PRESCIENT
ASSURANCE

November 21, 2024

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

In connection with your engagement to report on Mobly, Inc's (service organization) description of its Mobly system titled Mobly System Description throughout the period January 1, 2024 to October 1, 2024 (description) based on the criteria set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (description criteria) and the suitability of the design and operating effectiveness of the controls included in the description throughout the period January 1, 2024 to October 1, 2024 to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the trust services criteria relevant to "Security" set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria), we recognize that obtaining representations from us concerning the information contained in this letter is a significant procedure in enabling you to form an opinion about whether the description presents the system that was designed and implemented throughout the period observation period in accordance with the description criteria and whether the controls stated in the description were suitably designed and operating effectively throughout the period January 1, 2024 to October 1, 2024 to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

We confirm, to the best of our knowledge and belief, as of November 21, 2024, the date of your report, the following representations made to you during your examination:

1) We are responsible for the preparation and presentation of the description, including the completeness, accuracy, and method of presentation of the description, in accordance with the description criteria and the suitability of the design and operating effectiveness of the controls included in the description to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

2) We also are responsible for our written assertion that accompanies the description of the system, both of which will be provided to you and users of the report. We are responsible for the completeness, accuracy, and method of presentation of the assertion and for having a reasonable basis for it. We reaffirm our assertion attached to the description.

3) We have evaluated the presentation of the description in accordance with the description criteria and the suitability of the design and operating effectiveness of the controls stated therein to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, and all relevant matters have been considered and reflected in our evaluation and in our assertion.

4) We have disclosed to you all known matters that may contradict the presentation of the description or the suitability of the design of the controls stated in the description, or our assertion.

5) We have disclosed to you any communications from regulatory agencies, user entities, or others received through the date of this letter affecting the presentation of the description or the suitability of the design or operating effectiveness of the controls included in the description.

6) We are responsible for determining the scope of your examination, including identifying the time period covered by the engagement, services that are the subject of the examination, the system providing the services (including boundaries of the system), and risks relevant to business partners who provide intellectual property or services related to the system.

7) We are responsible for selecting the trust services category(ies) and criteria to be included within the scope of our examination and determining that they are appropriate for our purposes. We are responsible for stating the applicable trust services criteria and related controls in the description. For any additional criteria specified by law, regulation, or another party, we are responsible for identifying that party in the description.

8) We are responsible for determining the effect on our service commitments and system requirements of any services provided to the service organization by other organizations and determining whether those entities are subservice organizations. We are also responsible for determining whether we will use the carve-out method or inclusive method to present information about services provided at any subservice organizations in our description.

9) We are responsible for identifying and analyzing the risks that threaten the achievement of our service commitments and system requirements based on the applicable trust services criteria.

10) We are responsible for designing, implementing, and documenting controls that are suitably designed and operating effectively to provide reasonable assurance that our service commitments and system requirements are achieved based on the applicable trust services criteria.

11) We are responsible for specifying the principal service commitments made to user entities and the system requirements necessary to operate the system and meet commitments to our business partners.

12) We have provided you with the following:

    a) All relevant information and access, as agreed upon in the terms of the engagement, to all information such as records, documentation, service-level agreements, and internal audit or other reports, of which we are aware that is relevant to your examination and our assertion.

    b) Access to additional information you have requested from us for the purpose of the engagement.

    c) Unrestricted access to persons within the appropriate parties from whom you determined was necessary to obtain evidence relevant to your engagement.

13) We believe the effects of uncorrected misstatements (such as discrepancies in the description or deficiencies in the controls described), if any, are immaterial, individually and in the aggregate, to the presentation of the description in accordance with the description criteria or to the suitability of the design or operating effectiveness of the controls stated therein to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

14) We have disclosed to you any known events subsequent to the period covered by the description of the system up to the date of this letter that would have a material effect on the presentation of the description or the suitability of the design or operating effectiveness of the controls, or our assertion.

15) We have disclosed to you any instances of noncompliance with laws and regulations, fraud, or uncorrected misstatements attributable to the service organization that are not clearly trivial and that may affect one or more user entities, and whether such incidents have been communicated appropriately to affected user entities.

16) We have disclosed to you any actual, suspected, or alleged fraud or noncompliance with laws or regulations that could adversely affect the description of the service organization’s system, the suitability of the design of the controls stated therein, or achievement of its service commitments and system requirements.

17) We also have disclosed to you all instances about which we are aware of the following:

    a) Misstatements and omissions in the description.

    b) Instances in which controls have not been suitably designed or implemented as described.

    c) Instances in which controls did not operate effectively or as described.

18) We have disclosed to you all identified system incidents that resulted in a significant impairment of the service organization's achievement of its service commitments and system requirements throughout the period January 1, 2024 to October 1, 2024.

19) We have disclosed to you any changes in the controls that are likely to be relevant to report users occurring through the date of this letter.

20) We have disclosed to you the effects of the COVID-19 pandemic on Mobly, Inc, its operations, and technologies used in providing services.

21) We have disclosed to you any communications to customers and business partners about changes in our service level agreements or commitments as a result of the COVID-19 pandemic.

22) We have responded fully to all inquiries made to us by you during the examination.

23) We understand that your report is intended solely for the use and information of management of the service organization and others within the organization, user entities to which we provide services, and other specified parties who have sufficient knowledge and understanding to consider it, along with other information, if any. We intend to distribute your report only to those specified parties.

We understand that your examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and was designed for the purpose of expressing an opinion about whether, in all material respects, the description is presented in accordance with the description criteria and whether the controls stated therein were suitably designed and operating 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 also understand that the opinion was based on your examination and that the procedures performed in the examination were limited to those that you considered necessary.

Signed by:
Zach Barney
C5DDE2E58C6741A...

Name

CEO

Title

mobly

SOC 2 Type 2 Report

Mobly, Inc

January 1, 2024 to October 1, 2024

A Type 2 Independent Service Auditor’s Report on Controls Relevant to Security

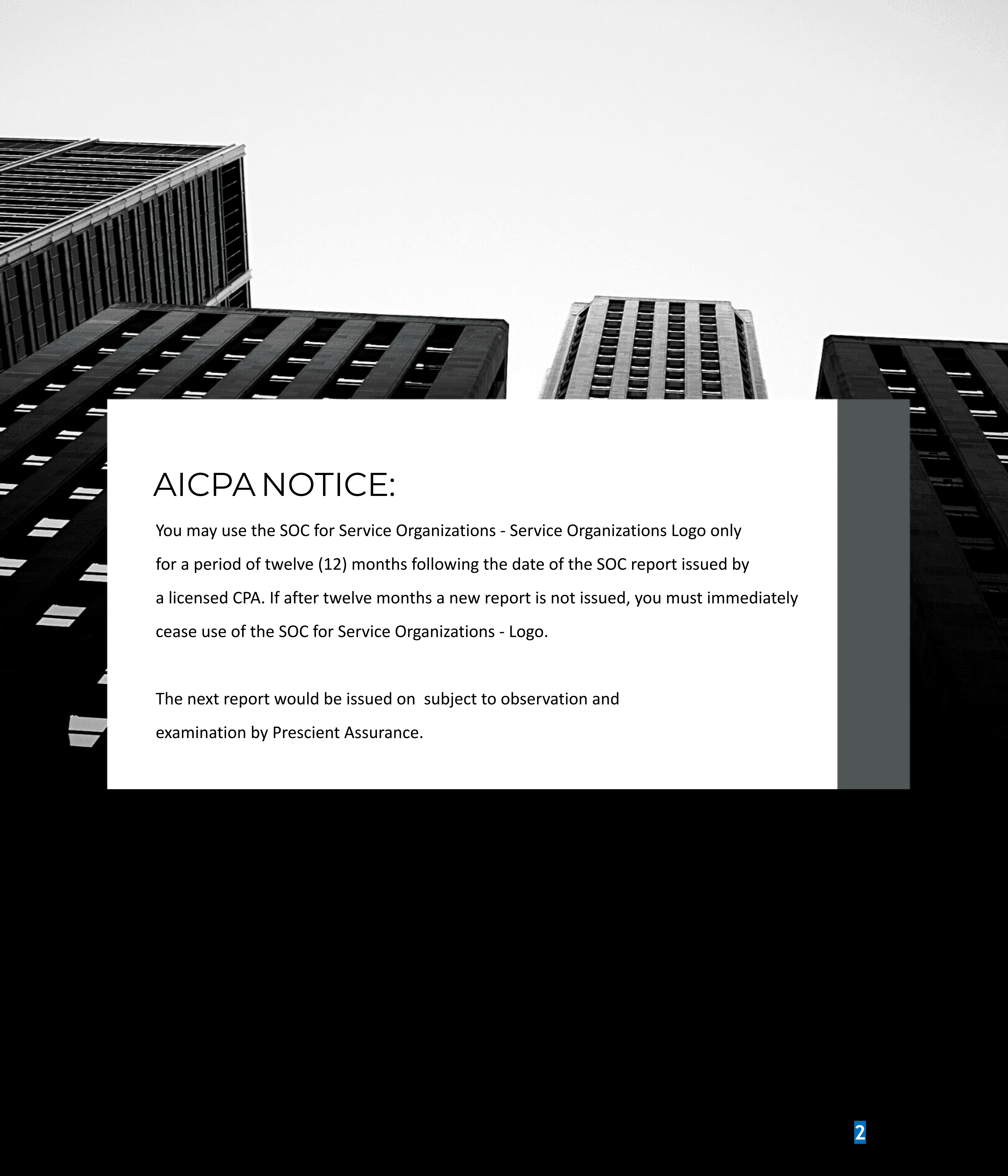
AUDIT AND ATTESTATION BY

PRESCIENT
ASSURANCE

CPA

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

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

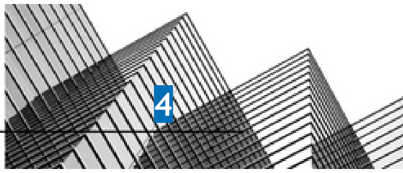


AICPA NOTICE:

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

The next report would be issued on subject to observation and examination by Prescient Assurance.

Table of Contents



SECTION 1

Management's Assertion

Management Assertion

We have prepared the accompanying description of Mobly, Inc's system throughout the period January 1, 2024 to October 1, 2024, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report. The description is intended to provide report users with information about Mobly, Inc's system that may be useful when assessing the risks arising from interactions with Mobly, Inc's system, particularly information about system controls that Mobly, Inc 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 set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

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

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

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

a. The description presents Mobly, Inc's system that was designed and implemented throughout the period January 1, 2024 to October 1, 2024 in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period January 1, 2024 to October 1, 2024, to provide reasonable assurance that Mobly, Inc's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Mobly, Inc's controls during that period.

c. The controls stated in the description operated effectively throughout the period January 1, 2024, to October 1, 2024, to provide reasonable assurance that Mobly, Inc's service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization and complementary user entity controls assumed in the design of Mobly, Inc's controls operated effectively throughout the period.

Signed by:

Zach Barney

C5DDE2E58C6741A...

Zach Barney

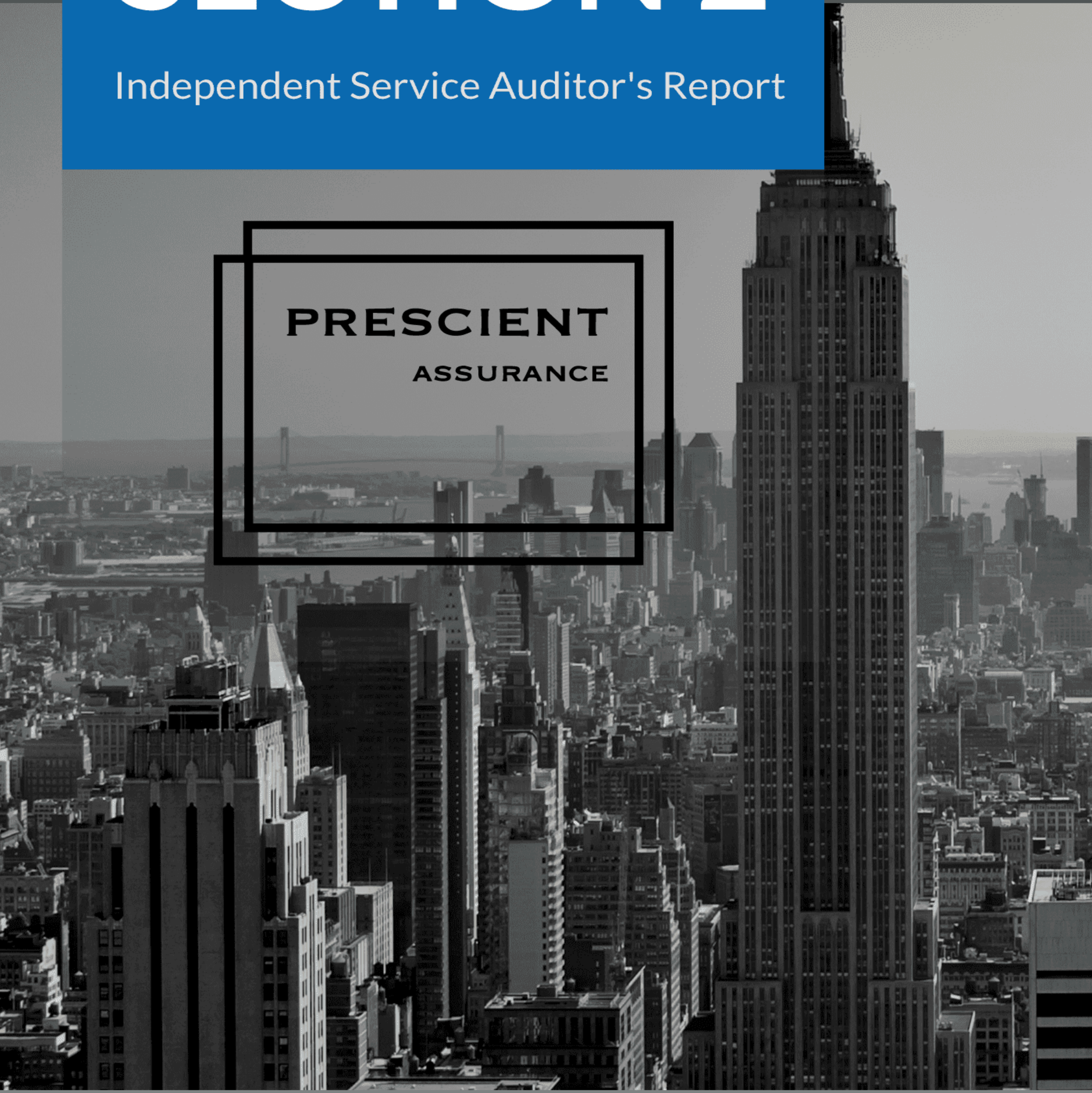
CEO

Mobly, Inc

SECTION 2

Independent Service Auditor's Report

PRESCIENT ASSURANCE



Independent Service Auditor's Report

To: Mobly, Inc

Scope

We have examined Mobly, Inc's ("Mobly, Inc") accompanying description of its Mobly system found in Section 3, titled Mobly, Inc System Description throughout the period January 1, 2024, to October 1, 2024, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report, and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2024, to October 1, 2024, to provide reasonable assurance that Mobly, Inc's service commitments and system requirements were achieved based on the trust services criteria relevant to Security set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

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

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

Service Organization's Responsibilities

Mobly, Inc 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 Mobly, Inc's service commitments and system requirements were achieved. In Section 1, Mobly, Inc has provided the accompanying assertion titled "Management's Assertion of Mobly, Inc" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. Mobly, Inc 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 Auditors' Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operating 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:

1. Obtaining an understanding of the system and the service organization's service commitments and system requirements.
2. 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.
3. Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
4. Performing procedures to obtain evidence about whether 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.
5. Testing the operating effectiveness of 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.
6. 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 examination 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 report users may consider important to meet their informational needs. There are inherent limitations in 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 or 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.

Opinion

In our opinion, in all material respects:

a. The description presents Mobly, Inc's system that was designed and implemented throughout the period January 1, 2024, to October 1, 2024, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period January 1, 2024, to October 1, 2024, to provide reasonable assurance that Mobly, Inc's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period and if the subservice organization and user entities applied the complementary controls assumed in the design of Mobly, Inc's controls throughout the period.
c. The controls stated in the description operated effectively throughout the period January 1, 2024, to October 1, 2024, to provide reasonable assurance that Mobly, Inc'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 Mobly, Inc's controls operated effectively throughout the period.

Restricted Use

This report is intended solely for the information and use of Mobly, Inc, user entities of Mobly, Inc's system during some or all of the period January 1, 2024 to October 1, 2024, business partners of Mobly, Inc subject to risks arising from interactions with the system, 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:

1. The nature of the service provided by the service organization.
2. How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
3. Internal control and its limitations.
4. 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.
5. User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
6. The applicable trust services criteria.
7. 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.

DocuSigned by:

Prescient Assurance

66274D51A66C4C8

Prescient Assurance LLC

November 21, 2024

SECTION 3

System Description

DC 1: Company Overview and Types of Products and Services Provided

Company Overview

Mobly, INC (the “company” or “Mobly”) was founded in 2023 and is headquartered in Lehi, Utah with personnel working remote and from the main office location. Mobly provides Speedy and Accurate Lead Capture services to people in Field Sales and Field Marketing.

Description of Services Provided

Mobly’s core product in-scope is the Mobly Platform (the “system”) that provides:

- Event Agnostic Badge Scanning and Lead Capture

Users can go to an event and use the Mobly Mobile Application scan a badge, provide context about the conversation that just occurred and then send that information to their CRM

Data Enrichment

- Mobly takes the data from the events and uses publicly available information to find contact and occupation information for that lead.

DC 2: The Principal Service Commitments and System Requirements

Mobly designs its processes and procedures related to the Mobly Platform to meet its objectives for providing field marketing and sales services. Those objectives are based on the service commitments that Mobly makes to user entities, the laws and regulations that govern services, and the financial, operational, and compliance requirements that Mobly has established for the services.

Terms and conditions are presented to provide a mechanism for communicating the terms of service within the company and between the company, customers, and website users. The terms and conditions outline terms for services, use of services, enforcement, intellectual property rights, and warranties. Terms of service documents can be found at https://www.getmobly.com/main-services-agreement and the service-level agreement (SLA) is available upon request at support@getmobly.com.

The terms of service are reviewed at least annually or more frequently when deemed necessary. Any changes are reviewed by management and sent to the marketing team for execution of the changes. Customers are notified via e-mail of any changes. The customer is not required to accept or agree to any change.

Security commitments to user entities are documented and communicated in SLAs and other customer agreements, as well as in the description of the service offering provided online.

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

- System features and configuration settings designed to authorize user access while restricting unauthorized users;
- Use of security monitoring to detect and prevent potential security attacks from users outside the boundaries of the system;
- Weekly vulnerability scans on externally facing endpoints, and annual penetration tests over the production environment; and,
- Operational procedures for managing security incidents and breaches, including notification procedures.

Such requirements are communicated in Mobly's system policies and procedures, system design documentation, and agreements with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired, trained and managed. In addition to these policies, standard operating procedures are documented on how to carry out specific manual and automated processes required in the operation and development of the services.

In accordance with our assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

DC 3: The Components of the System Used to Provide the Services

The Mobly Platform has been designed, implemented, and is operated to achieve specific business objectives in accordance with management-specified requirements to meet our customers needs. The purpose of the system description is to delineate the boundaries of the system, which includes the services and commitments outlined above and the five components described below: infrastructure, software, people, procedures and data.

3.1 Primary Infrastructure

The system is hosted at Google Cloud Provider (GCP) within a virtual private cloud (VPC) environment and behind a perimeter security firewall which protects the network from unauthorized external access. The network topology includes public and private subnets with access control lists (ACLs). Compute and data storage resources are protected by Google Load Balancers, and industry standard security and programming standards and checks. Mobly uses Google Load Balancers and Google Threat Detection platform, among others to identify and protect against threats.

The underlying physical infrastructure is hosted, managed and protected by GCP. Production resources for compute, storage, networking and virtualization maintain high availability and failover support within GCP.

User requests to the Mobly Web Portal are encrypted with a secure version of Transport Layer Security (TLS) by using certificates from an established third party certificate authority. Remote access by developers and administrators is limited and requires multi-factor authentication.

3.2 Primary Software

Mobly is responsible for managing the development and operation of the Mobly Platform including infrastructure resources such as compute, storage, networking and virtualization. The in-scope Mobly Platform infrastructure and software components are shown in the table below:

Primary Infrastructure and Software		
System/Application	**Business/Function**	**Description**
Mobly Platform Web-based Platform	Main product provided by Mobly.	Provides access to the Mobly Platform through a web interface and user authentication
Google Cloud Armor	Perimeter Security Firewall	Defends our platform at the network border from unauthorized access and external attacks (e.g., DDoS).

Primary Infrastructure and Software

System/Application	Business/Function	Description
Google Compute Engine built-in Firewalls	Host-based Firewalls	Used to setup access rules at the resource/instance level
Google Cloud VPC	Public and Private Network Segmentation	Defines and enforces isolation between public and private network areas in our cloud environment.
Google Cloud VPC	Network ACLs/Subnets (network segmentation)	Used to allow or deny specific inbound or outbound traffic at the subnet level within VPCs (virtual private cloud)
Google Firebase	Content delivery network (CDN)	Used to distribute static and dynamic content quickly and reliably with high speed to our user interface application
Google Cloud DNS	Highly available and scalable cloud Domain Name System (DNS) web service	Used to connect user requests to our web-based platform
Google Cloud Load Balancing	Automatically distributes incoming network and application traffic	Used to increase availability and fault tolerance for our user interface application
Google Kubernetes Engine (GKE)	Fully managed container orchestration service	Used with EC2 instances and Docker images to easily build, run, test, deploy, manage, and scale our code
Google Cloud SQL - PostgreSQL	Fully managed, open-source cloud relational database service	Used to securely store configuration data for our customers individual accounts
Google Cloud Storage	Highly available and scalable object storage solution	Google Cloud Storage is controlled through the GCP IAM interface and securely stores machine language models
Google Filestore	Simple, scalable fully managed elastic NFS file system	Used to securely store files for our customers individual accounts

Primary Infrastructure and Software

System/Application	Business/Function	Description
Google Cloud Key Management Service	Provision, manage, and deploy public and private SSL/TLS certificates	Used to create, store, and renew our public SSL/TLS certificates to protect customer data in transit
SendGrid	Email Communication	Used to sent email updates and alerts to customers
Google Cloud Identity & Access Management	Web service to securely control access to AWS resources	Used to ensure segregation of duties and role-based access control (RBAC) for our internal engineering team
Google Identity Platform	Identity platform for web and mobile applications	Used as an authorization service for OAuth 2.0 access tokens, by using OpenID Connect, to provide single-sign on (SSO) for our customers using their identity providers (IdP) (e.g., Google, Microsoft)
GitHub	Build, release, and continuous integration systems	Source code repositories, version control systems, code reviews, and build software are hosted by GitHub.

Supporting Tools

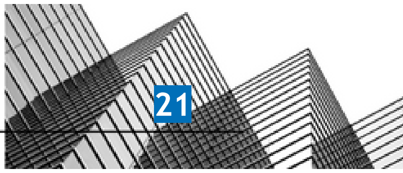
System/Application	Business/Function	Description
TriNet	HRIS (Human Resource Information/Management System) & Performance Evaluation	The centralized system used for managing HR processes, including payroll, benefits, performance evaluations, and employee data
TriNet and Google Docs	Modern ATS (Applicant Tracking System) and Collaborative Recruitment Software	Used for streamlining recruitment, from posting jobs to hiring, essential for maintaining data on recruitment processes

Supporting Tools		
System/Application	**Business/Function**	**Description**
Checkr	Employee Background Screening	Used for verifying candidate backgrounds, including criminal records and employment history
TriNet	Employee Performance Evaluations	Used for documenting and assessing employee performance
Home Grown, TriNet monitoring and Quarterly REviews	Web-based Security Awareness & Training Platform	Used for educating employees on SOC 2 compliance and information security, necessary for mitigating risks and ensuring adherence to security policies and regulations
Miradore	Mobile Device Management (MDM) Solution	Used to enforce encryption, malware protection, security updates, and enable remote wipe capabilities on all company-owned laptops
Google Cloud Suite	Collection of Cloud Productivity and Collaboration Tools	Central platform used for emails, document creation, collaboration, and productivity
Google Cloud Suite, and Slack	Cloud-based Team Communication Platform	Used for real-time messaging and monitoring alerts from automated scanning technologies (e.g., vulnerabilities, application errors and crashes, security events)
Google Drive	Web-based Corporate Wiki	Platform used for internal knowledge sharing and documentation (e.g., posting policies, plans and procedures)
SalesForce	Fully Integrated CRM Solution	Used by our customer success team for managing customer inquiries and support tickets, and provide knowledge base articles

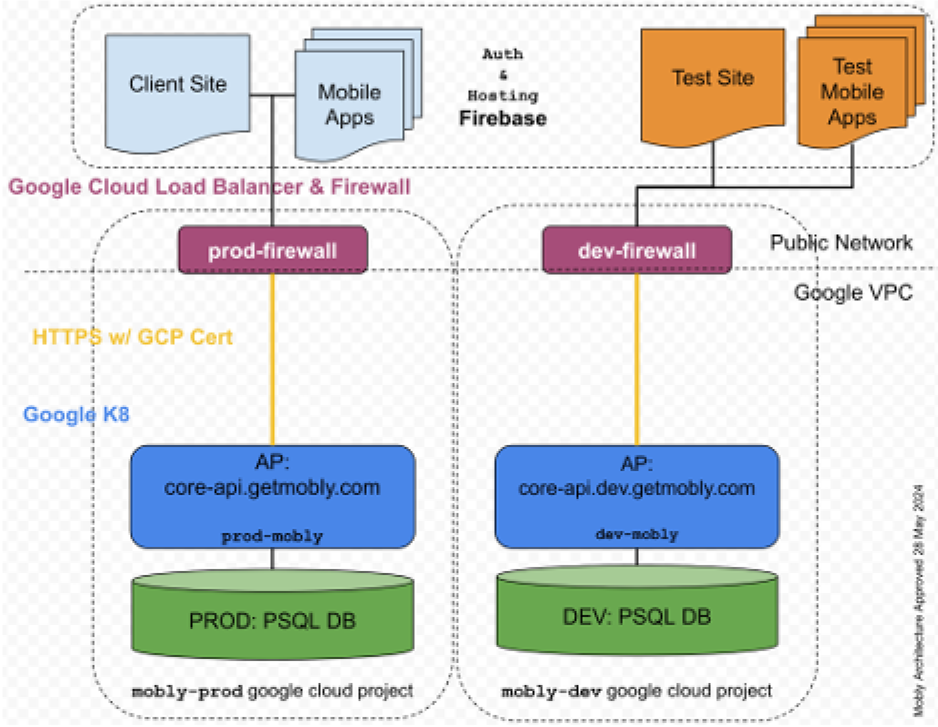
Supporting Tools		
System/Application	**Business/Function**	**Description**
Trello, Jira and GitHub	Software Development Tool and Project Work Management	Used for tracking internal tasks and projects from submission to completion (software development, change management, business projects, access requests and removals)
Google Clouds Operation Suite (formerly Stackdriver)	Modern Application Performance Monitoring (APM)	Used to continuously monitor for errors and crashes at the application layer across web and backend applications, to detect and resolve root causes faster, and avoid system downtime
Google Cloud Security And Command Center.	Automated Vulnerability Management Service	Used to continuously scan (minimum: weekly) our GCP workloads for software vulnerabilities and unintended network exposure
Event Threat Detection (Security Command Center Premium Tier)	Intelligent Threat Detection Services	Used to monitor our GCP accounts, workloads and data to identify malicious activity and anomalous behavior, and if threat is detected sends an alert to Slack
Google Clouds Operations Suite (formerly Stackdriver)	Records events taken by a user, role or an GCP service	Events are filtered and set to trigger an alert when an event occurs for areas that are known targets or indicate potential individual with malicious intent has unauthorized access
Google Clouds Operations Suite (formerly Stackdriver)	Performance Monitoring Tool	Used to collect and track preset metrics, to measure resources and applications
Google Cloud Build, YAML files, and scripts	Infrastructure as Code (IaC) provisioning tool	Used to model, provision and manage GCP resources, with templates and stacks

Supporting Tools

System/Application	Business/Function	Description
Google Cloud Security And Command Center	Cloud security posture management (CSPM) service	Use to proactively monitor GCP resources to identify misconfigurations and prioritizes finding based on severity level
GitHub Dependabot, and Google Vulnerability Scanning	Automated dependency updates built into GitHub	Used to generate alerts when repository is using software dependency with a known vulnerability
GitHub SAST Tooling	Open source security static analysis tool (SAST)	Used to find bugs and detect vulnerabilities, prior to each pull requests (PRs) being merged
Google Cloud and Slack	Modern incident management for operating always-on services	Used by on-call engineers to build and modify schedules, and respond promptly to critical issues to avoid system downtime
Slack and Email	Proactive customer communication piece of incident management	Used to proactively communicate system operational status (uptime and downtime)



Overall Technical Diagram


Client Site
Mobile Apps
Auth & Hosting
Firebase
Test Site
Test Mobile Apps
Google Cloud Load Balancer & Firewall
prod-firewall
dev-firewall
Public Network
Google VPC
HTTPS w/ GCP Cert
Google K8
AP: core-api.getmobly.com
prod-mobly
AP: core-api.dev.getmobly.com
dev-mobly
PROD: PSQL DB
DEV: PSQL DB
mobly-prod google cloud project
mobly-dev google cloud project
Mobly Architecture Approved 28 May 2024

3.3 People

Mobly has established an organizational structure that includes consideration of key areas of authority and responsibility, as well as appropriate lines of reporting:

- **Executive Management:** Consists of the management committee, as outlined within the Mobly security committee charter, and is responsible for overseeing company wide activities, establishing and accomplishing goals, and overseeing objectives.
- **GRC (Governance, Risk, and Compliance):** Responsible for information security oversight and policies, annual risk assessments, third party/vendor risk management, and compliance, etc.
- **Product:** Responsible for the product life cycle, including adding additional product features and functionality, and overseeing change management.
- **Engineering:** Responsible for the development, testing, deployment, and maintenance of the source code for the system.
- **Security Operations:** Responsible for maintaining production infrastructure, managing access and security for production infrastructure and incident response. Members of the security operations team may also be members of the engineering team.
- **IT:** Responsible for access controls and security of the production environment, managing laptops, software, and other technology involved in employee productivity and business operations.
- **Sales, Marketing and Customer Success Operations:** Responsible for sales, marketing, account management, and customer success teams and activities.

3.4 Data

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. This data is managed and stored in a range of database technologies.

Data Classification		
Data Sensitivity	**Description**	**Example**
Public	Information intended or required for public release. Disclosure of such information does not adversely impact Mobly's business operations, financial wellbeing, or image and reputation.	● Published website content ● Press releases
Sensitive	Sensitive data that requires additional levels of protection.	● Operational information ● Personnel records ● Information security procedures ● Research ● Internal communications\ ● Log records (firewall logs, audit trails, etc.)
Confidential	Sensitive data that must be protected from unauthorized disclosure or public release based on state or federal law, and other constitutional, statutory, judicial, and legal agreements.	● Personally identifiable information (PII), such as name Social Security Number (SSN) and/or financial account numbers ● Employment Records ● Intellectual property, such as: copyrights, patents, and trade secrets ● Client/Customer data

Processes and Procedures

Formal IT security policies and procedures exist that describe incident response, network security, encryption, and system security standards. All teams are expected to adhere to Mobly policies and procedures that define how services should be delivered. These are located on Mobly's internal designated Share Google Drive page and are accessible to all Mobly personnel.

Mobly has the following information security policies in place with corresponding documented information security operational activities, which are owned by the acting CISO:

- Asset Management
- Business Continuity
- Change and Release Management
- Human Resources Security
- Identity and Access Management
- Incident and Event Management
- Information Protection (Data Classification)
- Information Security
- Legal and Compliance
- Risk Assessment and Management
- Secure Configuration
- Software Development Lifecycle
- Supplier Relationships Security
- System and Network Security
- Threat and Vulnerability Management

Policies are reviewed on an annual basis and changes are made to the policies when necessary. Members of the management team are authorized to perform reviews of policies with final approval for changes from the acting CISO in conjunction with other senior management. Approvals are documented and tracked as they occur. Any changes to the policies are then communicated to employees via e-mail and are posted on Mobly's internal designated Google Shared Drive accessible to all employees.

DC 4: Disclosures about Identified Security Incidents

There were no system incidents during the period of time covered by the description, requiring disclosure that either:

- Were the result of controls failing due to not being suitably designed or operating effectively; or,
- Otherwise resulted in a significant failure in the achievement of one or more of the service commitments and system requirements.

Disclosure of Incidents

There were no system incidents during the period from 1 January 2024 - 1 October 2024, requiring disclosure that either:

- Were the result of controls failing; or,
- Resulted in a significant impairment to the achievement of systems requirements or service commitments to customers.

DC 5: The Applicable Trust Services Criteria and the Related Controls Designed to Provide Reasonable Assurance that the Service Organization's Service Commitments and System Requirements were Achieved

The applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Although the applicable trust services criteria and related controls are included in Section IV, they are an integral part of Mobly's description of the system. This section provides information about the five interrelated components of internal control at Mobly, including:

Control environment: Sets the tone, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.

Risk assessment: The entity's identification and analysis of relevant risks to the achievement of its objectives, forming a basis for determining how the risks can be managed.

Control activities: The policies and procedures that help make sure that management's directives are carried out.

Information and communication: Systems, both automated and manual, that support the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities.

Monitoring controls: A process that assesses the quality of internal control performance over time.

Control Environment

The objectives of internal control as it relates to Mobly are to provide reasonable, but not absolute, assurance that controls are suitably designed and operating effectively to meet the relevant controls, that assets are protected from unauthorized use or disposition, and that transactions are executed in accordance with management's authorization and client instructions. Management has established and maintains controls designed to monitor compliance with established policies and procedures. The remainder of this subsection discusses the tone at the top as set by management, the integrity, ethical values, and competence of Mobly employees, the policies and procedures, the risk management process and monitoring, and the roles of significant control groups. The internal control structure is established and refreshed based on Mobly's assessment of risk facing the organization.

5.1 Integrity and Ethical Values

Integrity and ethical values are essential elements of the control environment, affecting the design, administration and monitoring of key processes. Integrity and ethical behavior are the products of Mobly's ethical and behavioral standards, how they are communicated, and how they are monitored and enforced in its business activities. They include management's actions to remove or reduce incentives/pressures, and opportunities that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of the entity's values and behavioral standards to personnel through policy statements and codes of conduct, and by the examples the executives set.

Mobly's senior management recognizes their responsibility to foster a strong ethical environment within Mobly to determine that its business affairs are conducted with integrity, and in accordance with high standards of personal and corporate conduct. This responsibility is characterized and reflected in Mobly's Code of Conduct, which is distributed to all employees of the organization.

All employees are required to maintain ongoing compliance with all statements of policies, procedures, and standards of the Code of Conduct and with lawful and ethical business practices, whether or not they are specifically mentioned in the Code of Conduct. Each employee is required to affirm annually that he or she received, read, understood, and complied with the requirements set forth in the Information Security Policy, Acceptable Use Policy, Employee Handbook, and Code of Conduct within the first week of employment and annually thereafter.

5.2 Executive Management Governance and Oversight

The management committee, chaired by the chief executive officer (CEO), has been delegated by the board the responsibility for managing Mobly and its business on a daily basis. Members of Mobly's management committee draw experience from their former roles as senior executives of large organizations specializing in software integrations, product oversight, development, sales, and marketing, customer service, and governance, risk, and compliance.

In its role, the management committee assigns authority and responsibility for operating activities and establishes reporting relationships and authorization hierarchies. The management committee designs policies and communications so that personnel understand Mobly's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Lines of authority and responsibility are clearly established throughout the organization under the management committee. These lines of authority and the associated responsibilities are communicated through: (1) management's philosophy and operating style; (2) organizational structure; (3) employee job descriptions; and (4) policy and procedure manuals.

Managers are expected to be aware of their responsibilities and lead employees in complying with Mobly policies and procedures.

5.3 Organizational Structure and Assignment of Authority and Responsibility

Mobly's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Mobly has established an organizational structure that includes consideration of key areas of authority and responsibility, as well as appropriate lines of reporting.

Mobly has an established organizational structure with defined roles and responsibilities.

5.4 Commitment to Competence

Mobly has implemented a structured performance appraisal process. Managers are asked to discuss performance expectations and goals with each employee. These objectives and development goals are formally documented. Mobly conducts an annual performance review for each employee per calendar year. Annual performance evaluations affirmed by the employee, and their leader or manager are maintained in electronic form. Managers are also strongly encouraged to have ongoing, informal conversations with employees regarding their performance throughout the year.

Mobly has developed a mandatory training program for its employees, including a coordinated new hire orientation program. Additional continuing professional education and development opportunities are identified through the goal-setting and development-planning process. Managers and HR identify learning plans both by role and level. It is also the manager's role to identify what training a particular employee requires to comprehend Mobly's policies and procedures as they relate to specific job requirements. Each employee has the opportunity to partake in formal training classes, on-the-job training, or online education courses. A record of training program attendance is maintained for each employee.

5.5 Accountability

Human resource (HR) policies and practices relate to hiring, orienting, training, evaluating, counseling, promoting and compensating personnel. The competence and integrity of Mobly personnel are essential elements of its control environment. The organization's ability to recruit and retain a sufficient number of competent and responsible personnel is dependent to a great extent on its HR policies and processes.

The HR policies and processes of Mobly are designed to: (1) identify and hire competent personnel; (2) provide employees with the training and information they need to perform their jobs; (3) evaluate the performance of employees to verify their ability to perform job assignments; and (4) through performance evaluation, identify opportunities for growth and job performance improvement.

Formal written job descriptions are developed and maintained for each position.

Mobly has established formal web-based security awareness training that is required to be completed by all new employees within the first two weeks of employment and on an annual basis. Employees are also encouraged to actively participate in professional organizations and forums to maintain their knowledge and develop awareness of issues facing Mobly.

HR, in unison with the hiring manager, screens potential candidates and selects resumes of potential candidates to be interviewed. The managers review documentation, select candidates, and inform HR of individuals with whom they wish to schedule interviews. The relevant manager and HR conduct interviews and potential offers are submitted to the appropriate authority within the organization for approval. Individuals offered a position at Mobly are subject to background checks (as appropriate for each country with respect to local laws and regulations) prior to commencing employment. Prospective employees complete an employment application and sign waivers to release information for the background check. In addition, it is the policy of Mobly to request employment references to determine whether the candidate is well-qualified and has the potential to be productive and successful during his or her tenure.

After receiving a signature, all new employees receive an email containing information pertaining to the first day of employment. Mobly's onboarding program includes the distribution and acknowledgement of the Employee Handbook, Information Security Policy and Acceptable Use Policy, relevant compensation materials, benefit materials, and Code of Conduct.

HR is responsible for managing voluntary and involuntary terminations. Voluntary terminations are identified by the employee's supervisor and are tracked and recorded. HR personnel communicate with the employee to identify the employee's final day of employment and to inform the employee of his or her rights and responsibilities. The final day is entered into the HR management system and an exit interview is scheduled. During the exit interview, the employee is asked to return any of Mobly assets in their possession, including laptop, and so on. The HR person records and tracks the information.

5.6 Risk Assessment

The process of identifying, assessing and managing risks is a critical component of Mobly's internal control system. The purpose of Mobly's risk assessment process is to identify, assess, and manage risks that affect the organization's ability to achieve its objectives. The management of Mobly also monitors controls to consider whether they are operating as intended and whether they are modified as appropriate for changes in conditions or risks facing the organization.

Ongoing monitoring procedures are built into the normal recurring activities of Mobly's and include regular management and supervisory activities. Managers of the various organizational units are regularly in touch with personnel and may question the accuracy of the information that differs significantly from their knowledge of operations.

Mobly has established an independent organizational business unit, that is responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. The acting CISO's approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. The acting CISO attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership and senior management.

At least annually, the acting CISO is responsible for assessing Mobly's risk and control environment through rigorous evaluation of financial, operational, and administrative controls, risk management practices, and compliance with laws, regulations, and Mobly policies and procedures. The acting CISO reports functionality, significant findings and the status of corrective actions directly to the executive management team. The acting CISO adheres to standards of moral and ethical conduct, in addition to upholding relevant information security and privacy certifications and abiding by regulatory body requirements.

An annual third party risk assessment is performed including a review of attestation reports (i.e., SOC 2, or ISO 27001) for critical vendors where user data is shared. Results and action items are communicated to the respective owners and tracked through internal risk management tools.

Control Activities

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of the trust service security category.

User Identification and Authentication

Employees and approved personnel sign into Mobly information systems using a unique ID and password, shared accounts are not permitted. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of Identity and Access Management (IAM) Solutions for the Gsuite and Google Cloud Provider..

Passwords must conform to defined password standards and are enforced through parameter settings in Identity and Access Management (IAM) Solutions for the Gsuite and Google Cloud Provider. These settings are part of the configuration standards and force users to change passwords at a defined interval, will lock laptop screens, and require reentry of the user ID and password after a period of inactivity.

Mobly's personnel, who work remote and from the office, are required to use multi-factor authentication when accessing Mobly's information systems. Password composition rules, including a minimum of nine characters, at least one number, special character, uppercase letter and lowercase letter, are systematically enforced across all production system components in accordance with company policy. Administrator access is restricted to authorized system and security administrators.

Customers access cloud services through the Internet using a secure version of Transport Layer Security (TLS) through their web browser.

Laptops are initially configured in accordance with Mobly's configuration standards, but these configuration parameters may be changed by the Mobile Device Management Policy.

Access Provisioning/Deprovisioning

Upon hire, employees are assigned to a position in the HR management system. Prior to the employees' start date, HR completes an onboarding form with accounts to be created and access to be granted. Next, HR submits an access request ticket for authorized team leads to provide access to approved systems. Access requests are also submitted for employees with position changes and the associated roles to be changed.

On an annual basis, access for each user is reviewed by a working group composed of the HR manager and each department head, who is responsible for approving access for their assigned team. In evaluating user access, group members consider job description, duties requiring segregation, and risks associated with access. Completed user access is reviewed and approved by the CEO or acting CISO. As part of this process, the CEO or acting CISO reviews access by privileged roles and requests modifications based on this review.

All access request changes to user access are submitted through the access request ticket tracking system for review and approval by management.

For terminated employees, HR completes an offboarding form based on the employee's initial onboarding form. The form with a ticket request for access removal is submitted to authorized team leads to ensure access is removed within one business day.

Asset Management

All dynamic resources (virtual instances and services) are generated with automation and tracked to ensure complete asset inventory of all virtual assets.

Laptops are inventoried and formally documented to include device identifier and device owner. The list is kept up-to-date by the IT team.

Laptop Management and Protection

For laptop endpoint protection and management, a mobile device management solution is used that includes: encryption, malware protection (antivirus), security updates and ability to set and enforce policies (i.e., screen saver, require password etc.), and remote wipe of laptop due to loss, damage, or theft.

Encryption of Communication Outside the Boundaries

Authorized employees may access the system from the internet through the use of a leading virtual private network (VPN) technology. Employees are authenticated through the use of a multi-factor authentication system.

Mobly uses a certificate authority, to provide digital certificates used to support encrypted communication for customer user requests to and from the Mobly Platform web portal.

Encryption for Storage of Customer Data

The storage of all customer data is securely encrypted. Mobly ensures the proper and effective use of cryptography to protect the confidentiality, authenticity, and integrity of information according to business and information security requirements, and takes into consideration legal, statutory, regulatory, and contractual requirements related to cryptography.

Configuration Management

For cloud-based images, if base images are used outside of preconfigured operating systems (OS) provided by the hosting provider, images are pulled directly from the verified official repositories and contain latest security updates. With preconfigured operating systems, live updates ensure that OSs and software are kept up-to-date with security patches.

For automation in Mobly's cloud-based environments, Infrastructure as Code (IaC) is used to manage security configurations. Security configurations are continuously monitored and reviewed.

5.7 Change Management

Mobly has a formal process for tracking and managing system changes for the introduction of new systems and major changes to existing systems.

Changes are classified as (1) emergency deployment, meaning that they must be deployed on all production elements within a defined number of weeks; (2) standard deployment, which must be deployed on all production elements within a defined number of months; and (3) deploy on rebuild, which is classified as being deployed only when other changes are made to the system configuration.

Secure Development

Mobly has a formalized security and systems development methodology that includes project planning, tracking, designing, testing, implementation, maintenance, and disposal or decommissioning. Proposed changes are evaluated to determine if they present a security risk and what mitigating actions, including employee and user entity notifications, must be performed.

All infrastructure and code changes require independent validation prior to implementation to production to help ensure change requirements are met and security issues are resolved.

Changes to infrastructure and software are developed and tested in a separate development or test environment. Changes are tested according to the nature of the change prior to deployment to production. Customer content and personal information are not used in non-production environments. Applications are peer reviewed to address any concerns prior to production deployment. Developers do not have the ability to migrate their own code changes into production environments.

New information systems, upgrades and new versions are thoroughly tested and verified during the development processes. Security testing is an integral part of the testing for systems or components. Static code analysis and dependency scanner tools are used to identify and remediate security vulnerabilities, prior to deploying to production.

Development, testing and production environments are separated and secured to protect the production environment and data from compromise by development and test activities.

5.8 Physical Access and Environmental Controls

No servers or computer facilities for the system applications are hosted on site. All computer facilities and access thereto are controlled at cloud infrastructure data centers. As such, trust service criteria CC6.4 is not applicable to Mobly.

Networks Security

Networks and network devices are secured, managed, and controlled to protect against attacks that can affect availability, compromise security, or consume excessive resources.

Mobly keeps an accurate and up-to-date architecture/network diagram. Google Firewalls and Load Balancers are configured to control access and monitor requests that are forwarded to protected web application resources: (1) to block all requests except the ones specified; (2) to protect against threats at the network and transport layers (e.g., DDoS attacks); (3) to manage, setup and configure web access control lists (ACLs); and (4) to ensure all egress and ingress traffic is going through the VPC Endpoints (firewall).

Google VPC Firewalls support our private, public and test network segmentations, which are set up and configured for network segregation to split the network into security boundaries and to control traffic between them based on business needs. This helps ensure development, testing, and production environments are separated and secured to protect the production environment and data from compromise by development and test activities. Network administration channels are also segregated from other network traffic.

Monitoring Activities

Networks, systems and applications are monitored for anomalous behavior and appropriate actions are taken to evaluate potential information security incidents.

The following are included within the monitoring system: (1) outbound and inbound network, system and application traffic; (2) access to systems, servers, networking equipment, monitoring systems, critical applications, etc.; (3) critical or admin level system and network configuration files; (4) logs from security tools (e.g., antivirus, IDS, intrusion prevention system or IPS, web filters, firewalls, data leakage prevention); (5) event logs relating to system and network activity; (6) code being executed is authorized to run in the system and that it has not been tampered with (e.g., by recompilation to add additional unwanted code); and (7) use of the resources (e.g., CPU, hard disks, memory, bandwidth) and their performance.

5.9 Incident Management

Mobly management defines and communicates the roles and responsibilities within the Incident Response Plan (IRP) to ensure individuals responsible understand the organization's priorities for handling information security incidents including resolution time frame based on potential consequences and severity.

All personnel and customers are made aware of their responsibility to report information security events as quickly as possible in order to prevent or minimize the effect of information security incidents.

Mobly uses a status and incident communication tool to keep customers and employees informed during downtime via Slack and Email.

Vulnerability Management and Penetration Testing

Vulnerability scanning is performed on a weekly basis in accordance with Mobly policy. The scanning method uses industry standard scanning technologies and a formal methodology specified by Mobly. These technologies are customized to test Mobly's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as-needed basis. Tools requiring installation in the system are implemented through the change management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

An annual penetration test is conducted by a third party vendor to measure the security posture of a target system or environment. The vendor uses an accepted industry standard penetration testing methodology specified by Mobly. The vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test. Once vulnerabilities are identified, the vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network layer testing as well as testing of controls and processes around the networks, and occurs from outside (external testing) the network.

The penetration testing reports specify identified vulnerabilities, a level of assessed risk for each vulnerability identified, and suggested remediation. The report includes an executive summary and client summary, which is available to Mobly customers upon request.

Individual vulnerabilities identified during penetration and vulnerability testing are logged to the event management software and managed through the incident management process.

5.10 Information and Communication

Information and communication is an integral component of Mobly's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Mobly, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Customer Support and Agreements

The organization plans and prepares for managing customer support requests and reporting of security incidents by defining, establishing, and communicating a formal process to ensure quick, effective, consistent, and orderly responses. A ticketing system is used to monitor, respond to, and track customer support requests and incidents:

- During onboarding, clients are trained and provided a link to submit requests and security incidents. A backup option is provided to submit an email directly to the ticketing system or internal customer care team opens a ticket.
- Tickets are used to document and track ongoing status updates and communication related to ticket requests

Customer service agreements are established and documented to ensure there is clear understanding between the organization and customer regarding both parties' obligations to fulfill relevant information security requirements. A cloud-based tool to manage, deploy, and catalog signed agreements is used. Management ensures the standard customer service agreement template is kept up-to-date and includes:

- Applicable standards, laws, and regulations
- Defined SLAs
- Rules of use (link to terms of use on website)
- Defined confidentiality and security clauses with customer responsibilities

The company makes descriptions of its services, component systems, and their boundaries readily available to customers and other stakeholders via its website, product documentation, emails, and/or blog posts.

Mobly also maintains internal informational websites describing the system environment, its boundaries, user responsibilities, and services to employees.

5.11 Monitoring Controls

In addition to the quarterly testing, continuous monitoring tools are in place. Refer to Monitoring Activities and Incident Management sections above.

DC 6: Complementary User Entity Controls

Mobly controls were designed with the assumption that certain internal controls would be in place at customer organizations. The application of such internal controls by customer organizations is necessary to achieve certain trust services criteria identified in this report. In addition, there may be control activities that are not identified in this report that would be appropriate for processing of transactions for Mobly customers.

For customers to rely on the information processed through the Mobly Platform, each customer is expected to evaluate its own internal controls to ensure appropriate control activities are in place. The following general procedures and controls should be considered. They should not, however, be regarded as a comprehensive list of all controls that should be implemented by customer organizations.

- User entity is responsible for protecting established user IDs within their organizations.
- User entity is responsible for reviewing customer access to the Mobly Platform periodically to validate appropriateness of access levels.
- User entity is responsible for approving and creating new user access to the Mobly Platform.
- User entity is responsible for removing terminated employee access to the Mobly Platform.
- User entity is responsible for implementing policies and procedures over the types of data that are allowed to be entered into the Mobly Platform.
- User entity is responsible for sending data to Mobly via a secure connection and/or the data should be encrypted.
- User entities are responsible for notifying Mobly if they detect or suspect a security incident related to the Mobly Platform.
- User entity is responsible for reviewing email and other forms of communications from Mobly, related to changes that may affect Mobly customers and users, and their security obligations.
- User entity is responsible for establishing, monitoring, and maintaining controls over the security for system-generated outputs and reports from the system.
- User entity is responsible for endpoint protection of workstations used to access the system.

DC 7: Complementary Subservice Organization Controls (CSOCs)

Mobly uses a subservice organization in support of its system. Mobly's controls related to the system cover only a portion of overall internal control for user entities. It is not feasible for the trust services criteria over the Mobly Platform to be achieved solely by Mobly. Therefore, user entity controls must be evaluated in conjunction with Mobly's controls described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Mobly periodically reviews the quality of the outsourced operations by various methods including:

- Review of the sub service organization's SOC reports
- Regular meetings to discuss performance
- Non-disclosure agreements

Control Activity Expected to be Implemented by Subservice Organization	Subservice Organization	Applicable Criteria
Logical access to the underlying network and virtualization management software for cloud architecture is appropriate.	Google Cloud Provider	CC6.1, CC6.2, CC6.3, CC6.5, CC7.2
Physical access to the data center facility is restricted to authorized personnel.	Google Cloud Provider	CC6.4, CC6.5
Intrusion detection mechanisms are in place to prevent or identify potential security attacks by unauthorized actors outside boundaries of the system.	Google Cloud Provider	CC6.1, CC7.2, CC7.3, CC7.4
Environmental protections, including monitoring and alarming mechanisms, are implemented to address physical security and environmental control requirements.	Google Cloud Provider	CC6.4
A defined Data Classification Policy specifies classification levels and control requirements in order to meet the company's commitments related to confidentiality.	Google Cloud Provider	CC1.1
A defined process is in place to sanitize and destroy hard drives and back up media containing customer data prior to leaving company facilities.	Google Cloud Provider	CC1.2

DC 8: Any Specific Criterion of the Applicable Trust Services Criteria that is Not Relevant to the System and the Reasons it is Not Relevant

All the trust services criteria for the category or categories addressed by the description are relevant to the system.

DC 9: Disclosures of Significant Changes in Last 1 Year

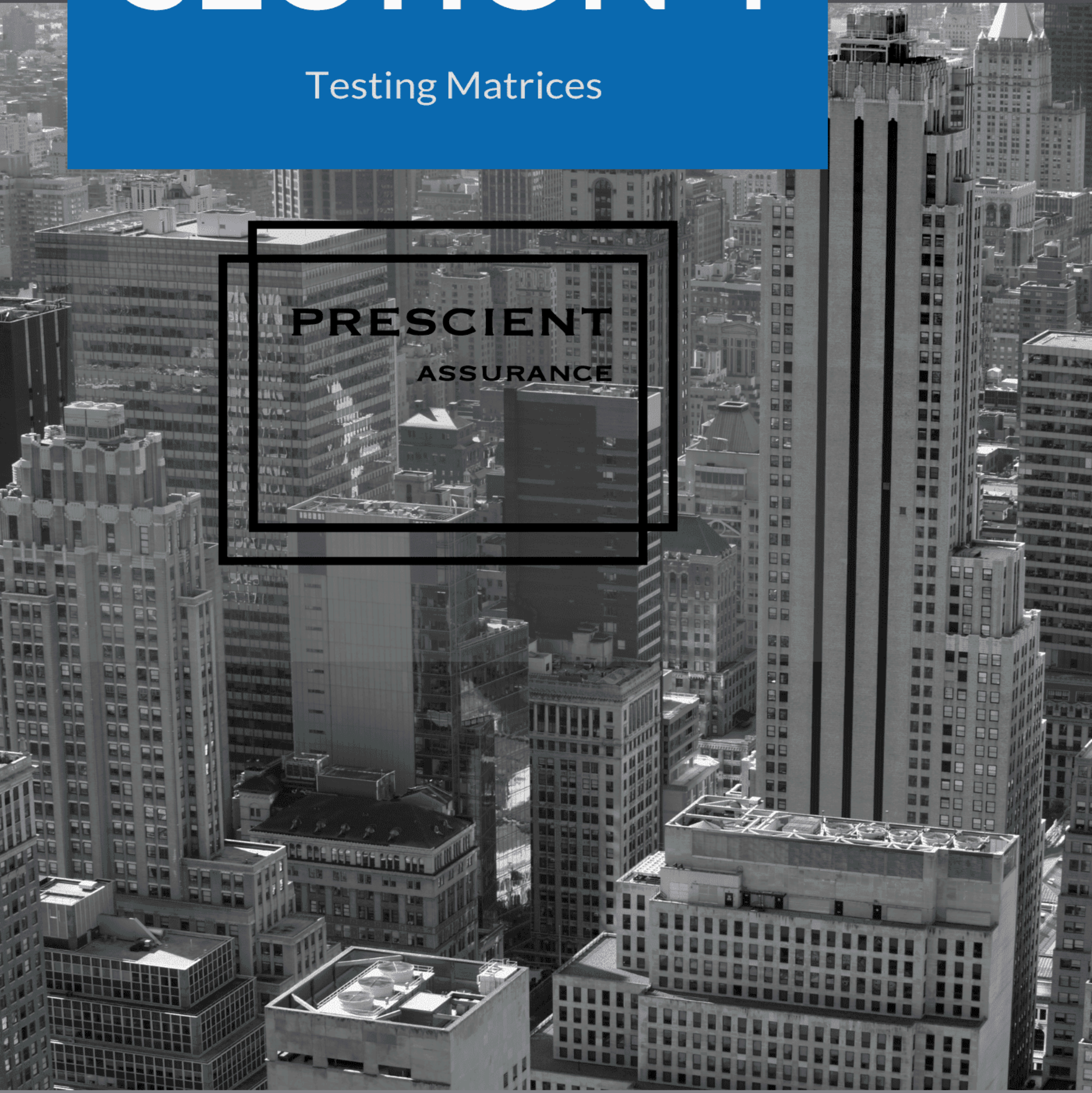
There were no changes that are likely to affect report users' understanding of how the system is used to provide the service during the period of time covered by the description.

Changes to the System During the Period

There were no changes that are likely to affect report users' understanding of how the system is used to provide the service during the period from 1 January 2024 - 1 October 2024

SECTION 4

Testing Matrices



PRESCIENT ASSURANCE

Tests of Operating Effectiveness and Results of Tests

Scope of Testing

This report on the controls relates to Mobly provided by Mobly, Inc. The scope of the testing was restricted to Mobly, and its boundaries as defined in Section 3.

Prescient Assurance LLC conducted the examination testing throughout the period January 01, 2024 to October 1, 2024.

The tests applied to test the Operating Effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that all applicable trust services criteria were achieved during the review date. In selecting the tests of controls, Prescient Assurance LLC considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates.
- The control risk mitigated by the control.
- The effectiveness of entity-level controls, especially controls that monitor other controls.
- The degree to which the control relies on the effectiveness of other controls.
- Whether the control is manually performed or automated.

Types of Tests Generally Performed

The table below describes the nature of our audit procedures and tests performed to evaluate the operational effectiveness of the controls detailed in the matrices that follow:

Test Types	Description of Tests
Inquiry	**Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.**
Inspection	**Inspected documents and records indicating performance of the control. This includes, but is not limited to, the following:** ● **Examination / Inspection of source documentation and authorizations to verify transactions processed.** ● **Examination / Inspection of documents or records for evidence of performance, such as existence of initials or signatures.**

	● Examination / Inspection of systems documentation, configurations, and settings; and ● Examination / Inspection of procedural documentation such as operations manuals, flow charts and job descriptions.
Observation	Observed the implementation, application or existence of specific controls as represented. Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Re-performance	Re-performed the control to verify the design and / or operation of the control activity as performed if applicable.

General Sampling Methodology

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Prescient Assurance utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, to determine the number of items to be selected in a sample for a particular test. Prescient Assurance, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

The table below describes the sampling methodology utilized in our testing to evaluate the operational effectiveness of the controls detailed in the matrices that follow:

Type of Control and Frequency	Minimum Number of Items to Test (Period of Review Six Months or Less)	Minimum Number of Items to Test (Period of Review More than Six Months)
Manual control, many times per day	At least 25	At least 40
Manual control, daily (Note 1)	At least 25	At least 40

Manual control, weekly	At least 5	**At least 10**
Manual control, monthly	At least 3	**At least 4**
Manual control, quarterly	At least 2	**At least 2**
Manual control, annually	Test annually	**Test annually**
Application controls	Test one operation of each relevant aspect of each application control if supported by effective IT general controls; otherwise test at least 15	**Test one operation of each application control if supported by effective IT general controls; otherwise test at least 25**
IT general controls	Follow guidance above for manual and automated aspects of IT general controls	**Follow guidance above for manual and automated aspects of IT general controls**
Notes: 1.) Some controls might be performed frequently, but less than daily. For such controls, the sample size should be interpolated using the above guidance. Generally, for controls where the number of occurrences ranges from 50 to 250 during the year, our minimum sample size using the above table should be approximately 10% of the number of occurrences.		

Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase "No exceptions noted." in the test result column of the Testing Matrices. Any phrase other than this constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the Operating Effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors.

Trust ID	Trust Service criteria	Control Description	Test Applied by the Service Auditor	Test Results
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Executive leadership conducts quarterly executive leadership meetings to demonstrate leadership and commitment per requirements in Security Program Committee Charter.	Inspected the Security Program Committee Charter to determine that executive leadership was required to conduct quarterly meetings to demonstrate leadership and commitment. Inspected the Security Committee Meeting Minutes from September 2024, to determine that quarterly executive leadership meetings were held.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Management establishes and assigns, structures, reporting lines, and appropriate authorities and responsibilities aligned with business objectives.	Inspected the Security Program Committee Charter to determine that the management has established and assigned appropriate authorities and responsibilities aligned with business objectives, including regular executive leadership meetings, the establishment of policies and security objectives, and ongoing strategic collaboration for continual improvement.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Employee contractual agreements upon hire include the Employee Handbook (includes conduct and ethics), Confidentiality Agreements (e.g. NDA), Acceptable Use Policy and Information Security Policy.	Inspected the policy and employee handbook acknowledgment record to determine that employees were required to sign an NDA upon hire and annually thereafter.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	An organizational chart is created to define reporting lines and divisions for segregation of duties and updated at least twice a year, to reduce the risk of fraud, error and bypassing of controls.	Inspected the Personnel Security Policy to determine that an organizational chart is created to define reporting lines and divisions for segregation of duties and updated at least twice a year, to reduce the risk of fraud, error, and bypassing of controls. Inspected the company's organizational chart showing the reporting lines and positions of authority to determine that the company has a formal organizational	No exceptions noted.

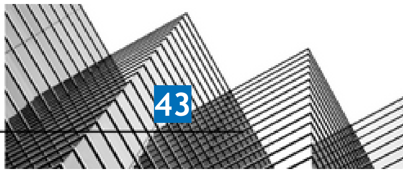


			chart in place that is accessible to internal personnel.	
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Acceptable Use Policy outlines the relevant conditions and restrictions for personnel working remotely to protect information accessed, processed or stored outside the organization's premises.	Inspected the Acceptable Use Policy to determine that the company has defined a formal procedure for personnel working remotely to protect information accessed, processed, or stored outside the organization.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Background verification checks on all candidates for employment are carried out prior to employment.	Inspected the record of the Checkr background list to determine that background verification checks on all candidates for employment were carried out before employment.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Define clear desk and clear screen rules within Acceptable Use Policy and ensure employees acknowledge at least annually.	Inspected the Acceptable Use Policy to determine that the company has a formal procedure in place outlining clean desks and clear screen rules. Inspected the policy acknowledgment record to determine that the employees had accepted the acceptable use policy at least annually.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the Personnel Security Policy to determine that performance evaluations are required to be completed on an annual basis for all personnel. Inspected the list of employees along with performance evaluation review dates to determine that formal performance evaluations were conducted annually for personnel.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Acceptable use for handling information and assets is identified, documented and implemented.	Inspected the Acceptable Use Policy to determine that the acceptable use for handling information and assets was identified and documented.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from	Executive leadership evaluates the performance and the effectiveness of	Inspected the Security Program Committee Charter to determine the performance and effectiveness of compliance controls based on predefined	No exceptions noted.

	management and exercises oversight of the development and performance of internal control.	controls based on predefined metrics.	metrics by establishing and monitoring Key Performance Indicators (KPIs) to ensure controls adequately addressed risk and met compliance requirements. Inspected the compliance automation platform to determine that executive leadership could monitor controls and evaluate their effectiveness using predefined metrics.	
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Business continuity planning is conducted to ensure that the organization’s objectives can continue to be met during disruption.	Inspected the Business Continuity Policy defining Business Impact Analysis procedure to determine that it defines the necessary steps to conduct a thorough analysis of potential business impacts, ensuring the organization's objectives can continue to be met during a disruption. Inspected the Business Impact Analysis report to determine that it defines the necessary steps to conduct a thorough analysis of potential business impacts, ensuring the organization's objectives can continue to be met during a disruption.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Management establishes and assigns, structures, reporting lines, and appropriate authorities and responsibilities aligned with business objectives.	Inspected the Security Program Committee Charter to determine that the management has established and assigned appropriate authorities and responsibilities aligned with business objectives, including regular executive leadership meetings, the establishment of policies and security objectives, and ongoing strategic collaboration for continual improvement.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	An organizational chart is created to define reporting lines and divisions for segregation of duties and updated at least twice a year, to reduce the risk of fraud, error and bypassing of controls.	Inspected the Personnel Security Policy to determine that an organizational chart is created to define reporting lines and divisions for segregation of duties and updated at least twice a year, to reduce the risk of fraud, error, and bypassing of controls. Inspected the company's organizational chart showing the reporting lines and positions of authority to determine that	No exceptions noted.

			the company has a formal organizational chart in place that is accessible to internal personnel.	
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	An organizational chart is created to define reporting lines and divisions for segregation of duties and updated at least twice a year, to reduce the risk of fraud, error and bypassing of controls.	Inspected the Personnel Security Policy to determine that an organizational chart is created to define reporting lines and divisions for segregation of duties and updated at least twice a year, to reduce the risk of fraud, error, and bypassing of controls. Inspected the company's organizational chart showing the reporting lines and positions of authority to determine that the company has a formal organizational chart in place that is accessible to internal personnel.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	An Information Security Policy with aligned topic-specific policies is defined, approved by management, published, communicated to employees, and reviewed annually or when significant changes occur.	Inspected the Information Security Policy to determine that the policy was last reviewed on December 04, 2023. Additionally, confirmed that the policy includes supporting topic-specific policies, procedures, and guidelines accessible to all employees and third parties on the company's internal website.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer process.	Inspected the Personnel Security Policy to determine that job requirements were documented, and abilities were evaluated during hiring or transfer to ensure competent employees filled roles. Inspected the Job description for the position of CISO to determine that requirements were formally documented and employees were evaluated as part of hiring or transfer.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and	Management establishes and assigns, structures, reporting lines, and appropriate authorities and responsibilities aligned with business objectives.	Inspected the Security Program Committee Charter to determine that the management has established and assigned appropriate authorities and responsibilities aligned with business objectives, including regular executive leadership meetings, the establishment of	No exceptions noted.

	responsibilities in the pursuit of objectives.		policies and security objectives, and ongoing strategic collaboration for continual improvement.	
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer process.	Inspected the Personnel Security Policy to determine that job requirements were documented, and abilities were evaluated during hiring or transfer to ensure competent employees filled roles. Inspected the Job description for the position of CISO to determine that requirements were formally documented and employees were evaluated as part of hiring or transfer.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Background verification checks on all candidates for employment are carried out prior to employment.	Inspected the record of the Checkr background list to determine that background verification checks on all candidates for employment were carried out before employment.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	An information security awareness, education and training platform is used to deliver and track assigned courses for new hires and ongoing annual training for all employees.	Inspected the Personal Security Policy to determine that all employees were required to receive security training, with new hires receiving it within one week and all employees receiving it annually. Inspected the training completion records to determine that employees had completed the information security training assignments.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the Personnel Security Policy to determine that performance evaluations are required to be completed on an annual basis for all personnel. Inspected the list of employees along with performance evaluation review dates to determine that formal performance evaluations were conducted annually for personnel.	No exceptions noted.

CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Define clear desk and clear screen rules within Acceptable Use Policy and ensure employees acknowledge at least annually.	Inspected the Acceptable Use Policy to determine that the company has a formal procedure in place outlining clean desks and clear screen rules. Inspected the policy acknowledgment record to determine that the employees had accepted the acceptable use policy at least annually.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Acceptable Use Policy outlines the relevant conditions and restrictions for personnel working remotely to protect information accessed, processed or stored outside the organization's premises.	Inspected the Acceptable Use Policy to determine that the company has defined a formal procedure for personnel working remotely to protect information accessed, processed, or stored outside the organization.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Acceptable use for handling information and assets is identified, documented and implemented.	Inspected the Acceptable Use Policy to determine that the acceptable use for handling information and assets was identified and documented.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the Personnel Security Policy to determine that performance evaluations are required to be completed on an annual basis for all personnel. Inspected the list of employees along with performance evaluation review dates to determine that formal performance evaluations were conducted annually for personnel.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	An Information Security Policy with aligned topic-specific policies is defined, approved by management, published, communicated to employees, and reviewed annually or when significant changes occur.	Inspected the Information Security Policy to determine that the policy was last reviewed on December 04, 2023. Additionally, confirmed that the policy includes supporting topic-specific policies, procedures, and guidelines accessible to all employees and third parties on the company's internal website.	No exceptions noted.

CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Employee contractual agreements upon hire include the Employee Handbook (includes conduct and ethics), Confidentiality Agreements (e.g. NDA), Acceptable Use Policy and Information Security Policy.	Inspected the policy and employee handbook acknowledgment record to determine that employees were required to sign an NDA upon hire and annually thereafter.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Executive leadership evaluates the performance and the effectiveness of controls based on predefined metrics.	Inspected the Security Program Committee Charter to determine the performance and effectiveness of compliance controls based on predefined metrics by establishing and monitoring Key Performance Indicators (KPIs) to ensure controls adequately addressed risk and met compliance requirements. Inspected the compliance automation platform to determine that executive leadership could monitor controls and evaluate their effectiveness using predefined metrics.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Information security risk assessments and treatments are performed and formally documented via risk register annually or when significant changes occur.	Inspected the Risk Assessment and Treatment Policy to determine that information security risk assessments and treatments are performed and formally documented via the risk register annually or when significant changes occur. Observed a sample of risks within the risk register maintained on the company's compliance platform, last updated within the audit period, to determine that risks are assigned, tracked, and categorized via a risk register, with risk assessments completed at least annually.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support	An Information Security Policy with aligned topic-specific policies is defined, approved by management, published, communicated to employees, and reviewed annually or	Inspected the Information Security Policy to determine that the policy was last reviewed on December 04, 2023. Additionally, confirmed that the policy includes supporting topic-specific policies, procedures, and guidelines accessible to all employees and third parties on the company's internal website.	No exceptions noted.

	the functioning of internal control.	when significant changes occur.		
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Information security operational activities are documented and made available to all users who need them.	Inspected the Information Security Operational Activities to determine that formal security operational procedures were in place and available to all users via the Trustero platform.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Customer service agreements are established and documented to ensure that there is clear understanding between the organization and the customer regarding both parties' obligations to fulfill relevant information security requirements.	Inspected the Main Services Agreement to determine that service agreements are maintained and documented to ensure clear understanding between the relevant parties.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The organization establishes and communicates a formal process for managing customer support requests and security incidents.	Inspected the Information Security Policy to determine that the organization plans and prepares for managing customer support requests and reporting security incidents by defining, establishing, and communicating a formal process, to ensure quick, effective, consistent, and orderly responses. A ticketing system is used to monitor, respond to, and track customer support requests and incidents. Inspected the email and contact number on the company's website to determine that a formal process for managing customer support requests and security incidents is in place.	No exceptions noted.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Executive leadership ensures planning, formal documentation, implementation and control of the operational processes needed to conduct information security risk assessments and treatment.	Inspected the Risk Assessment and Treatment Policy to determine that the management ensures planning and formal documentation of risk assessment and treatment. Inspected the risk register on the compliance platform to determine that	No exceptions noted.

			the company's processes enable a formal risk assessment to be conducted and identified risk tracked to resolution.	
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Information security risk assessments and treatments are performed and formally documented via risk register annually or when significant changes occur.	Inspected the Risk Assessment and Treatment Policy to determine that information security risk assessments and treatments are performed and formally documented via the risk register annually or when significant changes occur. Observed a sample of risks within the risk register maintained on the company's compliance platform, last updated within the audit period, to determine that risks are assigned, tracked, and categorized via a risk register, with risk assessments completed at least annually.	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.	Information security risk assessments and treatments are performed and formally documented via risk register annually or when significant changes occur.	Inspected the Risk Assessment and Treatment Policy to determine that information security risk assessments and treatments are performed and formally documented via the risk register annually or when significant changes occur. Observed a sample of risks within the risk register maintained on the company's compliance platform, last updated within the audit period, to determine that risks are assigned, tracked, and categorized via a risk register, with risk assessments completed at least annually.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	An organizational chart is created to define reporting lines and divisions for segregation of duties and updated at least twice a year, to reduce the risk of fraud, error and bypassing of controls.	Inspected the Personnel Security Policy to determine that an organizational chart is created to define reporting lines and divisions for segregation of duties and updated at least twice a year, to reduce the risk of fraud, error, and bypassing of controls. Inspected the company's organizational chart showing the reporting lines and positions of authority to determine that the company has a formal organizational chart in place that is accessible to internal personnel.	No exceptions noted.

CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Information security risk assessments and treatments are performed and formally documented via risk register annually or when significant changes occur.	Inspected the Risk Assessment and Treatment Policy to determine that information security risk assessments and treatments are performed and formally documented via the risk register annually or when significant changes occur. Observed a sample of risks within the risk register maintained on the company's compliance platform, last updated within the audit period, to determine that risks are assigned, tracked, and categorized via a risk register, with risk assessments completed at least annually.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	A formal process for tracking and managing system changes is followed for the introduction of new systems and major changes to existing systems.	Inspected the Change Management Policy to determine that a formal process for tracking and managing system changes was required to be followed for the introduction of new systems and major changes to existing systems. Inquired with the company to determine that there were no major changes or introduction of new system during the audit window.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Information security risk assessments and treatments are performed and formally documented via risk register annually or when significant changes occur.	Inspected the Risk Assessment and Treatment Policy to determine that information security risk assessments and treatments are performed and formally documented via the risk register annually or when significant changes occur. Observed a sample of risks within the risk register maintained on the company's compliance platform, last updated within the audit period, to determine that risks are assigned, tracked, and categorized via a risk register, with risk assessments completed at least annually.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate	An annual formal review of physical and logical access	Inspected the Identity and Access Management Policy to determine that user access rights reviews were required to be conducted and formally documented on	No exceptions noted.

	evaluations to ascertain whether the components of internal control are present and functioning.	rights is conducted for primary systems in scope.	an annual basis Inspected the RBAC Matrix to determine that the annual formal physical and logical access rights review was conducted for primary systems in scope.	
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.	Cloud-based accounts and services (e.g. workloads and instances) are continuously monitored for malicious activity (e.g. compromised accounts, malware, anomalous behavior) to detect threats.	Inspected the Security Event and Incident Management to determine that cloud-based accounts and services are continuously monitored for malicious activity to detect threats. Inspected the GCP Security Command System Findings to determine that the accounts and services are continuously monitored against threats or malicious activity.	No exceptions noted.
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.	Automated technical vulnerability scans are conducted weekly to identify and manage vulnerabilities to prevent exploitation of known vulnerabilities.	Inspected the Threat and Vulnerability Management Policy to determine that technical vulnerabilities are identified and managed to prevent exploitation of technical vulnerabilities. As a follow-up requirement to technical vulnerability scans, external penetration tests are conducted at least annually or when major changes occur to the systems in scope. Inspected the GCP Command Center findings to determine that automated technical vulnerability scans are conducted weekly to identify and manage vulnerabilities to prevent exploitation of known vulnerabilities.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are	Independent third-party penetration testing is conducted at least annually or when major changes occur to the systems in scope.	Inspected the penetration test provided to determine that third-party penetration testing was performed at least annually.	No exceptions noted.

	present and functioning.			
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.	Executive leadership evaluates the performance and the effectiveness of controls based on predefined metrics.	Inspected the Security Program Committee Charter to determine the performance and effectiveness of compliance controls based on predefined metrics by establishing and monitoring Key Performance Indicators (KPIs) to ensure controls adequately addressed risk and met compliance requirements. Inspected the compliance automation platform to determine that executive leadership could monitor controls and evaluate their effectiveness using predefined metrics.	No exceptions noted.
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.	Executive leadership conducts quarterly executive leadership meetings to demonstrate leadership and commitment per requirements in Security Program Committee Charter.	Inspected the Security Program Committee Charter to determine that executive leadership was required to conduct quarterly meetings to demonstrate leadership and commitment. Inspected the Security Committee Meeting Minutes from September 2024, to determine that quarterly executive leadership meetings were held.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Information security risk assessments and treatments are performed and formally documented via risk register annually or when significant changes occur.	Inspected the Risk Assessment and Treatment Policy to determine that information security risk assessments and treatments are performed and formally documented via the risk register annually or when significant changes occur. Observed a sample of risks within the risk register maintained on the company's compliance platform, last updated within the audit period, to determine that risks are assigned, tracked, and categorized via a risk register, with risk assessments completed at least annually.	No exceptions noted.
CC5.2	The entity also selects and develops	An Information Security Policy with aligned	Inspected the Information Security Policy to determine that the policy was last	No exceptions noted.

	general control activities over technology to support the achievement of objectives.	topic-specific policies is defined, approved by management, published, communicated to employees, and reviewed annually or when significant changes occur.	reviewed on December 04, 2023. Additionally, confirmed that the policy includes supporting topic-specific policies, procedures, and guidelines accessible to all employees and third parties on the company's internal website.	
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	An organizational chart is created to define reporting lines and divisions for segregation of duties and updated at least twice a year, to reduce the risk of fraud, error and bypassing of controls.	Inspected the Personnel Security Policy to determine that an organizational chart is created to define reporting lines and divisions for segregation of duties and updated at least twice a year, to reduce the risk of fraud, error, and bypassing of controls. Inspected the company's organizational chart showing the reporting lines and positions of authority to determine that the company has a formal organizational chart in place that is accessible to internal personnel.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Management establishes and assigns, structures, reporting lines, and appropriate authorities and responsibilities aligned with business objectives.	Inspected the Security Program Committee Charter to determine that the management has established and assigned appropriate authorities and responsibilities aligned with business objectives, including regular executive leadership meetings, the establishment of policies and security objectives, and ongoing strategic collaboration for continual improvement.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Information security operational activities are documented and made available to all users who need them.	Inspected the Information Security Operational Activities to determine that formal security operational procedures were in place and available to all users via the Trustero platform.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in	An Information Security Policy with aligned topic-specific policies is defined, approved by management, published,	Inspected the Information Security Policy to determine that the policy was last reviewed on December 04, 2023. Additionally, confirmed that the policy includes supporting topic-specific policies,	No exceptions noted.

	procedures that put policies into action.	communicated to employees, and reviewed annually or when significant changes occur.	procedures, and guidelines accessible to all employees and third parties on the company's internal website.	
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Information security operational activities are documented and made available to all users who need them.	Inspected the Information Security Operational Activities to determine that formal security operational procedures were in place and available to all users via the Trustero platform.	No exceptions noted.
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.	An inventory of laptops and cloud-based virtual infrastructure are maintained to help ensure critical data is located in authorized locations and protected.	Inspected the Asset Management Policy to determine that an inventory of cloud-based virtual infrastructure was required to be maintained to help ensure critical data was located in authorized locations and protected. Inspected the asset inventory list to determine that a complete inventory of all personnel assets was maintained with assigned owners.	No exceptions noted.
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.	Information is classified (e.g. public, confidential and sensitive) to ensure proper identification and understanding of protection needs of information.	Inspected the Information Classification and Handling Policy to determine that information is classified based on sensitivity levels to ensure proper protection needs are identified and understood.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from	Strong passwords and multi-factor authentication are used for accessing critical information systems to reduce the possibility of unauthorized access.	Inspected the Identity and Access Management Policy to determine that strong passwords and multi-factor authentication are used for accessing critical information systems to reduce the possibility of unauthorized access. Inspected the list of users for Google Workspace, and GitHub which had MFA	No exceptions noted.

	security events to meet the entity's objectives.		enabled and password configurations to determine that access was restricted to authorized personnel only.	
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.	Personnel return all company assets upon change or termination of their employment, contract or agreement.	Inquired with the company to determine that no employees were terminated during the audit period.	Not tested
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.	The granting, provisioning and use of privileged access rights is restricted and managed.	Inspected the list of users for GCP and GitHub, which had MFA enabled and an access log, to determine that access was restricted to authorized personnel only.	No exceptions noted.
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	All employees are assigned unique user IDs and shared accounts are not permitted to allow for the unique identification of individuals accessing information and assets.	Inspected the Identity and Access Management policy to determine that all employees are assigned unique user IDs and shared accounts are not allowed. Observed lists of employees, GitHub, and Google Workspace users along with their user names and IDs to determine that employees are assigned unique user IDs and shared accounts are not permitted to allow for the unique identification of individuals accessing information and assets.	No exceptions noted.

	credentials are removed when user access is no longer authorized.			
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.	Systems access that is no longer required for terminated or transferred users is removed within one business day.	Inquired with the company to determine that no employees were terminated during the audit period.	Not tested
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.	Access rights are provisioned, reviewed and approved by management to allow only authorized access.	Inspected the dashboard to determine that no access requests were made during the audit period.	Not tested
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets	Access to source code is managed to prevent unauthorized functionality, avoid unintentional or malicious changes and to maintain the confidentiality	Inspected the Identity and Access Management Policy to determine that access to source code is managed through MFA to prevent unauthorized functionality, unintentional or malicious changes, and maintain the confidentiality of valuable intellectual property.	No exceptions noted.

	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.	of valuable intellectual property.	Inspected the document displaying the list of GitHub users along with the MFA status enabled to determine that access to source code is restricted to authorized personnel only.	
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.	Secure areas (e.g. data centers, backup media storage, server rooms) are protected by appropriate entry controls and access points.		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.	Information stored on, processed by or accessible via laptops is protected against unauthorized access, malware, cyber threats and to prevent loss, damage or theft and interruption to operations.	Inspected the Asset Management Policy to determine that all information stored on, processed by, or accessible via laptops is protected against unauthorized access, malware, and cyber threats and to prevent loss, damage, or theft and interruption to operations. Inspected the list of devices displaying antivirus status and management details to determine that data is secured against unauthorized access, malware, and cyber threats and to prevent loss, damage, or theft and interruption to operations.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data	Prior to disposal or reuse, equipment, devices and storage media containing sensitive data and licensed software are securely wiped.	Inspected the Asset Management Policy to determine that equipment, devices, and storage media containing sensitive data and licensed software are securely wiped before disposal or reuse. Inquired with the company to determine	Not tested

	and software from those assets has been diminished and is no longer required to meet the entity's objectives.		that no media was disposed of or reused during the audit period.	
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Networks and network devices are secured, managed and controlled to protect against attacks that can affect availability, compromise security, or consume excessive resources.	Inspected the Network Security Policy to determine that networks and network devices were secured, managed, and controlled to protect against attacks that could affect availability, compromise security, or consume excessive resources. Inspected the Network Security Topology to determine that the network's mechanism and devices were secured and controlled to protect against attacks that could affect availability, compromise security, or consume excessive resources.	No exceptions noted.
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.	The storage of production data classified as sensitive or confidential per contractual or regulatory requirements is securely encrypted.	Inspected the Secure Configuration Policy to determine that the storage of production data classified as sensitive or confidential per contractual or regulatory requirements is securely encrypted. Inspected the encryption status of GCP Cloud storage buckets and GCP SQL instances to determine that sensitive or confidential production data is securely encrypted at rest.	No exceptions noted.
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.	The transmission of production data classified as sensitive or confidential per contractual or regulatory requirements is securely encrypted.	Inspected the Secure Configuration Policy to determine that the transmission of production data classified as sensitive or confidential per contractual or regulatory requirements is securely encrypted. Inspected the security certificate on the company's website which is valid until October 06, 2024, to determine that the company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.

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.	Cloud-based accounts and services (e.g. workloads and instances) are continuously monitored for malicious activity (e.g. compromised accounts, malware, anomalous behavior) to detect threats.	Inspected the Security Event and Incident Management to determine that cloud-based accounts and services are continuously monitored for malicious activity to detect threats. Inspected the GCP Security Command System Findings to determine that the accounts and services are continuously monitored against threats or malicious activity.	No exceptions noted.
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.	Information stored on, processed by or accessible via laptops is protected against unauthorized access, malware, cyber threats and to prevent loss, damage or theft and interruption to operations.	Inspected the Asset Management Policy to determine that all information stored on, processed by, or accessible via laptops is protected against unauthorized access, malware, and cyber threats and to prevent loss, damage, or theft and interruption to operations. Inspected the list of devices displaying antivirus status and management details to determine that data is secured against unauthorized access, malware, and cyber threats and to prevent loss, damage, or theft and interruption to operations.	No exceptions noted.
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.	Independent third-party penetration testing is conducted at least annually or when major changes occur to the systems in scope.	Inspected the penetration test provided to determine that third-party penetration testing was performed at least annually.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations	Configurations, including security configurations, are established, documented, implemented, monitored and reviewed to ensure required security settings, and configuration are not altered	Inspected the Secure Configuration Policy to determine that it states the organization's defined processes and tools to enforce configurations, including security configurations, for hardware, software, services, and networks.	No exceptions noted.

	that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	by unauthorized or incorrect changes.	Inspected the GCP Security Command Center findings and MDM list and settings to determine that subscribed security standards were tested against, with the number of checks passed and failed indicated to ensure required security settings and configurations are established and implemented.	
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.	Automated technical vulnerability scans are conducted weekly to identify and manage vulnerabilities to prevent exploitation of known vulnerabilities.	Inspected the Threat and Vulnerability Management Policy to determine that technical vulnerabilities are identified and managed to prevent exploitation of technical vulnerabilities. As a follow-up requirement to technical vulnerability scans, external penetration tests are conducted at least annually or when major changes occur to the systems in scope. Inspected the GCP Command Center findings to determine that automated technical vulnerability scans are conducted weekly to identify and manage vulnerabilities to prevent exploitation of known vulnerabilities.	No exceptions noted.
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.	Applications errors and crashes are captured and reviewed to make adjustments to the code as needed.	Inspected the Slack channel displaying alert notifications to determine that errors and crashes were formally documented and reviewed.	No exceptions noted.

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.	Cloud-based accounts and services (e.g. workloads and instances) are continuously monitored for malicious activity (e.g. compromised accounts, malware, anomalous behavior) to detect threats.	Inspected the Security Event and Incident Management to determine that cloud-based accounts and services are continuously monitored for malicious activity to detect threats. Inspected the GCP Security Command System Findings to determine that the accounts and services are continuously monitored against threats or malicious activity.	No exceptions noted.
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.	The use of production resources is monitored and adjusted in line with current and expected capacity requirements to prevent downtime of services.	Inspected the Business Continuity Policy to determine that the use of production resources is monitored and adjusted in line with current and expected capacity requirements to prevent downtime of services. System tuning and monitoring must be applied to ensure and, where necessary, improve the availability and efficiency of systems. Inspected the GCP logs and instances to determine that it is set to monitor production resources in line with current and expected capacity requirements.	No exceptions noted.
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	Event logs recording user activities, exceptions, faults and information security events are produced, stored, protected and analyzed.	Inspected the Security Event and Incident Management Policy to determine that event logs recording user activities, exceptions, faults, and information security events are produced, stored, protected, and analyzed. Observed the GCP audit log and Google Workspace admin activity log to determine that event logs recording user activities, exceptions, faults, and information security events are produced, stored, protected, and analyzed.	No exceptions noted.

	determine whether they represent 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.	Information security incidents are responded to in accordance with the Incident Response Plan to ensure efficient and effective response to information security incidents.	Inquired with the company to determine that no incidents were recorded during the audit period.	Not tested
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.	Information security incidents are responded to in accordance with the Incident Response Plan to ensure efficient and effective response to information security incidents.	Inquired with the company to determine that no incidents were recorded during the audit period.	Not tested
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Backup copies of information, software and systems are maintained and regularly tested to enable recovery from loss of data or systems.	Inspected the Business Continuity Policy to determine that backup copies of information, software, and systems must be maintained and regularly tested following the agreed topic-specific policy on backup to enable recovery from loss of data or systems. Inspected the log of backup and test performed to determine that the company maintains backup copies of information, software, and systems. Additionally, they are regularly tested to enable recovery from loss of data or systems.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from	Business continuity planning is conducted to ensure that the organization’s objectives	Inspected the Business Continuity Policy defining Business Impact Analysis procedure to determine that it defines the necessary steps to conduct a thorough	No exceptions noted.

	identified security incidents.	can continue to be met during disruption.	analysis of potential business impacts, ensuring the organization's objectives can continue to be met during a disruption. Inspected the Business Impact Analysis report to determine that it defines the necessary steps to conduct a thorough analysis of potential business impacts, ensuring the organization's objectives can continue to be met during a disruption.	
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.	A formal process for tracking and managing system changes is followed for the introduction of new systems and major changes to existing systems.	Inspected the Change Management Policy to determine that a formal process for tracking and managing system changes was required to be followed for the introduction of new systems and major changes to existing systems. Inquired with the company to determine that there were no major changes or introduction of new system during the audit window.	No exceptions noted.
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.	Static analysis security testing (SAST) and dependency scanning are used to identify and remediate security vulnerabilities, prior to deploying code to production.	Inspected the Threat and Vulnerability Management Policy to determine that the company is required to perform technical vulnerability scanning and external penetration tests. Inspected the GitHub repositories displaying status to determine that scanning is used to identify and remediate security vulnerabilities, before deploying code to production.	No exceptions noted.
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.	Access to source code is managed to prevent unauthorized functionality, avoid unintentional or malicious changes and to maintain the confidentiality of valuable intellectual property.	Inspected the Identity and Access Management Policy to determine that access to source code is managed through MFA to prevent unauthorized functionality, unintentional or malicious changes, and maintain the confidentiality of valuable intellectual property. Inspected the document displaying the list of GitHub users along with the MFA status enabled to determine that access to	No exceptions noted.

			source code is restricted to authorized personnel only.	
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.	Test information is appropriately selected, protected and managed to ensure relevance of testing and protection of operational information used for testing.	Inspected the Secure Development Policy to determine that test information is to be selected to ensure the reliability of test results and the confidentiality of the relevant operational information. inspected the GCP SQL instances to determine that test information is appropriately selected, and protected, and managed to ensure the relevance of testing and protection of operational information used for testing.	No exceptions noted.
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.	During coding and prior to code being operational, pull requests have to pass a set of checks before being merged to the master branch.	Inspected the Secure Development Policy to determine that during coding and before code is operational, pull requests have to pass a set of checks before being merged to the master branch Inspected the GitHub pull request and reviewer displaying request and approver names to determine that the pull requests are required to pass a set of checks before being merged to the master branch.	No exceptions noted.
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.	Development, testing and production environments are separated and secured.	Inspected the Secure Development Policy to determine that Development, testing, and production environments are separated and secured. Observed the GCP resources displaying separate repositories to determine that the company maintains separate development, testing, and production environments within the GCP infrastructure.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Backup copies of information, software and systems are maintained and regularly tested to enable recovery from loss of data or systems.	Inspected the Business Continuity Policy to determine that backup copies of information, software, and systems must be maintained and regularly tested following the agreed topic-specific policy on backup to enable recovery from loss of	No exceptions noted.

			data or systems. Inspected the log of backup and test performed to determine that the company maintains backup copies of information, software, and systems. Additionally, they are regularly tested to enable recovery from loss of data or systems.	
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Formal processes for acquisition, use, management and exit from cloud and SaaS services are established in accordance with the organization's information security requirements.	Inspected the Supplier Relationships Security Policy to determine that formal processes for acquisition, use, management, and exit from cloud and SaaS services were established following the organization's information security requirements. Inspected the list of vendors along with the owners and SOC 2 report links to determine that processes for acquisition, use, management, and exit from cloud services were in place.	No exceptions noted.