructure	7
2. Software	9
3. People	9
4. Data	10
5. Processes and Procedures	10
D. Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring	10
1. Control Environment	10
2. Risk Assessment Process	13
3. Information and Communication	14
4. Monitoring Controls	14
E. Trust Services Category, Criteria, and Related Controls	15
F. Complementary Subservice Organization Controls	15
IV. Trust Services Category, Criteria, Related Controls, and Tests of Controls	17
A. Applicable Trust Services Criteria	17
Common Criteria	17
B. Description of Test of Controls and Results	34
V. Other Information Provided by Quavo That Is Not Covered by the Service Auditor’s Report	52
A. Management’s Response to Identified Testing Exceptions	52

I. Independent Service Auditor's Report

Quavo, Inc.
1201 North Orange Street
Wilmington, DE 19801

To the Management of Quavo, Inc. (Quavo):

Scope

We have examined Quavo's accompanying description of its system in Section III titled "Quavo's Description of Its Fraud Dispute Offerings" throughout the period October 1, 2021 to September 30, 2022 (description) based on the criteria for a description of a service organization's system in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that Quavo's service commitments and system requirements were achieved based on the trust services criteria for Security (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*).

The information included in Section V titled "Other Information Provided by Quavo That Is Not Covered by the Service Auditor's Report" is presented by Quavo management to provide additional information and is not a part of Quavo's description. Information about Quavo's management responses to identified testing exceptions has not been subjected to the procedures applied in the examination of the description and of the suitability of the design and operating effectiveness of the controls to achieve Quavo's service commitments and system requirements based on the applicable trust services criteria, and accordingly, we express no opinion on it.

Quavo uses Amazon Web Services (AWS) for cloud hosting and infrastructure services (subservice organization). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Quavo, to achieve Quavo's service commitments and system requirements based on the applicable trust services criteria. The description presents Quavo's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Quavo'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.



Service Organization's Responsibilities

Quavo 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 Quavo's service commitments and system requirements were achieved. Quavo has provided the accompanying assertion in Section II titled "Quavo's Assertion" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Quavo is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of the controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and Quavo's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether the controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of the controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

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

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating 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.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of our tests are listed in Section IV of this report titled "Trust Services Category, Criteria, Related Controls, and Tests of Controls."

Opinion

In our opinion, in all material respects:

- the description presents Quavo's Fraud Dispute Offerings that was designed and implemented throughout the period October 1, 2021 to September 30, 2022, in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the period October 1, 2021 to September 30, 2022 to provide reasonable assurance that Quavo's service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively throughout that period, and if the subservice organization applied the complementary controls assumed in the design of Quavo's controls throughout that period.
- the controls stated in the description operated effectively throughout the period October 1, 2021 to September 30, 2022 to provide reasonable assurance that Quavo's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Quavo's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Quavo, user entities of Quavo's Fraud Dispute Offerings during some or all of the period October 1, 2021 to September 30, 2022, business partners of Quavo subject to risks arising from interactions with the Fraud Dispute Offerings, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties



- Internal control and its limitations
- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

MOSS ADAMS LLP

San Francisco, California
December 15, 2022

II. Quavo's Assertion

We have prepared the accompanying description of Quavo's system in Section III titled "Quavo's Description of Its Fraud Dispute Offerings" throughout the period October 1, 2021 to September 30, 2022 (description) based on the criteria for a description of a service organization's system in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the Fraud Dispute Offerings that may be useful when assessing the risks arising from interactions with Quavo's Fraud Dispute Offerings, particularly information about system controls that Quavo has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security (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*).

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

We confirm, to the best of our knowledge and belief, that:

- the description presents Quavo's Fraud Dispute Offerings that was designed and implemented throughout the period October 1, 2021 to September 30, 2022, in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the period October 1, 2021 to September 30, 2022 to provide reasonable assurance that the Quavo service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively throughout the period, and if the subservice organization applied the complementary controls assumed in the design of Quavo's controls throughout that period.
- the controls stated in the description operated effectively throughout the period October 1, 2021 to September 30, 2022 to provide reasonable assurance that Quavo's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Quavo's controls operated effectively throughout that period.



III. Quavo's Description of Its Fraud Dispute Offerings

A. Services Provided

COMPANY OVERVIEW

Quavo is a financial technology (fintech) provider of automated dispute management solutions to issuing financial institutions. Quavo's disputes-as-a-service offering features automated software, artificial intelligence (AI) technology, and human intelligence services for financial organizations of all sizes. Quavo's goal is to establish and advance the industry standard in fraud and dispute management by instituting best-in-class principles, delivering unparalleled technology, and advocating for change in the community. Quavo's vision is to challenge industry norms through automation, innovation, and collaboration, delivering leading dispute management solutions that support and empower the fintech community while also inspiring the next generation of financial services technologists.

Quavo believes in providing a supportive and collaborative environment where the best financial and tech minds work together to drive client success and providing groundbreaking dispute management software and solutions.

SYSTEM DESCRIPTION

Quavo's automated dispute management software, Quavo Fraud and Disputes (QFD), is an end-to-end dispute management platform supporting all transaction types, facilitating cross-departmental communication, and integrating with virtually any banking platform. QFD automates workflows; Regulation E (electronic fund transfers), Regulation Z (truth in lending), and National Automated Clearing House Association (Nacha) compliance; and network mandates in one easily accessible system. Features like self-service, Spanish intake, and account holder communications are also supported, allowing QFD to integrate with current processes and corporate guidelines seamlessly. The dispute management AI completely automates the dispute resolution process.

ARIA is an AI system that performs an investigation, as a human would, collecting the data required by law for a successful resolution. ARIA applies tried and tested algorithms to virtually eliminate the challenges and complexities of this heavily regulated process.

Quavo also provides add-ons to its QFD software, namely Dispute Resolution Experts, the human intelligence service. Quavo's Dispute Resolution Experts manage back-office tasks for clients looking to outsource or supplement back-office staff. Clients maintain account-facing interactions and everyone operates on the QFD platform.

SYSTEM BOUNDARIES

The system boundaries for consideration within the scope of this report are the production systems, infrastructure, software, people, procedures, and data supporting QFD, ARIA, and Dispute Resolution Experts, collectively the Fraud Dispute Offerings (System).

Quavo offers the Fraud Dispute Offerings in hosted and customer on-premises versions. On-premises versions, or customer installations of the System, are excluded from the scope of this report.



SUBSERVICE ORGANIZATIONS

Quavo uses Amazon Web Services (AWS) for cloud hosting and infrastructure services. This subservice organization is excluded from the scope of this report. The controls it is expected to provide are included in the subsequent section titled Complementary Subservice Organization Controls.

B. Principal Service Commitments and System Requirements

Quavo designs its processes and procedures to meet its security objectives. Those objectives are based on the service commitments that Quavo makes to user entities and the financial, operational, and compliance requirements that Quavo has established for the System. Service commitments are declarations made by management to its customers regarding the performance of the Quavo System. Service commitments are set forth in standardized contracts and in the description of the service offering provided online and include commitments regarding the security of the system and of the information processed by the System in accordance with contractual stipulations.

Quavo establishes operational requirements that support the achievement of security commitments, relevant operational and compliance requirements, applicable laws and regulations, and other system requirements including the following:

- System functional and nonfunctional requirements derived from service commitments, published documentation of system functionality, and other descriptions of the system
- Monitoring of third-party providers to detect failures of those service providers to meet service agreements that could threaten the achievement of the service organization's service commitments and system requirements and respond to those failures

Such requirements are communicated in Quavo's system policies and procedures, system design documentation, and contracts with customers.

C. Components of the System Used to Provide the Services

1. Infrastructure

Quavo's System is a Software-as-a-Service (SaaS) cloud-based system. The primary components of the System are built on top of AWS using the following services:

AWS Service	Function
CloudFormation	CloudFormation is a service that helps model and set up AWS resources.
CloudFront	CloudFront is a web service that speeds up distribution of the static and dynamic web content.
CloudWatch	CloudWatch collects monitoring and operational data in the form of logs, metrics, and events and provides a unified view of AWS resources, applications, and services that run on AWS.



AWS Service	Function
Cognito	Cognito provides authentication, authorization, and user management of web and mobile apps.
DynamoDB	DynamoDB is a fully managed NoSQL database service.
Elastic Compute Cloud (EC2)	EC2 is a web service that provides secure, resizable compute capacity in the cloud.
Elastic File System (EFS)	EFS provides a simple, serverless, set-and-forget elastic file system to share file data without provisioning or managing storage.
Relational Database Service (RDS)	RDS is a web service used to operate relational databases in the AWS cloud.
Route 53	Route 53 is a scalable cloud Domain Name System (DNS) web service.
Simple Storage Service (S3)	S3 is virtual storage used in conjunction with EC2 to store object data. S3 is also used to automatically replicate data across AWS regions.
Virtual Private Cloud (VPC)	VPC is used to provision logically isolated virtual networks in the AWS cloud. VPC is used to manage the virtual networking environment, including selection of IP address ranges, creation of subnets, and configuration of route tables and network gateways.
Cloud9	Cloud9 is a cloud-based integrated development environment (IDE) to write, run, and debug code with just a browser.
Identity and Access Management (IAM)	IAM enables users to create and manage AWS users and groups and use permissions to allow and deny their access to AWS resources.
Key Management Service (KMS)	KMS makes it easy to create and manage cryptographic keys and control their use across a wide range of AWS services.
Lambda	Lambda is a serverless compute service for running code without provisioning or managing servers, creating workload-aware cluster scaling logic, maintain event integrations, or managing runtimes.
Secrets Manager	Secrets Manager is a secrets management service that helps protect access to applications, services, and IT resources.



AWS Service	Function
Systems Manager	Systems Manager gives visibility and control over infrastructure in AWS.
Web Application Firewall (WAF)	WAF is a web application firewall that helps protect web applications or application programming interfaces (APIs) against common web exploits that may affect availability, compromise security, or consume excessive resources.

2. Software

The System is built using the Pega platform, which generates Java source code. ARIA is built using AWS serverless tools.

Additionally, the following vendor software is used to help manage the System:

Vendor Software	Function
Bitbucket	Bitbucket is a Git-based source code repository hosting service.
Datadog	Datadog is a monitoring service for cloud-scale applications, providing monitoring of servers, databases, tools, and services, through a SaaS-based data analytics platform.

3. People

The control framework that supports Quavo's organizational environment starts with its executive team. The following are key roles involved in control implementation and maintenance:

- Chief Executive Officer (CEO)
- Chief Financial Officer (CFO)
- Chief Operating Officer (COO)

Responsibility for Quavo's information security resides with the COO. In addition to the overall governance provided by the executive team, the following teams play a key role in the execution of controls:

- *Engineering* – The Engineering team is responsible for software development.
- *Human Resources (HR)* – The HR team is responsible for employee onboarding, setting policies, and employee reviews.
- *Security* – The Security team is responsible for security of the applications and service data.



4. Data

Within the System, service data includes names, phone numbers, email addresses, mailing addresses, and other similar information and data retrieved from customer systems of record, such as Visa and Mastercard.

5. Processes and Procedures

Quavo has developed and communicated to its personnel procedures to protect service data and the company's assets. Procedures are documented and updated on the company intranet to help ensure personnel are informed and equipped to perform their duties to preserve the security of the System and the service data. These procedures include the following policies:

- Acceptable Use
- Asset Management
- Change Management / Separation of Duties
- Code of Conduct
- Data Protection
- Encryption and Key Management
- Incident Response
- Information Security
- Password
- Risk Assessment and Management
- System Access and Authorization Control
- Vendor Risk Management
- Vulnerability Management and Patch Program

D. Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

1. Control Environment

The Quavo control environment reflects the philosophy of senior management concerning the importance of integrity and ethical values. Quavo understands that leadership sets the tone from the top, where the actions of, and decisions by, management at all levels of the organization establish the basis for acceptable behavior. Quavo has established a Code of Conduct outlining ethical expectations, behavior standards, and ramifications of noncompliance, and requires internal personnel to acknowledge it.

ORGANIZATIONAL STRUCTURE

The Board of Directors is composed of senior management and external members, who are independent from Quavo's operations. On a quarterly basis, senior management meets with the Board of Directors to review business objectives, company initiatives, resource needs, and risk management activities, including results from internal and external assessments.



The structure of Quavo is defined in the organizational chart posted on the intranet. Management maintains the organizational chart to clearly identify positions of authority and the lines of communication and publishes this organizational chart to internal personnel.

HUMAN RESOURCES

Prior to employee onboarding, HR creates job descriptions as a standard to evaluate whether candidates are qualified to perform the required duties. Job descriptions document experience, skills, and education for new positions. Employment candidates pass through evaluative interviews against the posted job descriptions. If a candidate is successful in the screening process, a background check is initiated for new hires.

Formal hiring procedures are followed for new hires. The onboarding process begins when a candidate accepts and signs an offer letter. During orientation, Quavo works to ensure new hires are aware of their obligation to protect Quavo and customer information. Specifically, new hires and contractors review the Acceptable Use, Code of Conduct, Data Protection, and Information Security Policies and formally acknowledge their responsibilities to protect Quavo and service data within 30 days of hire.

Internal personnel complete information security training programs when they are hired and annually thereafter to help them understand their obligations and responsibilities, including the identification and reporting of security incidents. Failure to comply with these agreed-upon policies may result in a warning or even employee termination. Quavo has a formal process for documenting and reporting issues of noncompliance. Events and behaviors that do not meet expectations as outlined in policies are documented and disciplinary action is taken for the personnel responsible.

Throughout employment, the company evaluates the performance of internal personnel through a formal, annual performance evaluation. This process assesses the performance and competence of each individual and their compliance with company policies and procedures.

CONTROL ACTIVITIES

Controls have been established to help ensure processes operate as intended to keep service data secure.

AUTHENTICATION

Quavo mandates strong authentication requirements on production systems. First, access to production systems requires unique IDs and valid Secure Shell (SSH) keys. Customer passwords to production systems are required to be at least eight characters in length and meet complexity requirements. Internal personnel authenticate with the same user ID and password requirements, but also require two-factor authentication through the use of one-time password tokens.

USER PROVISIONING AND DEPROVISIONING

Quavo has implemented role-based security to limit and control access within Quavo's production environment. Users are provisioned access to systems based on role as defined in the access matrix. System owners review and approve the matrix annually. The COO approves any additional access required outside the access matrix. When an employee is terminated, the COO revokes production access within one business day of the employee's or contractor's separation date.



Once onboarded, customers have the ability to set up a Quavo account by using their email address and creating a password. The administrator of the account can invite, add, or remove team members to their company's Quavo account.

ACCESS REVIEWS

On a quarterly basis, the system owners conduct user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities. Identified access changes are tracked to remediation.

SYSTEM INVENTORY

The Quavo Security team identifies its information assets and updates the description and owners at least annually.

NETWORK SECURITY

In order to protect Quavo's production environment, firewall configurations help ensure available networking ports and protocols are restricted to port 22 and Transmission Control Protocol (TCP) for incoming traffic. Administrative access to production servers and databases is restricted to the COO and lead engineers.

ENCRYPTION

Quavo maintains its Encryption and Key Management Policy to support the secure encryption and decryption of application secrets and govern the use of cryptographic controls. In addition, Quavo users connect to the web application via Hypertext Transfer Protocol Secure (HTTPS) / Transport Layer Security (TLS). The traffic between the Quavo System and external connections is also encrypted in transit. Lastly, databases housing service data are encrypted at rest.

VULNERABILITY MANAGEMENT

Quavo maintains a vulnerability management program to detect and remediate system vulnerabilities. As part of this program, the Security team performs monthly internal vulnerability scans. Identified vulnerabilities rated critical or high are analyzed, communicated to responsible parties, and tracked until resolved by the Engineering team.

USER ENDPOINTS

Management has deployed agents on user endpoint systems to detect malicious code and malware and enforce hard disk encryption. Updates to these agents are deployed automatically.

SYSTEM MONITORING

Quavo uses logging and monitoring software to collect data from servers and endpoints and detect potential security threats or unusual system activity.

Quavo has also implemented intrusion prevention and detection tools to provide monitoring of network traffic to the production environment. Engineering personnel receive the alerts and respond based on the severity of these alerts.



INCIDENT MANAGEMENT

Management has established an Incident Response Plan outlining the process of identifying, prioritizing, communicating, assigning, and tracking incidents. Identified security events and issues are triaged and tracked to resolution in accordance with the Incident Response Plan. A “lessons learned” document is created after each incident and shared with the Engineering team.

CHANGE MANAGEMENT

Quavo has a formalized change management process documented in its Change Management / Separation of Duties Policy. Specifically, Quavo has developed policies and procedures governing the system development life cycle, including documented processes for tracking, testing, approving, and validating changes. Code and infrastructure changes are recorded in a ticketing system. The production environment is segregated from the staging environment to allow for changes to be tested outside of production. Production data is not used in the development and staging environments.

For code changes, manual testing is performed prior to changes being merged into production. Following testing, an independent engineer reviews these changes prior to deploying into production. System users who make changes to the development system are unable to deploy their changes into production without independent approval.

CONFIGURATION MANAGEMENT

Quavo uses a configuration management tool to help ensure production infrastructure images are standard and are using the latest configurations. Changes to configurations are tested, reviewed, and approved by an independent engineer before being deployed into production.

2. Risk Assessment Process

Quavo has established a Risk Assessment and Management Policy that includes the identification, evaluation, communication, and mitigation of risks relating to the company operations, safeguarding of informational assets, product development, and fraud. Within this policy, risk tolerance and strategies are defined. The COO reviews the Risk Assessment and Management Policy annually.

RISK IDENTIFICATION AND MITIGATION

On an annual basis, the COO performs an annual formal risk assessment over the System. This assessment includes the identification of relevant internal and external threats related to security and fraud and an analysis of risks associated with those threats. The COO maintains a risk register, which records the risk mitigation strategies for identified risks and the development or modification of controls consistent with the risk mitigation strategy. Action plans are created and tracked to address identified risks that are deemed unacceptable.

Management has obtained a cyber risk insurance policy to minimize the financial impact of a cybersecurity loss event.



VENDOR RISK MANAGEMENT

Prior to engaging a new vendor, the CFO performs an assessment to validate potential third-party service providers meet compliance requirements as defined in the Vendor Risk Management Policy. Quavo management maintains an inventory of service providers. The CFO assesses service providers, including an annual review of providers' SOC reports, to help ensure they are meeting expected security commitments.

3. Information and Communication

To help Quavo achieve its goals, management is committed to using quality information and effective communication channels with employees and customers. Descriptions of the System and its boundaries are available to internal and external users on the website.

INTERNAL COMMUNICATION

Management publishes policies and procedures, including the primary end-user policies for security (Data Protection Policy, Information Security Policy, Password Policy, System Access and Authorization Control Policy, and Vulnerability Management and Patch Program), on the intranet. The Information Security Policy outlines the roles and responsibilities for personnel with responsibility for the security of the system. The COO is responsible for the design, implementation, management, and annual review of the security policies.

Quavo has established a confidential reporting process for internal users and a support portal for external users to report issues or items of concern. Management monitors customer and internal complaints reported and responds in accordance with the Incident Response Plan.

EXTERNAL COMMUNICATION

Quavo communicates security commitments and expectations, changes to roles and responsibilities, and changes impacting the security of the System to customers. Customers may also contact Quavo through the website to report incidents, complaints, and failures on issues related to security. Internal or customer-initiated incident tickets are assigned to the appropriate team or individual and are prioritized based on policy and business impact. An internal tracking system is used to document issues through to resolution.

4. Monitoring Controls

To evaluate the effectiveness of its controls, the COO utilizes a compliance monitoring tool to continually assess controls and to alert when controls are identified as out of compliance. Senior management evaluates the results at least annually and resolves any deficiencies in accordance with the Risk Assessment and Management Policy. In addition, management performs additional monitoring activities, including quarterly user access reviews, monthly vulnerability scanning, and annual review of third parties.



E. Trust Services Category, Criteria, and Related Controls

Although the applicable trust services category, criteria, and related controls are presented in Section IV of this report titled "Trust Services Category, Criteria, Related Controls, and Tests of Controls", they are an integral part of Quavo's system description throughout the period October 1, 2021 to September 30, 2022.

F. Complementary Subservice Organization Controls

Quavo's controls related to the System cover only a portion of overall internal control for each user entity of Quavo. It is not feasible for the criteria related to the System to be achieved solely by Quavo. Therefore, each user entity's internal controls must be evaluated in conjunction with Quavo's controls and the related tests and results described in Section IV of this report, taking into account the types of controls expected to be implemented by the subservice organization as described below.

Complementary Subservice Organization Controls		Related Criteria
AWS		
1	Access to hosted systems requires users to use a secure method to authenticate.	➤ CC6.1
2	User content is segregated and made viewable only to authorized individuals.	➤ CC6.1
3	Network security mechanisms restrict external access to the production environment.	➤ CC6.1 and CC6.6
4	New user accounts are approved by appropriate individuals prior to being provisioned.	➤ CC6.2
5	User accounts are removed when access is no longer needed.	➤ CC6.2 and CC6.3
6	User accounts are reviewed on a regular basis by appropriate personnel.	➤ CC6.2 and CC6.3
7	Access modifications to hosted systems are approved by appropriate individuals prior to being provisioned.	➤ CC6.3
8	Access to physical facilities is restricted to authorized users.	➤ CC6.4
9	Production media is securely decommissioned and physically destroyed prior to being removed from the data center.	➤ CC6.5
10	Encrypted communication is required for connections to the production system.	➤ CC6.6
11	Access to hosted data is restricted to appropriate users.	➤ CC6.7
12	Hosted data is protected during transmission through encryption and secure protocols.	➤ CC6.7



Complementary Subservice Organization Controls		Related Criteria
13	Anti-virus or anti-malware solutions are installed to detect or prevent unauthorized or malicious software.	➤ CC6.8
14	System configurations changes are logged and monitored.	➤ CC7.1
15	Vulnerabilities are identified and tracked to resolution.	➤ CC7.1
16	Security events are monitored and evaluated to determine potential impact per policy.	➤ CC7.2
17	Operations personnel log, monitor and evaluate to incident events identified by monitoring systems.	➤ CC7.3
18	Operations personnel respond, contain and remediate incident events, and update stakeholders, as needed.	➤ CC7.4
19	System changes are documented, tested, and approved prior to migration to production.	➤ CC8.1
20	Access to make system changes is restricted to appropriate personnel.	➤ CC8.1



IV. Trust Services Category, Criteria, Related Controls, and Tests of Controls

This SOC 2 Type 2 Report was prepared in accordance with the AICPA attestation standards and has been performed to examine the suitability of the design and operating effectiveness of controls to meet the criteria for the Security category set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) throughout the period October 1, 2021 to September 30, 2022.

The trust services category for the Security criteria and related controls specified by Quavo are presented in Section IV of this report.

A. Applicable Trust Services Criteria

Common Criteria

CC1.0 Common Criteria Related to Control Environment				
	Trust Services Criteria	Control #	Controls Specified by Quavo	Test Results
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	ORG-01	Quavo has established a Code of Conduct outlining ethical expectations, behavior standards, and ramifications of noncompliance.	ORG-04: For 1 of 10 internal personnel selected, an annual performance evaluation was not completed.
		ORG-04	Quavo evaluates the performance of internal personnel through a formal, annual performance evaluation.	
		ORG-10	Management publishes the Acceptable Use, Code of Conduct, Data Protection, and Information Security policies to internal personnel. In addition, internal personnel acknowledge these policies within 30 days of hire.	
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	ORG-02	The Board of Directors includes senior management who are independent from the company's operations.	No exceptions noted.
		ORG-03	Senior management meets with the Board of Directors semi-annually to review business objectives, company initiatives, resource needs, and risk management activities, including results from internal and external assessments.	



CC1.0 Common Criteria Related to Control Environment				
	Trust Services Criteria	Control #	Controls Specified by Quavo	Test Results
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	ORG-06	Management maintains a formal organizational chart to clearly identify positions of authority and the lines of communication and publishes the organizational chart to internal personnel.	No exceptions noted.
		POL-02	Quavo's Information Security Policy outlines roles and responsibilities for personnel with responsibility for the security of the system.	
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	ORG-04	Quavo evaluates the performance of internal personnel through a formal, annual performance evaluation.	ORG-04: For 1 of 10 internal personnel selected, an annual performance evaluation was not completed. ORG-07: For 1 of 10 new hires selected, the background check was not completed prior to their start date.
		ORG-07	Background checks are performed on new hires before the new hire's start date as permitted by local laws.	
		ORG-08	Hiring managers screen new hires to assess their qualifications, experience, and competency to fulfill their responsibilities.	
		ORG-09	Internal personnel complete annual training programs for information security to help them understand their obligations and responsibilities related to security. New hires complete training within 30 days of hire.	
		ORG-10	Management publishes the Acceptable Use, Code of Conduct, Data Protection, and Information Security policies to internal personnel. In addition, internal personnel acknowledge these policies within 30 days of hire.	
		POL-02	Quavo's Information Security Policy outlines roles and responsibilities for personnel with responsibility for the security of the system.	
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	ORG-01	Quavo has established a Code of Conduct outlining ethical expectations, behavior standards, and ramifications of noncompliance.	ORG-04: For 1 of 10 internal personnel selected, an annual performance evaluation was not completed.
		ORG-04	Quavo evaluates the performance of internal personnel through a formal, annual performance evaluation.	



CC2.0 Common Criteria Related to Communication and Information			
Trust Services Criteria	Control #	Controls Specified by Quavo	Test Results
CC2.1 The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	NET-05	The IT team uses logging and monitoring software to collect data from servers and endpoints and detect potential security threats and unusual system activity.	No exceptions noted.
	ORG-05	Quavo performs an annual assessment over internal controls used in the achievement of Quavo's service commitments and system requirements. Senior management evaluates the results and resolves any deficiencies in accordance with the Risk Assessment and Management Policy.	
	VM-03	Quavo engages a third party to conduct a network and application penetration test of the production environment at least annually. IT team reviews the results and tracks high priority findings to resolution.	



CC2.0 Common Criteria Related to Communication and Information			
Trust Services Criteria	Control #	Controls Specified by Quavo	Test Results
CC2.2 The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	COM-01	Descriptions of the company's system and its boundaries are available to internal personnel and external users.	No exceptions noted.
	COM-04	Quavo has a confidential reporting channel available for internal personnel and a support portal available for external users to report security concerns. Management monitors customer and internal complaints and responds in accordance with the Incident Response Plan.	
	ORG-01	Quavo has established a Code of Conduct outlining ethical expectations, behavior standards, and ramifications of noncompliance.	
	ORG-03	Senior management meets with the Board of Directors semi-annually to review business objectives, company initiatives, resource needs, and risk management activities, including results from internal and external assessments.	
	ORG-09	Internal personnel complete annual training programs for information security to help them understand their obligations and responsibilities related to security. New hires complete training within 30 days of hire.	
	ORG-10	Management publishes the Acceptable Use, Code of Conduct, Data Protection, and Information Security policies to internal personnel. In addition, internal personnel acknowledge these policies within 30 days of hire.	
	POL-02	Quavo's Information Security Policy outlines roles and responsibilities for personnel with responsibility for the security of the system.	



CC2.0 Common Criteria Related to Communication and Information				
	Trust Services Criteria	Control #	Controls Specified by Quavo	Test Results
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	COM-01	Descriptions of the company's system and its boundaries are available to internal personnel and external users.	No exceptions noted.
		COM-02	Quavo publishes its Privacy Statement to internal personnel and external users. This Privacy Statement details the company's security commitments.	
		COM-03	Customers are notified of any system changes impacting the security of the system.	
		COM-04	Quavo has a confidential reporting channel available for internal personnel and a support portal available for external users to report security concerns. Management monitors customer and internal complaints and responds in accordance with the Incident Response Plan.	



CC3.0 Common Criteria Related to Risk Assessment				
Trust Services Criteria		Control #	Controls Specified by Quavo	Test Results
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	RA-01	Management performs a formal review of the Risk Assessment and Management Program at least annually. Risk tolerance and strategies are defined in the policy.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	AC-01	Quavo identifies its information assets and maintains an inventory of its system components, owners, and their support of its information assets. IT maintains the list of information assets and inventory at least annually.	No exceptions noted.
		RA-02	The COO performs an annual formal risk assessment, which includes the identification of relevant internal and external threats related to security and fraud, and an analysis of risks associated with those threats.	
		RA-05	The relationship owner collects and reviews the SOC reports (or equivalent) of subservice organizations on an annual basis.	
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	RA-02	The COO performs an annual formal risk assessment, which includes the identification of relevant internal and external threats related to security and fraud, and an analysis of risks associated with those threats.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	RA-01	Management performs a formal review of the Risk Assessment and Management Program at least annually. Risk tolerance and strategies are defined in the policy.	No exceptions noted.
		RA-02	The COO performs an annual formal risk assessment, which includes the identification of relevant internal and external threats related to security and fraud, and an analysis of risks associated with those threats.	
		RA-04	Quavo's Vendor Risk Management Policy defines a framework for the onboarding and management of the vendor relationship lifecycle. The COO assesses new vendors according to the Vendor Risk Management Policy prior to engaging with the vendor.	



CC4.0 Common Criteria Related to Monitoring Activities				
	Trust Services Criteria	Control #	Controls Specified by Quavo	Test Results
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	ORG-05	Quavo performs an annual assessment over internal controls used in the achievement of Quavo's service commitments and system requirements. Senior management evaluates the results and resolves any deficiencies in accordance with the Risk Assessment and Management Policy.	No exceptions noted.
		VM-02	Vulnerability scans are executed monthly on production systems. IT tracks critical or high-risk vulnerabilities through resolution.	
		VM-03	Quavo engages a third party to conduct a network and application penetration test of the production environment at least annually. IT team reviews the results and tracks high priority findings to resolution.	
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	ORG-03	Senior management meets with the Board of Directors semi-annually to review business objectives, company initiatives, resource needs, and risk management activities, including results from internal and external assessments.	No exceptions noted.
		ORG-05	Quavo performs an annual assessment over internal controls used in the achievement of Quavo's service commitments and system requirements. Senior management evaluates the results and resolves any deficiencies in accordance with the Risk Assessment and Management Policy.	
		VM-02	Vulnerability scans are executed monthly on production systems. IT tracks critical or high-risk vulnerabilities through resolution.	
		VM-03	Quavo engages a third party to conduct a network and application penetration test of the production environment at least annually. IT team reviews the results and tracks high priority findings to resolution.	



CC5.0 Common Criteria Related to Control Activities				
	Trust Services Criteria	Control #	Controls Specified by Quavo	Test Results
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	AC-06	Internal users are provisioned access to systems based on role as defined in the access matrix. The Director of Technology reviews and approves the access matrix annually. The IT team approves any additional access required outside of the access matrix.	No exceptions noted.
		RA-03	The COO maintains a risk register, which records the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy.	
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	POL-02	Quavo's Information Security Policy outlines roles and responsibilities for personnel with responsibility for the security of the system.	No exceptions noted.
		POL-03	Quavo's Change Management Policy governs the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	



CC5.0 Common Criteria Related to Control Activities			
Trust Services Criteria	Control #	Controls Specified by Quavo	Test Results
CC5.3 The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	ORG-04	Quavo evaluates the performance of internal personnel through a formal, annual performance evaluation.	ORG-04: For 1 of 10 internal personnel selected, an annual performance evaluation was not completed.
	ORG-10	Management publishes the Acceptable Use, Code of Conduct, Data Protection, and Information Security policies to internal personnel. In addition, internal personnel acknowledge these policies within 30 days of hire.	
	POL-01	The COO and CFO are responsible for the design, implementation, and management of the organization's policies and procedures. Policy owners review these policies and procedures at least annually.	
	POL-04	Quavo's security policies (Asset Management, Data Classification, Encryption and Key Management, Incident Response, Password, System Access and Authorization Control, and Vulnerability Management and Patch Program) outline the processes and responsibilities for information security.	
	VM-01	Quavo's Vulnerability Management and Patch Program outlines the procedures to identify, assess, and remediate identified vulnerabilities.	



CC6.0 Common Criteria Related to Logical and Physical Access Controls			
Trust Services Criteria	Control #	Controls Specified by Quavo	Test Results
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	AC-01	Quavo identifies its information assets and maintains an inventory of its system components, owners, and their support of its information assets. IT maintains the list of information assets and inventory at least annually.	No exceptions noted.
	AC-02	Users are assigned unique IDs to access production machines, network devices, and support tools.	
	AC-03	Internal user access to systems and applications with service data requires two-factor authentication in the form of user ID / password, and one-time passcode.	
	AC-04	Quavo has formal policies for password strength and use of authentication mechanisms. These policies require the following: <ul style="list-style-type: none"> ● Minimum length of 8 characters ● Password complexity 	
	AC-06	Internal users are provisioned access to systems based on role as defined in the access matrix. The Director of Technology reviews and approves the access matrix annually. The IT team approves any additional access required outside of the access matrix.	
	AC-07	Upon termination, infrastructure and application access is removed within one business day.	
	AC-09	Service data is encrypted at rest.	
	NET-03	Firewall configurations restrict networking ports and protocols to approved business rules.	



CC6.0 Common Criteria Related to Logical and Physical Access Controls			
Trust Services Criteria	Control #	Controls Specified by Quavo	Test Results
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	AC-06	Internal users are provisioned access to systems based on role as defined in the access matrix. The Director of Technology reviews and approves the access matrix annually. The IT team approves any additional access required outside of the access matrix.	No exceptions noted.
	AC-07	Upon termination, infrastructure and application access is removed within one business day.	
	AC-08	System owners conduct quarterly user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities. Identified access changes are tracked to remediation.	
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	AC-05	Administrative access to production servers and databases is restricted to the Infrastructure and Internal IT Manager, COO, Director of Engineering and Technology, Infrastructure intern, Senior Infrastructure Engineer, and Release Engineer.	No exceptions noted.
	AC-06	Internal users are provisioned access to systems based on role as defined in the access matrix. The Director of Technology reviews and approves the access matrix annually. The IT team approves any additional access required outside of the access matrix.	
	AC-07	Upon termination, infrastructure and application access is removed within one business day.	
	AC-08	System owners conduct quarterly user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities. Identified access changes are tracked to remediation.	



CC6.0 Common Criteria Related to Logical and Physical Access Controls				
Trust Services Criteria		Control #	Controls Specified by Quavo	Test Results
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	N/A	Controls related to this criterion are the responsibility of AWS. See expected controls in the Complementary Subservice Organization Controls section.	Not applicable.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	N/A	Controls related to this criterion are the responsibility of AWS. See expected controls in the Complementary Subservice Organization Controls section.	Not applicable.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	AC-10	Encryption is used to protect the transmission of data over the internet.	No exceptions noted.
		NET-02	Management has implemented intrusion prevention and detection tools to provide monitoring of network traffic to the production environment.	
		NET-03	Firewall configurations restrict networking ports and protocols to approved business rules.	
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes and protects it during transmission, movement, or removal to meet the entity's objectives.	AC-05	Administrative access to production servers and databases is restricted to the Infrastructure and Internal IT Manager, COO, Director of Engineering and Technology, Infrastructure intern, Senior Infrastructure Engineer, and Release Engineer.	No exceptions noted.
		AC-10	Encryption is used to protect the transmission of data over the internet.	
		NET-04	Quavo encrypts hard drives for portable devices with full disk encryption.	



CC6.0 Common Criteria Related to Logical and Physical Access Controls				
Trust Services Criteria		Control #	Controls Specified by Quavo	Test Results
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	CM-01	Quavo uses a tool to enforce standard infrastructure configurations for production servers.	No exceptions noted.
		POL-03	Quavo's Change Management Policy governs the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	
		NET-01	Malware detection software is installed on endpoints that can access the production environment and is configured to perform daily scans.	



CC7.0 Common Criteria Related to System Operations				
Trust Services Criteria		Control #	Controls Specified by Quavo	Test Results
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	CM-01	Quavo uses a tool to enforce standard infrastructure configurations for production servers.	No exceptions noted.
		VM-02	Vulnerability scans are executed monthly on production systems. IT tracks critical or high-risk vulnerabilities through resolution.	
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	NET-02	Management has implemented intrusion prevention and detection tools to provide monitoring of network traffic to the production environment.	No exceptions noted.
		NET-05	The IT team uses logging and monitoring software to collect data from servers and endpoints and detect potential security threats and unusual system activity.	
		NET-06	The IT team uses alerting software to notify impacted teams of potential security events.	
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	COM-04	Quavo has a confidential reporting channel available to internal personnel and external users to report security concerns. Management monitors customer and internal complaints and responds in accordance with the Incident Response Plan.	No exceptions noted.
		IR-02	The IT team tracks identified incidents according to the Incident Response Plan.	
		NET-05	The IT team uses logging and monitoring software to collect data from servers and endpoints and detect potential security threats and unusual system activity.	
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	IR-01	Quavo's Incident Response Plan outlines the process for identifying, prioritizing, communicating, assigning, and tracking incidents through to resolution.	No exceptions noted.
		IR-02	The IT team tracks identified incidents according to the Incident Response Plan.	



CC7.0 Common Criteria Related to System Operations				
	Trust Services Criteria	Control #	Controls Specified by Quavo	Test Results
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	IR-02	The IT team tracks identified incidents according to the Incident Response Plan.	No exceptions noted.
		IR-03	IT creates a 'lessons learned' document after each incident and shares this document with the Engineering team to make any required changes.	



CC8.0 Common Criteria Related to Change Management			
Trust Services Criteria	Control #	Controls Specified by Quavo	Test Results
CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	CM-01	Quavo uses a tool to enforce standard infrastructure configurations for production servers.	No exceptions noted.
	CM-02	System changes are tested via test scripts prior to being deployed into production.	
	CM-03	Code merge requests are independently peer reviewed prior to integrating code changes into the master branch.	
	CM-04	System users who make changes to the development system do not have access to deploy changes to production.	
	CM-05	The production and staging environments are segregated.	
	CM-06	Production data is not used in the development and testing environments.	
	POL-03	Quavo's Change Management Policy governs the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	



CC9.0 Common Criteria Related to Risk Mitigation				
Trust Services Criteria		Control #	Controls Specified by Quavo	Test Results
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from business disruption.	ORG-11	Management has a current insurance policy to help minimize the financial impact of cybersecurity loss events.	No exceptions noted.
		RA-03	The COO maintains a risk register, which records the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy.	
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	RA-04	Quavo's Vendor Risk Management Policy defines a framework for the onboarding and management of the vendor relationship lifecycle. The COO assesses new vendors according to the Vendor Risk Management Policy prior to engaging with the vendor.	No exceptions noted.
		RA-05	The relationship owner collects and reviews the SOC reports (or equivalent) of subservice organizations on an annual basis.	



B. Description of Test of Controls and Results

Test procedures performed in connection with determining the operating effectiveness of controls detailed here in Section IV are described below:

Test Procedure	Description
Inquiry	➤ Inquiry of appropriate personnel and corroboration with management.
Observation	➤ Observation of the application, performance, or existence of the control.
Inspection	➤ Inspection of documents and reports indicating performance of the control.
Reperformance	➤ Reperformance of the control.

In addition, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.



Control #	Controls Specified by Quavo	Tests Performed by Moss Adams LLP	Test Results
AC-01	Quavo identifies its information assets and maintains an inventory of its system components, owners, and their support of its information assets. IT maintains the list of information assets and inventory at least annually.	<p>Inquired of the Senior Infrastructure Engineer to confirm Quavo identified its information assets and maintained an inventory of its system components, owners, and their support of its information assets; and IT maintained the list of information assets and inventory at least annually.</p> <p>Inspected the list of information assets and inventory of system components and owners to ascertain whether Quavo identified information assets and maintained an inventory of its system components during the examination period.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
AC-02	Users are assigned unique IDs to access production machines, network devices, and support tools.	<p>Inquired of the Director of Technology to confirm users were assigned unique IDs to access production machines, network devices, and support tools.</p> <p>Inspected access lists to production systems to ascertain whether users were assigned unique IDs to access production machines, network devices, and support tools.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
AC-03	Internal user access to systems and applications with service data requires two-factor authentication in the form of user ID / password, and one-time passcode.	<p>Inquired of the Senior Infrastructure Engineer to confirm internal user access to systems and applications with service data required two-factor authentication in the form of user ID / password, and one-time passcode.</p> <p>Inspected authentication configurations to ascertain whether internal user access to systems and applications with service data required two-factor authentication in the form of user ID / password, and one-time passcode.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
AC-04	<p>Quavo has formal policies for password strength and use of authentication mechanisms. These policies require the following:</p> <ul style="list-style-type: none"> ● Minimum length of 8 characters ● Password complexity 	<p>Inquired of the Director of Technology to confirm Quavo had formal policies for password strength and use of authentication mechanisms; and these policies required the listed configurations.</p> <p>Inspected the Password Policy to ascertain whether Quavo had formal password policies for password strength and use of authentication mechanisms.</p> <p>Inspected password configurations to ascertain whether passwords met the listed password configurations.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>



Control #	Controls Specified by Quavo	Tests Performed by Moss Adams LLP	Test Results
AC-05	Administrative access to production servers and databases is restricted to the Infrastructure and Internal IT Manager, COO, Director of Engineering and Technology, Infrastructure intern, Senior Infrastructure Engineer, and Release Engineer.	<p>Inquired of the Director of Technology to confirm administrative access to production servers and databases was restricted to the Infrastructure and Internal IT Manager, COO, Director of Engineering and Technology, Infrastructure intern, Senior Infrastructure Engineer, and Release Engineer.</p> <p>Inspected administrative access lists for production servers and databases and an organizational chart to ascertain whether access was restricted to the Infrastructure and Internal IT Manager, COO, Director of Engineering and Technology, Infrastructure intern, Senior Infrastructure Engineer, and Release Engineer.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
AC-06	Internal users are provisioned access to systems based on role as defined in the access matrix. The Director of Technology reviews and approves the access matrix annually. The IT team approves any additional access required outside of the access matrix.	<p>Inquired of the Director of Technology to confirm internal users were provisioned access to systems based on role as defined in the access matrix; the Director of Technology reviewed and approved the access matrix annually; and the IT team approved any additional access required outside of the access matrix.</p> <p>Inspected the Provisioning Matrix and tickets for a sample of new access and additional access requests to ascertain whether internal users were provisioned access to systems based on role as defined in the access matrix; and whether the IT team approved any additional access required outside of the access matrix.</p> <p>Inspected the Provisioning Matrix to ascertain whether the Director of Technology reviewed and approved the access matrix during the examination period.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
AC-07	Upon termination, infrastructure and application access is removed within one business day.	<p>Inquired of the Director of Technology to confirm, upon termination, infrastructure and application access was removed within one business day.</p> <p>Inspected tickets and user access lists for a sample of terminated users to ascertain whether infrastructure and application access for these users was removed within one business day.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>



Control #	Controls Specified by Quavo	Tests Performed by Moss Adams LLP	Test Results
AC-08	System owners conduct quarterly user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities. Identified access changes are tracked to remediation.	<p>Inquired of the Infrastructure and Internal IT Manager to confirm system owners conducted quarterly user access reviews of production servers, databases, and applications to validate internal user access was commensurate with job responsibilities; and identified access changes were tracked to remediation.</p> <p>Inspected access review documentation for a sample of quarters to ascertain whether system owners conducted user access reviews of production servers, databases, and applications for these quarters to validate internal user access was commensurate with job responsibilities.</p> <p>Inspected remediation documentation for identified access changes for a sample of quarters to ascertain whether identified access changes for these quarters were tracked to remediation.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
AC-09	Service data is encrypted at rest.	<p>Inquired of the Senior Infrastructure Engineer to confirm service data was encrypted at rest.</p> <p>Inspected the production database encryption configurations to ascertain whether service data was encrypted at rest.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
AC-10	Encryption is used to protect the transmission of data over the internet.	<p>Inquired of the Senior Infrastructure Engineer to confirm encryption was used to protect the transmission of data over the internet.</p> <p>Inspected website encryption configurations to ascertain whether encryption was used to protect the transmission of data over the internet.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
CM-01	Quavo uses a tool to enforce standard infrastructure configurations for production servers.	<p>Inquired of the Director of Technology to confirm Quavo used a tool to enforce standard infrastructure configurations for production servers.</p> <p>Inspected production image configurations to ascertain whether Quavo used a tool to enforce standard infrastructure configurations for production servers.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>



Control #	Controls Specified by Quavo	Tests Performed by Moss Adams LLP	Test Results
CM-02	System changes are tested via test scripts prior to being deployed into production.	<p>Inquired of the Director of Technology to confirm system changes were tested via test scripts prior to being deployed into production.</p> <p>Inspected tickets for a sample of system changes to ascertain whether these system changes were tested via test scripts prior to being deployed into production.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
CM-03	Code merge requests are independently peer reviewed prior to integrating code changes into the master branch.	<p>Inquired of the Director of Technology to confirm code merge requests were independently peer reviewed prior to integrating code changes into the master branch.</p> <p>Inspected tickets for a sample of code changes to ascertain whether code merge requests were independently peer reviewed prior to integrating these code changes into the master branch.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
CM-04	System users who make changes to the development system do not have access to deploy changes to production.	<p>Inquired of the Director of Technology to confirm system users who made changes to the development system did not have access to deploy changes to production.</p> <p>Inspected the user access list for the deployment tool and the company directory to ascertain whether system users who made changes to the development system did not have access to deploy changes to production without independent approval.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
CM-05	The production and staging environments are segregated.	<p>Inquired of the Director of Technology to confirm the production and staging environments were segregated.</p> <p>Inspected production and staging environment management consoles to ascertain whether the production and staging environments were segregated.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
CM-06	Production data is not used in the development and testing environments.	<p>Inquired of the Director of Technology to confirm production data was not used in the development and testing environments.</p> <p>Inspected the query results for a sample account within the development and production environments to ascertain whether production data was not used in the development and testing environments.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>



Control #	Controls Specified by Quavo	Tests Performed by Moss Adams LLP	Test Results
COM-01	Descriptions of the company's system and its boundaries are available to internal personnel and external users.	<p>Inquired of the Director of Technology to confirm descriptions of the company's system and its boundaries were available to internal personnel and external users.</p> <p>Inspected the company's website to ascertain whether descriptions of the company's system and its boundaries were available to internal personnel and external users.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
COM-02	Quavo publishes its Privacy Statement to internal personnel and external users. This Privacy Statement details the company's security commitments.	<p>Inquired of the Director of Technology to confirm Quavo published its Privacy Statement to internal personnel and external users; and this Privacy Statement detailed the company's security commitments.</p> <p>Inspected the company's website to ascertain whether Quavo published its Privacy Statement to internal personnel and external users.</p> <p>Inspected the Privacy Statement to ascertain whether this Privacy Statement detailed the company's security commitments.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
COM-03	Customers are notified of any system changes impacting the security of the system.	<p>Inquired of the Director of Technology to confirm customers were notified of any system changes impacting the security of the system.</p> <p>Inspected customer notifications for a sample of system changes impacting the security of the system to ascertain whether customers were notified of these system changes.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>



Control #	Controls Specified by Quavo	Tests Performed by Moss Adams LLP	Test Results
COM-04	Quavo has a confidential reporting channel available for internal personnel and a support portal available for external users to report security concerns. Management monitors customer and internal complaints and responds in accordance with the Incident Response Plan.	<p>Inquired of the Director of Technology to confirm Quavo had a confidential reporting channel available for internal personnel and a support portal available for external users to report security concerns; and management monitored customer and internal complaints and responded in accordance with the Incident Response Plan.</p> <p>Inspected Quavo's support page to ascertain whether Quavo had a confidential reporting channel available for internal personnel and a support portal available for external users to report security concerns.</p> <p>Inspected tickets for a sample of customer and internal complaints to ascertain whether management monitored and responded to these complaints in accordance with the Incident Response Plan.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
IR-01	Quavo's Incident Response Plan outlines the process for identifying, prioritizing, communicating, assigning, and tracking incidents through to resolution.	<p>Inquired of the Director of Technology to confirm Quavo's Incident Response Plan outlined the process for identifying, prioritizing, communicating, assigning, and tracking incidents through to resolution.</p> <p>Inspected the Incident Response Plan to ascertain whether Quavo's Incident Response Plan outlined the process for identifying, prioritizing, communicating, assigning, and tracking incidents through to resolution.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
IR-02	The IT team tracks identified incidents according to the Incident Response Plan.	<p>Inquired of the Director of Technology to confirm the IT team tracked identified incidents according to the Incident Response Plan.</p> <p>Inspected tickets for a sample of identified incidents to ascertain whether the IT team tracked these identified incidents according to the Incident Response Plan.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>



Control #	Controls Specified by Quavo	Tests Performed by Moss Adams LLP	Test Results
IR-03	IT creates a 'lessons learned' document after each incident and shares this document with the Engineering team to make any required changes.	<p>Inquired of the Director of Technology to confirm IT created a 'lessons learned' document after each incident and shared this document with the Engineering team to make any required changes.</p> <p>Inspected the lessons learned documentation for a sample of incidents to ascertain whether IT created a 'lessons learned' document after these incidents and shared this document with the Engineering team to make any required changes.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
NET-01	Malware detection software is installed on endpoints that can access the production environment and is configured to perform daily scans.	<p>Inquired of the Director of Technology to confirm malware detection software was installed on endpoints that could access the production environment and was configured to perform daily scans.</p> <p>Inspected the malware detection software console for a sample of user laptops that could access the production environment to ascertain whether malware detection software was installed on these user laptops.</p> <p>Inspected the malware detection software configurations to ascertain whether the software was configured to perform daily scans.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
NET-02	Management has implemented intrusion prevention and detection tools to provide monitoring of network traffic to the production environment.	<p>Inquired of the Director of Technology to confirm management had implemented intrusion prevention and detection tools to provide monitoring of network traffic to the production environment.</p> <p>Inspected intrusion prevention and detection tool configurations to ascertain whether management had implemented intrusion prevention and detection tools to provide monitoring of network traffic to the production environment.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
NET-03	Firewall configurations restrict networking ports and protocols to approved business rules.	<p>Inquired of the Director of Technology to confirm firewall configurations restricted networking ports and protocols to approved business rules.</p> <p>Inspected firewall configurations to ascertain whether firewall configurations restricted networking ports and protocols to approved business rules.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>



Control #	Controls Specified by Quavo	Tests Performed by Moss Adams LLP	Test Results
NET-04	Quavo encrypts hard drives for portable devices with full disk encryption.	<p>Inquired of the Director of Technology to confirm Quavo encrypted hard drives for portable devices with full disk encryption.</p> <p>Inspected encryption configurations for a sample of user laptops to ascertain whether Quavo encrypted the hard drives for these laptops with full disk encryption.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
NET-05	The IT team uses logging and monitoring software to collect data from servers and endpoints and detect potential security threats and unusual system activity.	<p>Inquired of the Director of Technology to confirm the IT team used logging and monitoring software to collect data from servers and endpoints and detect potential security threats and unusual system activity.</p> <p>Inspected monitoring consoles to ascertain whether the IT team used logging and monitoring software to collect data from servers and endpoints and detect potential security threats and unusual system activity.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
NET-06	The IT team uses alerting software to notify impacted teams of potential security events.	<p>Inquired of the Director of Technology to confirm the IT team used alerting software to notify impacted teams of potential security events.</p> <p>Inspected alert configurations to ascertain whether the IT team used alerting software to notify impacted teams of potential security events.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
ORG-01	Quavo has established a Code of Conduct outlining ethical expectations, behavior standards, and ramifications of noncompliance.	<p>Inquired of the Director of Technology to confirm Quavo had established a Code of Conduct outlining ethical expectations, behavior standards, and ramifications of noncompliance.</p> <p>Inspected the Code of Conduct to ascertain whether Quavo had established a Code of Conduct outlining ethical expectations, behavior standards, and ramifications of noncompliance.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>



Control #	Controls Specified by Quavo	Tests Performed by Moss Adams LLP	Test Results
ORG-02	The Board of Directors includes senior management who are independent from the company's operations.	<p>Inquired of the Director of Technology to confirm the Board of Directors included senior management who were independent from the company's operations.</p> <p>Inspected a list of Board members and the organizational chart to ascertain whether the Board of Directors included senior management who were independent from the company's operations.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
ORG-03	Senior management meets with the Board of Directors semi-annually to review business objectives, company initiatives, resource needs, and risk management activities, including results from internal and external assessments.	<p>Inquired of the Director of Technology to confirm senior management met with the Board of Directors semi-annually to review business objectives, company initiatives, resource needs, and risk management activities, including results from internal and external assessments.</p> <p>Inspected meeting notes for the semi-annual meetings to ascertain whether senior management met with the Board of Directors for these semi-annual periods to review business objectives, company initiatives, resource needs, and risk management activities, including results from internal and external assessments.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
ORG-04	Quavo evaluates the performance of internal personnel through a formal, annual performance evaluation.	<p>Inquired of the Director of Technology to confirm Quavo evaluated the performance of internal personnel through a formal, annual performance evaluation.</p> <p>Inspected performance evaluations for a sample of internal personnel to ascertain Quavo evaluated the performance of these internal personnel through a formal performance evaluation completed during the examination period.</p>	<p>No exceptions noted.</p> <p>For 1 of 10 internal personnel selected, an annual performance evaluation was not completed.</p> <p><i>See Section V - Other Information Provided by Quavo That Is Not Covered by the Service Auditor's Report for management response to the noted exception.</i></p>



Control #	Controls Specified by Quavo	Tests Performed by Moss Adams LLP	Test Results
ORG-05	Quavo performs an annual assessment over internal controls used in the achievement of Quavo's service commitments and system requirements. Senior management evaluates the results and resolves any deficiencies in accordance with the Risk Assessment and Management Policy.	<p>Inquired of the Director of Technology to confirm Quavo performed an annual assessment over internal controls used in the achievement of Quavo's service commitments and system requirements; and senior management evaluated the results and resolved any deficiencies in accordance with the Risk Assessment and Management Policy.</p> <p>Inspected the internal control continuous monitoring tool to ascertain whether the tool was configured to perform an assessment over internal controls.</p> <p>Inspected actions taken by senior management to ascertain whether senior management evaluated the results of the continuous monitoring tool and resolved deficiencies in accordance with the Risk Assessment and Management Policy.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
ORG-06	Management maintains a formal organizational chart to clearly identify positions of authority and the lines of communication and publishes the organizational chart to internal personnel.	<p>Inquired of the Director of Technology to confirm management maintained a formal organizational chart to clearly identify positions of authority and the lines of communication and published the organizational chart to internal personnel.</p> <p>Inspected the organizational chart and organizational chart repository to ascertain whether management maintained a formal organizational chart to clearly identify positions of authority and the lines of communication and published the organizational chart to internal personnel.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>



Control #	Controls Specified by Quavo	Tests Performed by Moss Adams LLP	Test Results
ORG-07	Background checks are performed on new hires before the new hire's start date as permitted by local laws.	<p>Inquired of the Director of Technology to confirm background checks were performed on new hires before the new hire's start date as permitted by local laws.</p> <p>Inspected background check results for a sample of new hires to ascertain whether background checks were performed on these new hires before the new hire's start date as permitted by local laws.</p>	<p>No exceptions noted.</p> <p>For 1 of 10 new hires selected, the background check was not completed prior to their start date.</p> <p><i>See Section V - Other Information Provided by Quavo That Is Not Covered by the Service Auditor's Report for management response to the noted exception.</i></p>
ORG-08	Hiring managers screen new hires to assess their qualifications, experience, and competency to fulfill their responsibilities.	<p>Inquired of the Director of Technology to confirm hiring managers screened new hires to assess their qualifications, experience, and competency to fulfill their responsibilities.</p> <p>Inspected interview documentation for a sample of new hires to ascertain whether hiring managers screened these new hires to assess their qualifications, experience, and competency to fulfill their responsibilities.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>



Control #	Controls Specified by Quavo	Tests Performed by Moss Adams LLP	Test Results
ORG-09	Internal personnel complete annual training programs for information security to help them understand their obligations and responsibilities related to security. New hires complete training within 30 days of hire.	<p>Inquired of the Director of Technology to confirm internal personnel completed annual training programs for information security to help them understand their obligations and responsibilities related to security; and new hires completed training within 30 days of hire.</p> <p>Inspected security training materials to ascertain whether training materials included information security topics.</p> <p>Inspected security training records for a sample of internal personnel to ascertain whether these internal personnel completed training programs for information security during the examination period.</p> <p>Inspected security training records for a sample of new hires to ascertain whether these new hires completed training within 30 days of hire.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
ORG-10	Management publishes the Acceptable Use, Code of Conduct, Data Protection, and Information Security policies to internal personnel. In addition, internal personnel acknowledge these policies within 30 days of hire.	<p>Inquired of the Director of Technology to confirm management published the Acceptable Use, Code of Conduct, Data Protection, and Information Security policies to internal personnel; and internal personnel acknowledged these policies within 30 days of hire.</p> <p>Inspected the internal wiki to ascertain whether management published the Acceptable Use, Code of Conduct, Data Protection, and Information Security policies to internal personnel.</p> <p>Inspected the policy acknowledgements for a sample of new hires to ascertain whether these new hires acknowledged these policies within 30 days of hire.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
ORG-11	Management has a current insurance policy to help minimize the financial impact of cybersecurity loss events.	<p>Inquired of the Director of Technology to confirm management had a current insurance policy to help minimize the financial impact of cybersecurity loss events.</p> <p>Inspected the insurance policy to ascertain whether management had a current insurance policy to help minimize the financial impact of cybersecurity loss events.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>



Control #	Controls Specified by Quavo	Tests Performed by Moss Adams LLP	Test Results
POL-01	The COO and CFO are responsible for the design, implementation, and management of the organization's policies and procedures. Policy owners review these policies and procedures at least annually.	<p>Inquired of the Director of Technology to confirm the COO and CFO were responsible for the design, implementation, and management of the organization's policies and procedures; and policy owners reviewed these policies and procedures at least annually.</p> <p>Inspected Quavo's policies to ascertain whether the COO and CFO were responsible for the design, implementation, and management of the organization's policies and procedures.</p> <p>Inspected the policy approval timestamps for Quavo's policies to ascertain whether the policy owners reviewed the policies and procedures during the examination period.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
POL-02	Quavo's Information Security Policy outlines roles and responsibilities for personnel with responsibility for the security of the system.	<p>Inquired of the Director of Technology to confirm Quavo's Information Security Policy outlined roles and responsibilities for personnel with responsibility for the security of the system.</p> <p>Inspected the Information Security Policy to ascertain whether Quavo's Information Security Policy outlined roles and responsibilities for personnel with responsibility for the security of the system.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
POL-03	Quavo's Change Management Policy governs the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	<p>Inquired of the Director of Technology to confirm Quavo's Change Management Policy governed the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.</p> <p>Inspected the Change Management Policy to ascertain whether Quavo's Change Management Policy governed the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>



Control #	Controls Specified by Quavo	Tests Performed by Moss Adams LLP	Test Results
POL-04	Quavo's security policies (Asset Management, Data Classification, Encryption and Key Management, Incident Response, Password, System Access and Authorization Control, and Vulnerability Management and Patch Program) outline the processes and responsibilities for information security.	<p>Inquired of the Director of Technology to confirm Quavo's security policies (Asset Management, Data Classification, Encryption and Key Management, Incident Response, Password, System Access and Authorization Control, and Vulnerability Management and Patch Program) outlined the processes and responsibilities for information security.</p> <p>Inspected the security policies to ascertain whether the policies outlined the processes and responsibilities for information security.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
RA-01	Management performs a formal review of the Risk Assessment and Management Program at least annually. Risk tolerance and strategies are defined in the policy.	<p>Inquired of the Director of Technology to confirm management performed a formal review of the Risk Assessment and Management Program at least annually; and risk tolerance and strategies were defined in the policy.</p> <p>Inspected the Risk Assessment and Management Program timestamp and approval to ascertain whether management performed a formal review of the Risk Assessment and Management Program during the examination period.</p> <p>Inspected the Risk Assessment and Management Program to ascertain whether risk tolerance and strategies were defined in this policy.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
RA-02	The COO performs an annual formal risk assessment, which includes the identification of relevant internal and external threats related to security and fraud, and an analysis of risks associated with those threats.	<p>Inquired of the Director of Technology to confirm the COO performed an annual formal risk assessment, which included the identification of relevant internal and external threats related to security and fraud, and an analysis of risks associated with those threats.</p> <p>Inspected the most recent risk assessment to ascertain whether the COO performed a formal risk assessment during the examination period, which included the identification of relevant internal and external threats related to security and fraud, and an analysis of risks associated with those threats.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>



Control #	Controls Specified by Quavo	Tests Performed by Moss Adams LLP	Test Results
RA-03	The COO maintains a risk register, which records the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy.	<p>Inquired of the Director of Technology to confirm the COO maintained a risk register, which recorded the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy.</p> <p>Inspected the risk register to ascertain whether the COO maintained a risk register, which recorded the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
RA-04	Quavo's Vendor Risk Management Policy defines a framework for the onboarding and management of the vendor relationship lifecycle. The COO assesses new vendors according to the Vendor Risk Management Policy prior to engaging with the vendor.	<p>Inquired of the Director of Technology to confirm Quavo's Vendor Risk Management Policy defined a framework for the onboarding and management of the vendor relationship lifecycle; and the COO assessed new vendors according to the Vendor Risk Management Policy prior to engaging with the vendor.</p> <p>Inspected the Vendor Risk Management Policy to ascertain whether Quavo's Vendor Risk Management Policy defined a framework for the onboarding and management of the vendor relationship lifecycle.</p> <p>Inspected the assessments for a sample of new vendors to ascertain whether the COO assessed these new vendors according to the Vendor Risk Management Policy prior to engaging with the vendor.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
RA-05	The relationship owner collects and reviews the SOC reports (or equivalent) of subservice organizations on an annual basis.	<p>Inquired of the Director of Technology to confirm the relationship owner collected and reviewed the SOC reports (or equivalent) of subservice organizations on an annual basis.</p> <p>Inspected the SOC report reviews for the population of subservice organizations to ascertain whether the relationship owner collected and reviewed the SOC reports (or equivalent) for these subservice organizations during the examination period.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>



Control #	Controls Specified by Quavo	Tests Performed by Moss Adams LLP	Test Results
VM-01	Quavo's Vulnerability Management and Patch Program outlines the procedures to identify, assess, and remediate identified vulnerabilities.	<p>Inquired of the Director of Technology to confirm Quavo's Vulnerability Management and Patch Program outlined the procedures to identify, assess, and remediate identified vulnerabilities.</p> <p>Inspected the Vulnerability Management and Patch Program to ascertain whether Quavo's Vulnerability Management and Patch Program outlined the procedures to identify, assess, and remediate identified vulnerabilities.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
VM-02	Vulnerability scans are executed monthly on production systems. IT tracks critical or high-risk vulnerabilities through resolution.	<p>Inquired of the Director of Technology to confirm vulnerability scans were executed monthly on production systems; and IT tracked critical or high-risk vulnerabilities through resolution.</p> <p>Inspected the vulnerability scans for a sample of months to ascertain whether vulnerability scans were executed for these months on production systems.</p> <p>Inspected the resolution log for a sample of critical or high-risk vulnerabilities identified within the vulnerability scans inspected to ascertain whether the IT team tracked these vulnerabilities to resolution.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>



Control #	Controls Specified by Quavo	Tests Performed by Moss Adams LLP	Test Results
VM-03	<p>Quavo engages a third party to conduct a network and application penetration test of the production environment at least annually. IT team reviews the results and tracks high priority findings to resolution.</p>	<p>Inquired of the Director of Technology to confirm Quavo engaged a third party to conduct a network and application penetration test of the production environment at least annually; and the IT team reviewed the results and tracked high priority findings to resolution.</p> <p>Inspected the most recent penetration test report to ascertain whether Quavo engaged a third party to conduct a network and application penetration test of the production environment during the examination period.</p> <p>Inspected tickets for a sample of high-risk findings identified within the penetration test report to ascertain whether the IT team reviewed the penetration test results and tracked these findings to resolution.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>The circumstances that warrant the operation of this control attribute did not occur as there were no high priority findings identified in the penetration test completed during the examination period; therefore, no testing was performed.</p>



V. Other Information Provided by Quavo That Is Not Covered by the Service Auditor's Report

The following information is provided for informational purposes only and has not been subjected to the procedures applied in the examination. Accordingly, Moss Adams expresses no opinion on the following information.

A. Management's Response to Identified Testing Exceptions

Control #	Controls Specified by Quavo	Exception Noted by Moss Adams LLP	Quavo Management Response
ORG-04	Quavo evaluates the performance of internal personnel through a formal, annual performance evaluation.	For 1 of 10 internal personnel selected, an annual performance evaluation was not completed.	As a rapidly growing organization, Quavo has continually changed to keep pace with our growth. We acknowledge that because of this organizational fluidity, we were unable to demonstrate 100% compliance with the completion of performance reviews for our team during the previous review period. Quavo recognized the need to continue to strengthen, develop, and mature our processes to achieve our goals. Earlier this year, we invested in a new leadership position, the VP of People, who is focused upon improving and maturing our people processes and practices and infusing accountability across our organization. We are confident that we will continue to demonstrate improvement.
ORG-07	Background checks are performed on new hires before the new hire's start date as permitted by local laws.	For 1 of 10 new hires selected, the background check was not completed prior to their start date.	As a rapidly growing organization, Quavo has continually changed to keep pace with our growth. We acknowledge that because of this organizational fluidity, we were unable to demonstrate 100% compliance with the completion of performance reviews for our team during the previous review period. Quavo recognized the need to continue to strengthen, develop, and mature our processes to achieve our goals. Earlier this year, we invested in a new leadership position, the VP of People, who is focused upon improving and maturing our people processes and practices and infusing accountability across our organization. We are confident that we will continue to demonstrate improvement.

