AARC 360

Assurance | Advisory
Risk | Compliance

Uplevel

Uplevel Inc.
Independent Service Auditor's Report on Controls at a Service Organization Relevant to Security and Confidentiality (SOC 2 Type 2)

November 16, 2021 through November 15, 2022

Table of Contents

SECTION 1 – INDEPENDENT SERVICE AUDITOR'S REPORT

Independent Service Auditor’s Report

To: Uplevel Inc.

Scope

We have examined Uplevel Inc.’s (‘Uplevel’, ‘the Company’, or ‘the Service Organization’) accompanying description of its Engineering Effectiveness Solution titled "Uplevel Inc.’s Description of its Engineering Effectiveness Solution" throughout the period November 16, 2021 through November 15, 2022, (description) based on the criteria for a description of a service organization’s system in DC section 200, *2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period November 16, 2021 through November 15, 2022, to provide reasonable assurance that Uplevel’s service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Uplevel uses Amazon Web Services (‘AWS’ or ‘the Subservice Organization’) to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Uplevel, to achieve Uplevel’s service commitments and system requirements based on the applicable trust services criteria. The description presents Uplevel’s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Uplevel’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 complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Uplevel, to achieve Uplevel’s service commitments and system requirements based on the applicable trust services criteria. The description presents Uplevel’s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Uplevel’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 controls.

Service Organization’s Responsibilities

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

Service Auditor's Responsibilities

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

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

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

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

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements related 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 users may consider important to meet their informational needs.

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

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

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section 4.

Opinion

In our opinion, in all material respects,

a. the description presents Uplevel's Engineering Effectiveness Solution that was designed and implemented throughout the period November 16, 2021 through November 15, 2022, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period November 16, 2021 through November 15, 2022, to provide reasonable assurance that Uplevel's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the Subservice Organization and user entities applied the complementary controls assumed in the design of Uplevel's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period November 16, 2021 through November 15, 2022, to provide reasonable assurance that Uplevel's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Uplevel's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Uplevel, user entities of Uplevel's Engineering Effectiveness Solution during some or all of the period November 16, 2021 through November 15, 2022, business partners of Uplevel subject to risks arising from interactions with the Engineering Effectiveness Solution, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the Service Organization
- How the Service Organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the Service Organization to achieve the Service Organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the Service Organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the Service Organization's service commitments and system requirements and how controls address those risks

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

AARC-360

Alpharetta, Georgia
January 9, 2023

SECTION 2 – ASSERTION OF UPLEVEL INC. MANAGEMENT

Assertion of Uplevel Inc. Management

January 9, 2023

We have prepared the accompanying description of Uplevel Inc.’s ('Uplevel’, ‘the Company’, or ‘the Service Organization’) Engineering Effectiveness Solution titled "Uplevel Inc.’s Description of its Engineering Effectiveness Solution" throughout the period November 16, 2021 through November 15, 2022, (description) based on the criteria for a description of a service organization’s system in DC section 200, *2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2® Report* (AICPA, Description Criteria) (description criteria). The description is intended to provide report users with information about the Engineering Effectiveness Solution that may be useful when assessing the risks arising from interactions with Uplevel’s system, particularly information about system controls that Uplevel 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 and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, (AICPA, Trust Services Criteria).

Uplevel uses Amazon Web Services (‘AWS’ or ‘the Subservice Organization’) to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Uplevel, to achieve Uplevel’s service commitments and system requirements based on the applicable trust services criteria. The description presents Uplevel’s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Uplevel’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 Uplevel, to achieve Uplevel’s service commitments and system requirements based on the applicable trust services criteria. The description presents Uplevel’s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Uplevel’s controls.

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

a. the description presents Uplevel’s Engineering Effectiveness Solution that was designed and implemented throughout the period November 16, 2021 through November 15, 2022, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period November 16, 2021 through November 15, 2022, to provide reasonable assurance that Uplevel’s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the Subservice Organization and user entities applied the complementary controls assumed in the design of Uplevel’s controls throughout that period.
c. the controls stated in the description operated effectively throughout the period November 16, 2021 through November 15, 2022, to provide reasonable assurance that Uplevel’s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Uplevel’s controls operated effectively throughout that period.

Joe Levy

Joe Levy
CEO
Uplevel Inc.

SECTION 3 – UPLEVEL INC.'S DESCRIPTION OF ITS ENGINEERING EFFECTIVENESS SOLUTION

Uplevel Inc.’s Description of Its Engineering Effectiveness Solution throughout the Period November 16, 2021 through November 15, 2022

Uplevel’s Services Overview

Company Founding

Uplevel was founded in June of 2018 to solve the problem of engineering effectiveness. Our mission is to free software engineers to do their best work. We envision a world where time for deep work actually happens, engineers aren’t stuck in meetings all day, code reviews don’t get stuck for days, and managers can understand what’s going on with their teams — because they have all the data.

The idea was born out of a hackathon at Madrona Venture Labs. Dave Matthews (product) who had the winning idea joined the founding team along with Madrona entrepreneur in residence David Youssefnia (strategy). Joe Levy (CEO) and Ravs Kaur (CTO) joined the team shortly after.

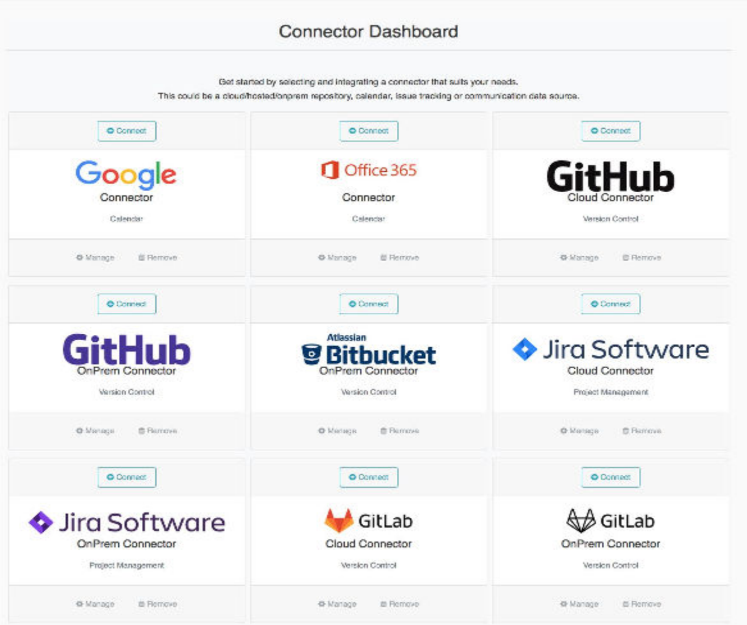
The company graduated from Madrona Venture Labs in summer of 2019 and has raised $7.5M in seed funding from Madrona, Norwest Venture Partners and Voyager Capital.

Product Overview

Uplevel is an engineering effectiveness platform that elevates engineers with ML data-driven insights, so their teams are empowered to do their best work.

Uplevel analyzes daily data from messaging tools like Slack, collaboration tools like Jira, calendar tools like Office 365, and code repository tools like GitHub to provide teams with a holistic view and actionable insights to make engineering teams work more effectively.

We offer dashboards for all levels of the organization - from the C-suite down to individual contributors, so that everyone in an organization has the data they need to do their best work.



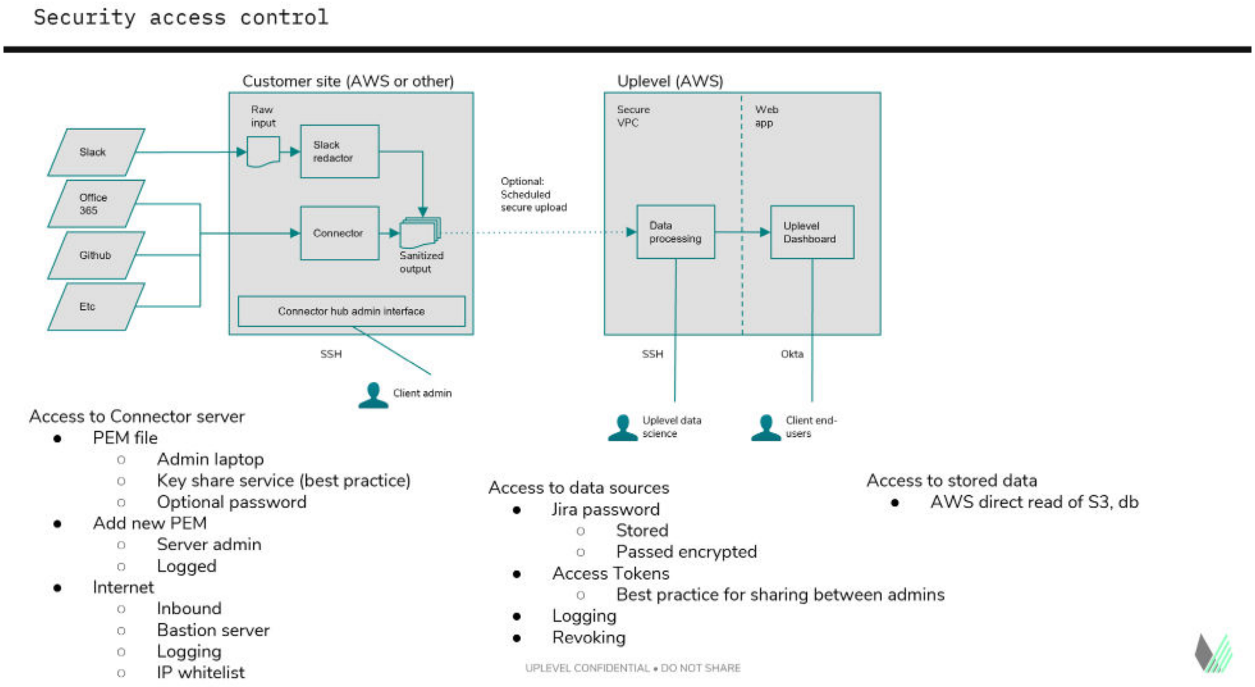
Connector Dashboard

Get started by selecting and integrating a connector that suits your needs.
This could be a cloud/hosted/onprem repository, calendar, issue tracking or communication data source.

Key benefits:

- Execution risk detection: Gain visibility into cross team dependencies, follow best practices, and understand team bandwidth and resources.
- Focus time protection: Reduce context switching, manage meetings and disruptions, and make deep work a team event so everyone can focus on high impact work.
- Manager development and team engagement: Enables data-driven conversations, makes 1:1s more productive, and creates healthy teamwork habits.

Principal Service Commitments and System Requirements



Security access control

Access to Connector server

- PEM file
  - Admin laptop
  - Key share service (best practice)
  - Optional password
- Add new PEM
  - Server admin
  - Logged
- Internet
  - Inbound
  - Bastion server
  - Logging
  - IP whitelist

Access to data sources

- Jira password
  - Stored
  - Passed encrypted
- Access Tokens
  - Best practice for sharing between admins
- Logging
- Revoking

Access to stored data

- AWS direct read of S3, db

UPLEVEL CONFIDENTIAL • DO NOT SHARE

Uplevel designs its processes and procedures related to the engineering effectiveness platform to meet its objectives for its effectiveness management services.

Those objectives are based on the service commitments that Uplevel makes to user entities, the laws and regulations that govern the provision of MT services, and the financial, operational, and compliance requirements that Uplevel has established for the services.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the engineering effectiveness platform that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit.

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

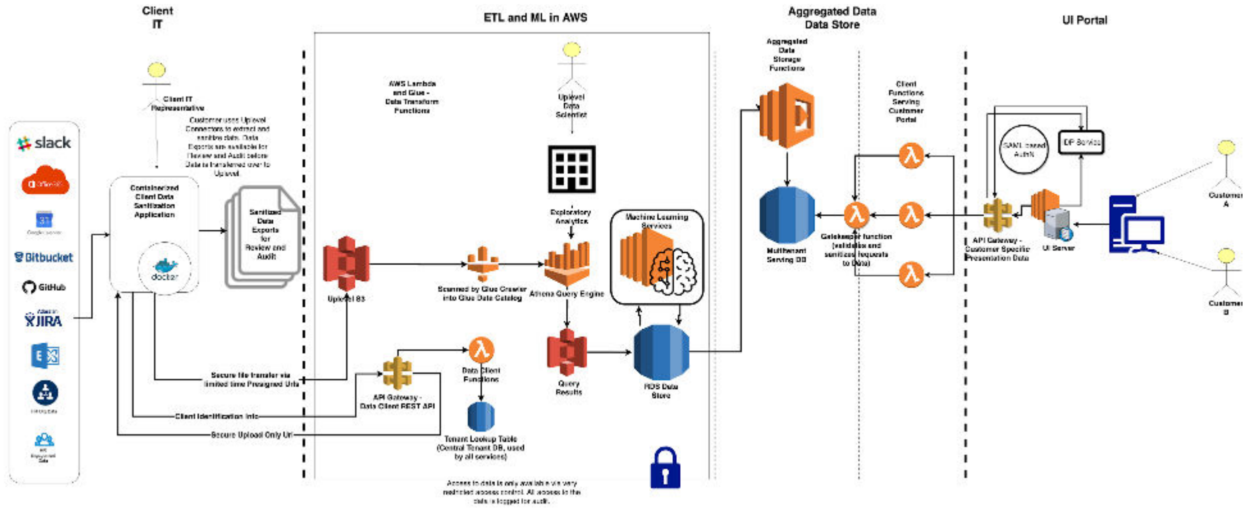
Components of the System Used to Provide the Services

Summary of Uplevel Data Architecture

Uplevel provides an analysis of employee collaboration behavior from sources such as Slack, Calendar, Org chart, etc., in order to give insights and coaching to Engineering teams.

Data is first collected on-prem in the client's environment, in order to provide full transparency and auditing of all data that is made available to Uplevel. Only data that is approved and sent to Uplevel is used, and no direct connection between Uplevel servers and client data sources such as Slack, Jira, GitHub is required.

The attached diagram details the flow of data from the client to Uplevel for processing, and end-user access to the derived reports in a manager facing dashboard:


Client IT
ETL and ML in AWS
Aggregated Data Data Store
UI Portal
Client IT Representative
Customer uses Uplevel Connectors to extract and sanitize data. Data Exports are available for Review and Audit before Data is transferred over to Uplevel
slack
Office 365
Google Calendar
Bitbucket
GitHub
JIRA
Containerized Client Data Sanitization Application
docker
Sanitized Data Exports for Review and Audit
Secure file transfer via limited time Presigned Urls
Client Identification Info
Secure Upload Only Url
Uplevel S3
AWS Lambda and Glue - Data Transform Functions
Uplevel Data Scientist
Exploratory Analytics
Scanned by Glue Crawler into Glue Data Catalog
Athena Query Engine
Machine Learning Services
API Gateway - Data Client REST API
Data Client Functions
Query Results
RDS Data Store
Tenant Lookup Table (Central Tenant DB, used by all services)
Access to data is only available via very restricted access control. All access to the data is logged for audit.
Aggregated Data Storage Functions
Multitenant Serving DB
Client Functions Serving Customer Portal
Gatekeeper function (validates and sanitizes requests to Data)
SAML based AuthN
DP Service
API Gateway - Customer Specific Presentation Data
UI Server
Custome A
Custome B

- Locked-down perimeter (including MFA for all users)
- IP whitelisted login access
- Data encrypted at rest (RDS, S3)
- No data stored on laptops
- Unnecessary services disabled, all access logged

Security Audit

On an annual basis, Uplevel will procure an audit by an independent third party, such as a SOC 2 audit (or audits of a substantially similar standard) of the facilities, networks and systems that are owned by Uplevel and used in connection with the provision of the Uplevel Services, as applicable. Uplevel will provide the results of annual audits to Customer within 30 days of completion, planned for Q4 2021.

Summary of Uplevel Data Sanitization

In order to calculate the building block metrics and provide our insights, Uplevel requires access to a sanitized copy of our customer's data. We realize this is super sensitive and have built a number of procedures and safeguards to ensure the data is safely and securely managed.
NOTE: this document describes how we functionally process and sanitize customer data. Separately, Uplevel has a number of security safeguards such as encryption, single sign-on, and 3rd party audits that we review and get approval with the customer's information security team. Uplevel also has many legal safeguards such as requirements for controlled access, background checks, and liability coverage that get incorporated into our customer contracts.
Design Tenets

- Uplevel does not collect anything without the customer being in full control. Practically, this means the customer has full control and the ability to audit the data before it is taken outside of your organization and delivered to Uplevel.
    - Uplevel does not connect directly to your systems from ours. For example, our services do not directly request access from Slack, Office 365, etc. to our servers.
    - Instead, we deliver tools which your IT department can run to download the data locally first, audit, and then upload a sanitized copy of the data to our servers.
- This critical intermediate step puts the customer in full control of the data being transferred. Our tools are provided as source code so you can know exactly what they are doing and even modify if desired. These tools can also be automated over time so that, once comfortable, there is minimal time impact on the customer's IT organization.

Sanitization of Slack

Uplevel takes a strong stance on redacting any potentially sensitive content from Slack before the data is transferred to Uplevel. Specifically:

- Public slack channels: Uplevel receives all data including the contents of the messages.
- Private slack channels and all DMs: Code provided by Uplevel and run by the customer (see above) will redact the contents of the message and leave only "meta" information. Meta information only contains the date/time, length, @mentions, emojis, sentiment score and channel name (private channels) or the participants (DMs). Uplevel specifically excludes the message contents. The message contents are deleted before the data is transferred to Uplevel.

Processing the full text of messages is only done for public channels and allows Uplevel to provide additional "building blocks" such as:

- Segmentation of work vs. non-work conversations (design issues vs. lunch location)
- Technical topic modeling (what technical topics are being discussed)
- Patterns of asking and answering questions (which teams are "go-to" for answers)

These building blocks often have strong correlations to engineering productivity. As a result, many customers have requested to provide Uplevel certain Slack channels that, while marked as private, are effectively public to that team and are valuable sources work information. These are commonly larger private channels of people discussing non-sensitive technical topics. We can discuss ways of ingesting these channels as well.

The table below is a summary of how the different types of Slack data are treated:

Type of Slack Data	Example of Raw Content	Content Sent to Uplevel
All Public Channels	"client_msg_id": "c869bc1e-f76c-4350-b1c9-648c6da1c8b1", "type": "message", "text": "That update to the algorithm is causing a build issue", "user": "U78RMUFT3", "ts": "1545082749.003200"	Same (no change)
All DMs and Private Channels	"client_msg_id": "c869bc1e-f76c-4350-b1c9-648c6da1c8b1", "type": "message", "text": "That update to the algorithm is causing a build issue", "user": "U78RMUFT3", "ts": "1545082749.003200"	"client_msg_id": "c869bc1e-f76c-4350-b1c9-648c6da1c8b1", "text": "", "ts": "1545082749.003200", "text_word_count": 10, "user": "U78RMUFT3", "text_length": 53, "text_at_mentions": [], "text_sentiment": 0.81, "type": "message", "text_emojis": []

Sanitization of Office 365 Calendar

Uplevel follows a similar logic for Office 365 Calendar as it does for Slack, treating most content like a DM or private channel message. Specifically:

- Uplevel does not look at any email. All email is ignored.
- Any meeting marked as private: Fully ignored and no details ever submitted to Uplevel.
- All meetings not marked as private: *Code provided by Uplevel and run by the customer (see above) will redact the body contents of all calendar items.*

Sanitization of Jira

For Jira, Uplevel uses the Jira Server REST API to collect data only from projects that are approved to be used for analytics by you. No modifications of any nature are made to the configuration or individual artifacts. While we may collect metadata about attachments that are part of an Issue, we do not look into or save attachments for analytics.

Similar to other data collected the customer has full visibility of what data was collected before it is sent over to Uplevel.

Sanitization of GitHub / Bitbucket

The metadata collected from source control repositories is intended to capture the patterns of work that occur in development projects. This includes the cadence of changes, collaboration between peers, and topics in issues and comments.

The actual source code of repositories and commits is not included.

A GitHub or Bitbucket admin can connect using OAuth to load the metadata for this analysis. Similar to other data collected, the customer has full visibility of what data was collected before it is sent over to Uplevel.

Uplevel has a staff of approximately 20 employees organized in the following functional areas:

- *Corporate.* Executives, senior operations staff, and company administrative support staff, such as legal, compliance, internal audit, training, contracting, accounting, finance, human resources, and transportation provider relations.
- *IT.* IT infrastructure, IT networking, IT system administration, software systems development and application support, information security, and IT operations personnel manage electronic interfaces and business implementation support and telecom.
    - The infrastructure, networking, and systems administration staff support Uplevel's IT infrastructure, which is used by the software. A systems administrator will deploy the releases of the software into the production environment.
    - The software development staff develops and maintains the custom software for Uplevel. This includes the supporting utilities, and the external websites that interact with Uplevel. The staff includes software developers, database administration, software quality assurance, and technical writers.
    - The information security staff supports Uplevel indirectly by monitoring internal and external security threats and maintaining current antivirus software.
    - The information security staff maintains the inventory of IT assets.

Relevant Aspects of the Control Environment, Risk Assessment Process, information and Communication, and Monitoring

The security category and applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Security criteria and controls designed, implemented, and operated to meet them ensure that the system is protected against unauthorized access.

The controls supporting the applicable trust services security criteria are included in section 4 of this report. Although the applicable trust services criteria and related controls are included in section 4, they are an integral part of Uplevel.

Control Environment

Management Philosophy

Uplevel's control environment reflects the philosophy of senior management concerning the importance of security of engineering data.

Uplevel's Security Review Board (SRB) meets quarterly and reports to the board annually.

The SRB, under the direction of the Uplevel board, oversees the security activities of Uplevel. The committee members are from each of the business lines. The committee is charged with establishing overall security policies and procedures for Uplevel. The importance of security is emphasized within Uplevel through the establishment and communication of policies and procedures and is supported by investment in resources and people to carry out the policies. In designing its controls, Uplevel has taken into consideration the relevance of controls to meet the relevant trust criteria.

Security Management

Uplevel has a dedicated information security team consisting of the Chief Information Security Officer who is a senior security specialist responsible for management of information security throughout the organization plus the CEO and the CTO. They hold positions on the Security Review Board and maintain security credentials and are required to annually sign and acknowledge their review of the information security policies. They are responsible for developing, maintaining, and enforcing Uplevel's information security policies.

As the information security team maintains security, it monitors known incidents and patches as well as results from recent vulnerability assessments and addresses necessary changes to the policies and procedures. Such changes can include a reclassification of data, a reassessment of risk, changes in incident response plans, and a verification of responsibilities for authorizing and monitoring accesses. Changes are reviewed and communicated during weekly IT maintenance meetings or through system alerts.

During annual security training and awareness programs, management ensures communication of the latest security policies as well as written job descriptions for security management.

Additionally, management is responsible for ensuring business associate agreements are current for third parties and for updating the annual IT risk assessment.

Security Policies

The following security policies and related processes are in place:

- Data classification and business impact assessment
- Selection, documentation, and implementation of security controls
- Assessment of security controls
- User access authorization and provisioning
- Removal of user access
- Monitoring of security controls
- Security management

Uplevel's Information Security policies and procedures contain formal usage guidelines that define appropriate IT resource usage to help ensure that information is utilized and maintained in a manner that ensures that such information remains secure. Access to the production applications is restricted to authorized personnel. Former employees' access to applications is removed promptly upon the employee leaving Uplevel.

Uplevel restricts access to system configurations, super-user functionality, master passwords, and security devices by implementing logical access controls. User access provisioning procedures exist to grant and revoke user access upon employee / contractor hire and termination respectively. Access reviews are conducted annually to help ensure that current application users were authorized to access the applications and that their access rights were appropriate. User passwords are defined and enforced in accordance with the Information Security policy. Access to the firewall is restricted to authorized personnel. Further, administrative access to configure firewall access control rules is restricted to authorized individuals.

Uplevel protects against unauthorized access to production system resources by restricting remote connectivity to authorized users. Administrator access is restricted to authorized users. Critical information system components require a separate password to gain access, and rights are limited to administrators.

Uplevel utilizes industry standard encryption techniques to protect user authentication information and the corresponding communication session transmitted over the Internet or other public networks. Transmission-level SSL security is implemented when information is being transmitted over public networks.

Personnel Security

Background checks are performed on all new employees, who are also required to review and acknowledge their receipt of relevant security policies. The new positions are supported by job descriptions. Once employed, employees are subject to Uplevel's procedures for accessing systems and sanctions for violating Uplevel's information security policy. Employees are instructed to report potential security incidents to the help desk.

Uplevel's business associate agreement instructs user entities and third-party service providers to notify their Uplevel if they become aware of a possible security breach.

Change Management

Uplevel has a formalized change management process in place, which requires identification and recording of significant changes, assessment of risk and potential effect of such changes, approval of proposed changes, and testing of changes to verify operational functionality. 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. The IT management team meets regularly to review and schedule changes to the IT environment.

Emergency changes follow the formalized change management process, but at an accelerated timeline. Prior to initiating an emergency change, necessary approvals are obtained and documented.

Changes to infrastructure and software are developed and tested in a separate development or test environment before implementation. Additionally, developers do not have the ability to migrate changes into production environments without review.

Uplevel has a formalized security and systems development methodology that includes project planning, design, testing, implementation, maintenance, and disposal or decommissioning.

Uplevel uses a standardized server build checklist to help secure its servers, and it conducts monthly vulnerability assessments to identify potential system vulnerabilities. Patches are applied regularly in accordance with Uplevel's patch management process.

Uplevel has implemented change control procedures to help ensure the integrity of network devices, programs, and data. Change control procedures are necessary to establish adequate testing and recovery plans. Change management processes include properly authorizing, testing, approving, implementing, documenting, and maintaining system applications and security patches. The Information Technology Department (ITD) oversees the change management process to help ensure that all changes are authorized, tested, and approved prior to migration to the production environment.

The ITD is responsible and accountable for:

- Oversight of the Change Management Policy
- Authorization of work performed by third-party providers
- Monitoring the status of all system testing and implementation
- Oversight of the implementation of appropriate controls for new network applications, servers, and related equipment
- Oversight of fundamental change requests to the company's network infrastructure
- Ensuring all users receive appropriate training on changes

Change Management Guidelines

The Change Management Policy covers the following types of system configurations:

- Installation of new computers
- Installation of new network software applications/parameter changes
- New or updated Microsoft Windows operating systems
- Installation of non-Microsoft Windows-based routine security patches and updates
- New policies, procedures, and standards
- New regulations
- New network devices
- Changes to the Wide Area Network (WAN) and VPN network
- Ensuring that all network systems are properly backed up prior to the implementation of significant system updates or changes
- Testing LAN/WAN network configuration changes prior to introduction into the production environment

Systems Operations

Incident reporting and incident response are documented within the Incident Response Policy and Procedures and tracked by management until resolution. Employees are encouraged to bring forth any concerns over information security. If employees have concerns over a potential loss of data or breach, they are to notify Uplevel's Management immediately and the Incident Response Policy and Procedures are followed.

For the purpose of protecting and securing vital data and related business information, Uplevel has configured backups to run on a daily basis. Backups are monitored for failure using an automated system. Critical systems are backed to the cloud, protecting the data from localized incidents and disasters.

Uplevel protects its systems against infection by computer viruses, malicious code, and unauthorized software by implementing antivirus software. Antivirus software is installed on workstations and laptops to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. Virus signatures/definitions are automatically updated on a defined schedule.

System Monitoring

The security administration team uses a variety of security utilities to identify and detect possible security threats and incidents. These utilities include, but are not limited to, firewall notifications, intrusion detection system (IDS) or intrusion prevention system (IPS) alerts, vulnerability assessment reports, and operating system event logs. These alerts and notifications are reviewed daily by the security administration team using a security incident and event monitoring (SIEM) product. Additionally, the security administration team has developed and will review the following SIEM reports:

- Failed object level access
- Daily IDS or IPS attacks
- Critical IDS or IPS alerts
- Devices not reporting in the past 24 hours
- Failed login detail
- Firewall configuration changes
- Windows policy changes
- Windows system shutdowns and restarts
- Security events requiring further investigation are tracked using a help desk ticket and monitored until resolved

Data Backup and Recovery

Uplevel uses data replication and tapes to back up its data files and software. Access to backup devices, scheduling utilities, systems, and media is restricted to authorized personnel.

System Account Management

Uplevel has implemented role-based security to limit and control access. Employees are granted logical access to in-scope systems based on documented approvals by appropriate management personnel. The ability to create or modify user access accounts and user access privileges is limited to authorized personnel. User access is reviewed quarterly to verify whether individuals' access is necessary for their job functions and to identify the existence of inappropriate accounts.

The human resources department provides IT personnel with an employee termination report on a timely basis. IT reconciles the termination report with current access privileges to determine if access has been appropriately removed or disabled. Dormant network accounts are disabled after 90 days of inactivity, and dormant accounts are disabled after 45 days of inactivity.

Administrative access to Active Directory and databases is restricted to authorized employees.

Unique user identification numbers, names, and passwords are required to authenticate all users Password parameters consist of the following:

- Passwords contain a minimum of six characters, including one non-alphanumeric character.
- Passwords expire every 120 days for non-privileged accounts and 60 days for privileged accounts.
- Log-on sessions are terminated after three failed log-on attempts.
- Users cannot reuse the last three passwords (five passwords for privileged accounts).

Risk Mitigation

Uplevel has implemented risk mitigation strategies to reduce the organizations exposure to the risk.

Vendor Management

Uplevel monitors commitments provided by their vendors and where applicable independent auditor's reports from the third parties are obtained as an aspect of monitoring vendor SLAs. Uplevel has assigned senior personnel to assess compliance by vendors.

Insurance coverage

Inadequate insurance coverage could result in severe financial loss for Uplevel as well as loss of reputation and increased liability**.** The overall integrity of Uplevel could be compromised by such inadequate coverage. Uplevel has arranged for insurance coverage by reputable institutions in order to complement an effective system of controls.

Risk Assessment Process

Uplevel regularly reviews the risks that may threaten the achievement of its service commitments and system requirements related to security and confidentiality based on the applicable trust services criteria set forth in TSP section 100, 2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

The information security team assesses security risks on an ongoing basis. This is done through regular management meetings with IT personnel, reviewing and acting upon security event logs, performing vulnerability assessments, and conducting a formal annual IT risk assessment in conjunction with the company-wide risk assessment.

An IT strategic plan is developed annually by the CTO and is communicated to and approved by senior management and the Security Steering Committee. As part of this plan, strategic IT risks affecting the organization and recommended courses of action are identified and discussed.

Senior management, as part of its annual information security policy review, considers developments in technology and the impact of applicable laws and regulations on Uplevel’s security policies.

Changes in security threats and risks are reviewed by Uplevel, and updates to existing control activities and information security policies are performed as necessary.

Uplevel performs risk assessments to determine the adequacy and implementation of technical, operational, and security controls to mitigate the potential risks and vulnerabilities to the security of information. Uplevel has completed a risk assessment which identifies threats to its information and assets. This risk assessment is reviewed and updated periodically to include new assets, threats, and controls. Security, Availability, Processing Integrity, Confidentiality, and Privacy processes and procedures are revised by Uplevel management based on the assessed threats identified during the risk assessment process. Uplevel’ system security is periodically evaluated and compared with the procedures defined in the Information Security policies and procedures.

Information and Communication Systems

Uplevel has an information security policy to help ensure that employees understand their individual roles and responsibilities concerning processing and controls to ensure significant events are communicated in a timely manner. These include formal and informal training programs and the use of email to communicate time-sensitive information and processes for security and system availability purposes that notify key personnel in the event of problems.

Uplevel uses checklists to help facilitate the upload of user information, such as encounter data, trip report, and client complaints, to the appropriate repository (for example, a portal or secure FTP folder) in accordance with the user’s instructions.

Uplevel has a documented system description addressing the system boundaries that are made available to authorized users. Security obligations and commitments to clients are outlined in service level agreements. Individual client contracts also define how client-specific confidential information is authorized and restricted. Procedures regarding how confidential information is used, shared, and if authorized, provided to third parties, are also described in individual client contracts and relevant information security policies. Vendors agree to use appropriate safeguards to prevent disclosure of confidential information. Customer contracts, service level agreements, and vendor contracts are negotiated before performance or receipt of service and formally signed off on by management.

Formally documented Incident Response Program policy exists that defines the process whereby Uplevel will report security incidents and breaches. The policy addresses breach notification and escalation processes. Changes that may affect system security are communicated in writing to affected customers under the provisions of the service level agreements. External users have the ability to communicate security incidents or concerns to Uplevel.

Monitoring Controls

In addition to the daily oversight, monthly vulnerability assessments, and use of SIEM, management provides further security monitoring through the internal audit department, which performs periodic audits to include information security assessments.

Uplevel has an Incident Response Program policy to identify, report, and act upon system security breaches and other incidents. Incidents are initially documented and escalated as needed based on severity.
Incident response is broken down into six (6) main categories which include the following:

- Identification of the Incident
- Assessment of the Incident
- Containing and Controlling the Incident
- Notification of Federal Regulators and Law Enforcement
- Customer Notification
- Post-Incident Assessment

Uplevel uses an industry standard centrally-managed monitoring software that is configured to monitor server events, data backup status, and anti-virus statistics. All relevant events are logged, and thresholds are defined to alert administrators of significant events.

Changes to the System During the Period

There were no changes that are likely to affect report users' understanding of how the Engineering Effectiveness Platform is used to provide the service during the period from November 16, 2021 through November 15, 2022.

Complementary Subservice Organization Controls (CSOCs)

Uplevel utilizes a subservice organization to perform certain key operating functions for the Uplevel software. The accompanying description of controls includes only those policies, procedures, and controls at Uplevel and does not extend to policies, procedures, and controls at the Subservice Organization.

Uplevel uses the following subservice organization to implement portions of its Engineering Effectiveness Solution System and the following tables present the applicable Trust Services Criteria that are intended to be met by controls at each subservice provider, alone or in combination with controls at Uplevel, and the types of controls expected to be implemented at the subservice provider meet those criteria.

Subservice Organization

Uplevel uses AWS for its cloud hosting services, making use of many of its managed services for the network and system infrastructure required to support the Engineering Effectiveness Solution service. AWS is also responsible for providing physical and environmental security controls, administration of their infrastructure and for reporting any logical or physical security incidents. AWS undergoes its own rigorous audit processes, including an annual SOC 2 audit, which is examined annually by Uplevel to review the appropriateness of scope, impact of exceptions, and applicable complementary user entity controls.

The following table outlines the Trust Service Criteria and AWS' related control for the monitoring area:

Complementary Subservice Organization Controls (CSOCs)	Related Criteria
AWS is responsible for restricting logical and physical access to data center facilities, back up media, and other system components including firewalls, routers, and servers	CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.5, CC6.6, CC6.7, CC9.2
AWS is responsible for implementing measures to prevent or mitigate threats consistent with the risk assessment.	CC3.1, CC9.2
AWS is responsible for maintaining segregation of Uplevel's environment(s) from other AWS clients.	CC6.1, CC6.6

Complementary Subservice Organization Controls (CSOCs)	Related Criteria
AWS is responsible for the management of any third-party vendors with access to customer environments.	C1.2, C1.3, C1.4

Trust Services Criteria and Related Controls

Although the trust services criteria and related controls are presented in Section 4, 'Trust Services Criteria of Security and Confidentiality, Applicable Criteria, Related Controls, and Tests of Controls,' they are an integral part of Uplevel's system description.

Complementary User Entity Controls

Certain criteria specified in the description can be achieved only if complementary user entity controls contemplated in the design of Uplevel's controls are suitably designed and operating effectively, along with related controls at Uplevel. Complementary User Entity Controls are specific user controls or issues each Uplevel client organization should implement or address respectively in order to achieve the applicable criteria identified in this report. These considerations are not necessarily a comprehensive list of all internal controls that should be employed by user entities, nor do they represent procedures that may be necessary in all circumstances.

1. User entities and subservice organizations are responsible for understanding and complying with their contractual obligations to Uplevel.
2. User entities are responsible for notifying Uplevel of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Uplevel's services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Uplevel's services.
6. User entities are responsible for ensuring that user IDs and passwords are assigned to only authorized individuals.
7. User entities are responsible for ensuring that data submitted to Uplevel is complete, accurate, and timely.
8. Standards and processes are in place for user entities to follow for security and industry guidelines.

SECTION 4 – TRUST SERVICES CRITERIA CATEGORY OF SECURITY AND CONFIDENTIALITY, APPLICABLE CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

Guidance Regarding Information Provided by the Service Auditor

AARC-360's examination of the controls of Uplevel was limited to the Trust Services Criteria Categories of Security and Confidentiality and related criteria and controls specified by the management of Uplevel and did not encompass all aspects of Uplevel's operations or operations at the Subservice Organization and User Entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) the Statement on Standards for Attestation Engagements No. 18 (AT-C section 205, *Examination Engagements*).

Our examination of the control activities was performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	AARC-360 made inquiries of Uplevel personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	AARC-360 observed application of the control activities by client personnel.
Inspection	AARC-360 inspected among other items, documents, reports, or electronic files that contain evidence of the performance of the controls, such as system log files.
Re-performance	AARC-360 independently re-performed (where applicable) procedures or controls that were originally performed by Uplevel as part of its internal control.

In determining whether the report meets the users' objectives, the users should perform the following procedures:

- Understand the aspects of Uplevel's controls that may affect the processing of the User Entity's transactions;
- Understand the flow of significant transactions through Uplevel; and
- Determine whether the criteria are relevant to the user's requirements.

CC1.0 – Common Criteria Related to Control Environment

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The strategic direction and oversight of the Company is conducted by senior management and the Board of Directors.	Inspected the Company organizational chart, listing of board of directors, and a sample of Board of Directors, and monthly management meeting minutes to determine that the strategic direction and oversight of the Company was conducted by senior management and the Board of Directors.	No deviations noted.
		An employee handbook is documented by the Company and distributed to new employees.	Inspected the employee handbook and handbook acknowledgements for a sample of new hires to determine that an employee handbook was documented by the Company and distributed to new employees.	No deviations noted.
		Procedures are in place for employee evaluations to be performed against individual objectives derived from the Company's goals, established standards, and specific job responsibilities.	Inspected the employee handbook and the performance reviews for a sample of current employees to determine that procedures were in place for employee evaluations to be performed against individual objectives derived from the Company's goals, established standards, and specific job responsibilities.	No deviations noted.
		The Company policies include disciplinary actions and termination as potential sanctions for employee misconduct.	Inspected the employee handbook to determine that the Company policies included disciplinary actions and termination as potential sanctions for employee misconduct.	This control is suitably designed; however, there were no instances of employee disciplinary actions during the review period to test the operating effectiveness of the control. No deviations noted.

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
		Forms, documents, and acknowledgements are utilized throughout the Company's vendor employee new hire process.	Inspected the onboarding checklist to determine that forms, documents, and acknowledgements were utilized throughout the Company's contractor onboarding process.	This control is suitably designed, however, there was no instance of a contractor being onboarded during the review period to test the operating effectiveness of the control. No deviations noted.
CC1.2	The Board of Directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The Company's Board of Directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations.	Inspected the Company organizational chart, listing of board of directors, and a sample of monthly Board of Directors meeting minutes to determine that the Company's Board of Directors identified and accepted its oversight responsibilities in relation to established requirements and expectations.	No deviations noted.
		The Board of Directors defines and documents the skills and expertise among its members.	Inspected the Board of Directors biographies to determine that the Board of Directors defined and documented evaluated the skills and expertise among its members.	No deviations noted.
		The Company's Board of Directors have sufficient members who are independent from management and objective in evaluations and decision making.	Inspected the Board of Directors listing and the organizational chart to determine that the Company's Board of Directors had sufficient members who were independent from management and objective in evaluations and decision making.	No deviations noted.
		The Board of Directors supplements its expertise relevant to security and confidentiality, as needed, through the use of a subcommittee or consultants.	Inspected the statement of work for a subject matter resource to determine that the Board of Directors supplemented its expertise relevant to security and confidentiality as needed, through the use of a subcommittee or consultants.	No deviations noted.

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Company organizational charts are in place to communicate the defined key areas of authority, responsibility and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system. These charts are communicated to employees and updated as needed.	Inspected the Company organizational chart and shared file location to determine that Company organizational charts were in place to communicate the defined key areas of authority, responsibility and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system, and that these charts were communicated to employees and updated as needed.	No deviations noted.
		Roles and responsibilities are defined in written job descriptions and communicated to managers and their supervisors taking into consideration segregation of duties as necessary at the various levels of the Company and requirements relevant to security and confidentiality.	Inspected a sample of job descriptions to determine that roles and responsibilities were defined in written job descriptions and communicated to managers and their supervisors taking into consideration segregation of duties as necessary at the various levels of the Company and requirements relevant to security and confidentiality.	No deviations noted.
		The Company has assigned senior level executives the responsibility of handling their primary vendors.	Inspected the CEO job description to determine that the Company had assigned senior level executives the responsibility of handling their primary vendors.	No deviations noted.
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 active employees' abilities to meet these requirements are evaluated as part of the performance review process.	Inspected a sample of job descriptions, the employee handbook, and performance reviews for a sample of current employees to determine that job requirements were documented in the job descriptions, and active employees' abilities met these requirements were evaluated as part of the performance review process.	No deviations noted.

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
		New employee hiring procedures are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the employee checklists.	Inspected the interview plan and resumes for a sample of new hires to determine that new employee hiring procedures were in place to guide the hiring process and included verification that candidates possessed the required qualifications to perform the duties as outlined in the employee checklists.	No deviations noted.
		Procedures exist in the form of training to reflect expectations of competence necessary to support the achievement of objectives.	Inspected the employee handbook, training policy, training slides, and training records for a sample of current employees to determine that procedures existed in the form of training to reflect expectations of competence necessary to support the achievement of objectives.	No deviations noted.
		Uplevel has developed contingency plans for assignments of responsibility important for internal control.	Inspected the succession plan to determine that Uplevel had developed contingency plans for assignments of responsibility important for internal control.	No deviations noted.
		Uplevel performs background checks on potential new hires.	Inspected the background checks for a sample of new hires to determine that Uplevel performed background checks on potential new hires.	One (1) out of a sample of five (5) new hires did not have a completed background check at the time of hire. We expanded our testing by an additional five (5) new hires and noted no further deviations.

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Employee evaluations are performed against individual objectives derived from the Company’s goals, established standards, and specific job responsibilities.	Inspected the employee handbook and performance reviews for a sample of current employees to determine that employee evaluations were performed against individual objectives derived from the Company’s goals, established standards, and specific job responsibilities.	No deviations noted.
		The Company's management establishes performance measures for responsibilities at all levels of the Company, reflecting appropriate dimensions of performance and expected standards of conduct.	Inspected the internal bonus report to determine that the Company's management established performance measures for responsibilities at all levels of the Company, reflecting appropriate dimensions of performance and expected standards of conduct.	No deviations noted.

CC2.0 – Common Criteria Related to Communication and Information

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The Company had documented information security policies and procedures.	Inspected the policies and procedures to determine that the Company had documented information security policies and procedures.	No deviations noted.
		The information system captures, processes, and maintains the quality of internal and external sources of data throughout the year.	Inquired of CISO regarding system architecture and inspected the policies and procedures, systems diagram, a sample of Board of Directors and management meeting minutes, and risk assessment to determine that the information system captured, processed, and maintained the quality of internal and external sources of data throughout the year.	No deviations noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Policy and procedures documents for significant processes are available on the Company's shared internal drive.	Inspected the shared network drive to determine that policy and procedures documents for significant processes were available on the Company's shared internal drive.	No deviations noted.
		Management's communication sets the tone and direction for the entire Company.	Inspected the Company organizational chart, listing of board of directors, and a sample of Board of Directors and management meeting minutes to determine that management's communication set the tone and direction for the entire Company.	No deviations noted.
		Employees can communicate confidential information when normal channels are not effective.	Inspected the internal message board to determine that employees could communicate confidential information when normal channels were not effective.	No deviations noted.
		The Company has documented incident response policies and procedures.	Inspected Incident Management Policy and Security Incident and Breach Notification Policy and a sample of incident tickets to determine that the Company had documented incident response policies and procedures.	No deviations noted.

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
		System changes are communicated to internal users.	Inspected a sample of change notifications to internal users to determine that system changes were communicated to internal users.	No deviations noted.
		The Company provides security training to employees to communicate security policies and procedures.	Inspected the employee handbook, training policy, training slides, and training records for a sample of current employees to determine that the Company provided security training to employees to communicate security policies and procedures.	No deviations noted.
		The Company has prepared an objective description of the system and its boundaries and communicates such description to authorized users.	Inquired of the CISO regarding system diagrams and inspected the system diagrams, architecture descriptions, and a sample of job descriptions to determine that the Company had prepared an objective description of the system and its boundaries and communicated such description to authorized users.	No deviations noted.
		The Company's security policies define and communicate information security responsibilities for all personnel.	Inquired of the CISO regarding internal system changes and inspected change notification to internal users for a sample of system changes to determine that the Company's security policies defined and communicated information security responsibilities for all personnel.	No deviations noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Client service agreements include documented external user responsibilities.	Inspected the customer services agreements for a sample of new customers to determine that customer's service agreements included documented external user responsibilities.	No deviations noted.
		Open communication channels allow input from customers providing management and the Board of Directors with relevant information.	Inspected the external communication channels to determine that open communication channels allowed input from customers providing management and the Board of Directors with relevant information.	No deviations noted.

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
		Relevant information resulting from assessments conducted by external parties is communicated to management and Board of Directors.	Inspected the Security Board meeting minutes to determine that relevant information resulting from assessments conducted by external parties was communicated to management and the Board of Directors.	No deviations noted.
		Changes that may affect system confidentiality are communicated in writing to affected customers.	Inspected the external communication channels and a sample of external communications to determine that changes that may affect system confidentiality were communicated in writing to affected customers.	No deviations noted.
		Clients are provided guidance in regard to best practices when utilizing the Company's services.	Inspected the system diagrams to determine that clients were provided guidance in regard to best practices when utilizing the Company's services.	No deviations noted.
		The Company communicates its system objectives to appropriate external users.	Inspected the Company website and the system diagrams and architecture descriptions to determine that the Company communicated its system objectives to appropriate external users.	No deviations noted.
		External users are provided with escalation procedures for reporting security incidents such as reporting failures, incidents, concerns, and other complaints.	Inspected the internal message board and the external communication channels to determine that external users were provided escalation procedures for reporting security incidents such as reporting failures, incidents, concerns, and other complaints.	No deviations noted.

CC3.0 – Common Criteria Related to Risk Assessment

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	**Operations Objectives**		
		The Company has defined a formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the information security policy and the risk assessment to determine that the Company had defined a formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No deviations noted.
		Company management considers the acceptable levels of risk relative to the achievement of operations objectives.	Inspected the Information Security Policy and risk assessment to determine that Company management considered the acceptable levels of risk relative to the achievement of operations objectives.	No deviations noted.
		The Company reflects the desired level of operations and financial performance for the Company within operations objectives.	Inspected the operational objectives to determine that the Company reflected the desired level of operations and financial performance for the Company within operations objectives.	No deviations noted.
		The Company's management uses operational objectives as a basis for allocating resources needed to attain desired operational performance.	Inspected the operational performance to determine that the Company's management used operational objectives as a basis for allocating resources needed to attain desired operational performance.	No deviations 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.	Risks to the Company are evaluated and mitigation procedures are implemented based on risk evaluations.	Inspected the risk assessment to determine that risks to the Company were evaluated and mitigation procedures were implemented based on risk evaluations.	No deviations noted.
		Risk identification considers both internal and external factors and their impact on the achievement of objectives.	Inspected the risk assessment to determine that risk identification considered both internal and external factors and their impact on the achievement of objectives.	No deviations noted.

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
		The Company risk management strategy involves appropriate levels of management.	Inspected Board of Directors meeting minutes to determine that the Company risk management strategy involved appropriate levels of management.	No deviations noted.
		Identified risks are analyzed through a process that includes estimating the potential significance of the risk.	Inspected the risk assessment to determine that identified risks were analyzed through a process that included estimating the potential significance of the risk.	No deviations noted.
		The risk assessment policy includes considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk.	Inspected the information security policy and the risk assessment to determine that the risk assessment policy included considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk.	No deviations noted.
		The Company's risk identification and assessment process includes (1) identifying information assets, including physical devices and systems, virtual devices, software, data and data flows, external information systems, and Company roles; (2) assessing the criticality of those information assets; (3) identifying the threats to the assets from intentional (including malicious) and unintentional acts and environmental events; and (4) identifying the vulnerabilities of the identified assets.	Inspected the risk assessment to determine that the Company's risk identification and assessment process included (1) identifying information assets, including physical devices and systems, virtual devices, software, data and data flows, external information systems, and Company roles; (2) assessing the criticality of those information assets; (3) identifying the threats to the assets from intentional (including malicious) and unintentional acts and environmental events; and (4) identifying the vulnerabilities of the identified assets.	No deviations noted.
		The Company's risk assessment process includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and vulnerabilities arising from business partners, customers, and others with access to the Company's information systems.	Inspected the risk assessment to determine that the Company's risk assessment process included the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and vulnerabilities arising from business partners, customers, and others with access to the Company's information systems.	No deviations noted.

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
		The Company's risk identification and assessment process includes (1) determining the criticality of identified assets in meeting objectives; (2) assessing the impact of identified threats and vulnerabilities in meeting objectives; (3) assessing the likelihood of identified threats; and (4) determining the risk associated with assets based on asset criticality, threat impact, and likelihood.	Inspected the risk assessment to determine that the Company's risk identification and assessment process included (1) determining the criticality of identified assets in meeting objectives; (2) assessing the impact of identified threats and vulnerabilities in meeting objectives; (3) assessing the likelihood of identified threats; and (4) determining the risk associated with assets based on asset criticality, threat impact, and likelihood.	No deviations noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Management has considered the various types of fraud that could affect the Company.	Inspected the Information Security Policy and fraud assessment to determine that management had considered the various types of fraud that could affect the Company.	No deviations noted.
		The Company assesses incentives and pressures as part of the evaluation of fraud.	Inspected the fraud assessment to determine that the Company assessed incentives and pressures as part of the evaluation of fraud.	No deviations noted.
		The Company assesses attitudes and rationalizations to justify inappropriate actions.	Inspected the fraud assessment to determine that the Company assessed attitudes and rationalizations to justify inappropriate actions.	No deviations noted.
		The Company considers the risks related to the use of IT and Access to information.	Inspected the risk assessment to determine that the Company considered the risks related to the use of IT and Access to information.	No deviations noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The risk identification process considers changes to the economic physical environment in which the Company operates.	Inspected the business risk and business impact assessment to determine that the risk identification process considered changes to the economic and physical environment in which the Company operated.	No deviations noted.
		The Company assesses changes in the business model while considering the potential impacts of new business lines.	Inspected the business risk and business impact assessment to determine that the Company assessed changes in the business model while considering the potential impacts of new business lines.	No deviations noted.

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
		The Company assesses changes in leadership based on the management attitudes and philosophies.	Inspected the business risk and business impact assessment and succession plan to determine that the Company assessed changes in leadership based on the management attitudes and philosophies.	No deviations noted.
		Risk assessment assesses changes in the systems and their potential impact.	Inspected the risk assessment to determine that the risk assessment assessed changes in the systems and their potential impact.	No deviations noted.
		The Company monitors services provided by their vendors, and where applicable, independent auditor's reports from the third parties are obtained as an aspect of monitoring vendor SLAs.	Inquired of the CISO regarding vendor management and inspected the vendor risk assessment to determine that the Company monitored services provided by their vendors, and where applicable, independent auditor's reports from the third parties were obtained as an aspect of monitoring vendor SLAs.	No deviations noted.

CC4.0 – Common Criteria Related to Monitoring Activities

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Management includes a balance of ongoing and separate evaluations.	Inspected the Information Security Policy, risk assessment, the vulnerabilities dashboard, the monitoring dashboard, and the penetration test reports to determine that management included a balance of ongoing and separate evaluations.	No deviations noted.
		Management takes into consideration the changes in business and IT environment during the evaluation of controls.	Inspected the business risk and business impact assessment to determine that management took into consideration the changes in business and IT environment during the evaluation of controls.	No deviations noted.
		Senior Management possess adequate knowledge and skills to perform the control evaluation accurately.	Inspected the Board of Directors biographies and a sample of job descriptions to determine senior management possessed adequate knowledge and skills to perform the control evaluation accurately.	No deviations noted.
		The feedback received from the control evaluations is integrated into the business and IT processes on an ongoing basis and subject to the changing business conditions.	Inquired of the CISO regarding lessons learned and inspected the Disaster Recovery Plan, risk assessment, the vendor risk assessments, and the business risk and business impact assessment to determine that the feedback received from the control evaluations was integrated into the business and IT processes on an ongoing basis and subject to the changing business conditions.	No deviations noted.
		A penetration test is performed annually to meet changing commitments and requirements.	Inspected the annual penetration test to determine that a penetration test was performed annually to meet changing commitments and requirements.	No deviations noted.

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
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.	The Company assesses results of the periodic and separate control evaluations regularly and reviews the corrective actions in regard to the identified deficiencies.	Inspected a sample of management meeting minutes to determine that the Company assessed results of the periodic and separate control evaluations regularly and reviewed the corrective actions in regard to the identified deficiencies.	No deviations noted.
		The Company identifies deficiencies to the respective parties to take corrective actions and to the senior management as needed.	Inspected the Incident Management Policy, the Security Incident and Breach Notification Policy, and a sample of closed incident tickets to determine that the Company identified deficiencies to the respective parties to take corrective actions and to the senior management as needed.	No deviations noted.

CC5.0 – Common Criteria Related to Control Activities

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	A risk management and risk assessment strategy are in place to help ensure that controls are developed and deployed adequately to mitigate risks.	Inspected Board of Directors meeting minutes and the risk assessment to determine that a risk management and risk assessment strategy were in place to help ensure that controls are developed and deployed adequately to mitigate risks.	No deviations noted.
		The risk assessment is regularly reviewed and reflects the business and its processes accurately with specific controls addressing Company-specific threats.	Inspected the Information Security Policy and the risk assessment to determine that the risk assessment was regularly reviewed and reflected the business and its processes accurately with specific controls addressing Company-specific threats.	No deviations noted.
		Management selects the business processes for applying the control activities based on their relevance.	Inspected the Information Security Policy and the risk register to determine that management selected the business processes for applying the control activities based on their relevance.	No deviations noted.
		The Company applies a mix of control activity types including manual and automated, preventive and detective to mitigate the risks.	Inspected the business risk and business impact assessment and risk register to determine that the Company applied a mix of control activity types including manual and automated, preventive and detective to mitigate the risks.	No deviations noted.
		The risk assessment defines controls according to individual or departmental responsibility.	Inspected the risk assessment to determine that the risk assessment defined controls according to individual or departmental responsibility.	No deviations noted.
		Segregation of duties is present for incompatible roles, and where not practical, management selects and develops alternative control activities.	Inspected a sample of job descriptions and the organizational chart to determine that segregation of duties was present for incompatible roles, and where not practical, management selected and developed alternative control activities.	No deviations noted.

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	As part of the IT strategic plan, strategic IT risks affecting the Company and recommended courses of action are identified and discussed.	Inquired of the CISO regarding separate evaluations and inspected the Information Security Policy, business risk and business impact assessment, the vulnerabilities dashboard, the monitoring dashboard, and the penetration test reports to determine that as part of the IT strategic plan, strategic IT risks affecting the Company and recommended courses of action were identified and discussed.	No deviations noted.
		Management has implemented role-based access policies which restricts user access to systems and resources based on job responsibilities.	Inspected the Information Security Policy and the applications user listings to determine that management had implemented role-based access policies which restricted user access to systems and resources based on job responsibilities.	No deviations noted.
		The Company has control activities in place over the acquisition, development, and maintenance of current IT systems and its infrastructure to achieve management's objectives.	Inspected the Information Security Policy and a sample of infrastructure changes to determine that the Company had control activities in place over the acquisition, development, and maintenance of current IT systems and its infrastructure to achieve management's objectives.	No deviations noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Management implements control activities integrated with the business processes and employees' day-to-day activities through policies establishing what is expected and relevant procedures specifying actions.	Inspected policies and procedures to determine that management implemented control activities integrated with the business processes and employees' day-to-day activities through policies establishing what was expected and relevant procedures specifying actions.	No deviations noted.
		Management assigns ownership and accountability for control activities to management of the business unit or function in which the relevant risks reside.	Inspected a sample of job descriptions to determine that management assigned ownership and accountability for control activities to management of the business unit or function in which the relevant risks resided.	No deviations noted.

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
		Procedures are in place to guide responsible personnel in performing their control activities in a timely manner and as defined by the policies and procedures.	Inspected the Information Security Policy Compliance Calendar to determine that procedures were in place to guide responsible personnel in performing their control activities in a timely manner and as defined by the policies and procedures.	No deviations noted.
		Uplevel identifies deficiencies to the respective parties to take corrective actions and to senior management, as needed.	Inspected the Incident Management Policy, the Security Incident and Breach Notification Policy, and a sample of closed incident tickets to determine that Uplevel identified deficiencies to the respective parties to take corrective actions and to senior management, as needed.	No deviations noted.
		The personnel performing control activities are competent for their role and perform the activity with diligence and continuing focus.	Inspected a sample of job descriptions to determine that the personnel performing control activities were competent for their role and perform the activity with diligence and continuing focus.	No deviations noted.
		A revision history is included within the Company's information security policy and is used to track reviews and updates to the policy.	Inspected policies and procedures to determine that a revision history was included within the Company's information security policy and was used to track reviews and updates to the policy.	No deviations noted.

CC6.0 – Common Criteria Related to Logical and Physical Access Controls

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	An inventory of all hardware and software within the scope of services are maintained.	Inspected the inventory listing to determine that an inventory of all hardware and software within the scope of services were maintained.	No deviations noted.
		Access to the applications requires a username, password, and dual factor authentication.	Observed the login procedures for Okta and AWS and inspected the application multi-factor authentication to determine that access to the applications required a username, password, and dual factor authentication.	No deviations noted.
		Unique user IDs are required to be used within the Company’s systems. Password configurations are enforced through the Company’s logical access control systems.	Inspected the login process and the password policies to determine that unique user IDs were required to be used within the Company’s systems and that password configurations were enforced through the Company’s logical access control systems.	No deviations noted.
		Encrypted VPNs are used to help ensure the security and integrity of the data passing over the public network.	Inspected the VPN configurations to determine that encrypted VPNs were used to help ensure the security and integrity of the data passing over the public network.	No deviations noted.
		The Company's virtual systems are segmented to permit unrelated portions of the information system to be isolated from each other.	Inspected the separate environments to determine that the Company's virtual systems were segmented to permit unrelated portions of the information system to be isolated from each other.	No deviations noted.

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
		A firewall is deployed to monitor and restrict inbound Internet traffic.	Inspected the firewall ruleset the intrusion detection dashboard, and the firewall administrators to determine that a firewall was deployed to monitor and restricted inbound Internet traffic.	No deviations noted.
		Web-based traffic is protected by industry standard encryption protocols. Remote connections to the Company's applications are provided through an SSL-based connection.	Inspected the SSL certificates to determine that web-based traffic was protected by industry standard encryption protocols and remote connections to the Company's applications were provided through an SSL-based connection.	No deviations noted.
		New internal and external infrastructure and software are registered, authorized, and documented prior to being granted access credentials and implemented on the network or access point. Credentials are removed and access is disabled when access is no longer required or the infrastructure and software are no longer in use.	Inspected the information security policy, inventory listing, the offboarding checklist for a sample of terminated users, and the onboarding checklists for a sample of new hires to determine that new internal and external infrastructure and software were registered, authorized, and documented prior to being granted access credentials and implemented on the network or access point and that credentials were removed and access was disabled when access was no longer required or the infrastructure and software were no longer in use.	No deviations noted.
		The Company stores data at rest on encrypted databases or backups.	Inspected the database encryption configuration to determine that the Company stored data at rest on encrypted databases or backups.	No deviations noted.

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
		The Company uses a key management system to manage entire lifecycle of encryption keys.	Inspected the managed keys dashboard to determine that the Company used a key management system to manage entire lifecycle of encryption keys.	No deviations 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 credentials are removed when user access is no longer authorized.	The Company utilizes a role-based access model for granting users access to its systems.	Inspected the Information Security Policy, the applications user listings, and the onboarding checklists for a sample of new hires to determine that the Company utilized a role-based access model for granting users access to its systems.	No deviations noted.
		Access is revoked for any terminated and separated employees.	Inspected the Information Security Policy and offboarding checklist and access for a sample of terminated employees to determine that access was revoked for any terminated and separated employees.	No deviations noted.
		User access reviews are conducted on a semi-annual basis to help ensure user identities are not compromised.	Inspected the user access review to determine that user access reviews were conducted on a semi-annual basis to help ensure user identities were not compromised.	No deviations noted.
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	Processes are in place to create or modify access to protected information assets based on authorization from the asset's owner.	Inspected onboarding checklists for a sample of new hires to determine that processes were in place to create or modify access to protected information assets based on authorization from the asset's owner.	No deviations noted.

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
	consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Access is revoked for any terminated and separated employees.	Inspected the offboarding checklist for a sample of terminated employees to determine that access was revoked for any terminated and separated employees.	No deviations noted.
		The Company utilizes a role-based access model for granting users access to its systems.	Inspected the Information Security Policy and the applications user listings to determine that the Company utilized a role-based access model for granting users access to its systems.	No deviations noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Uplevel has all its applications, data, and infrastructure in the cloud. Controls related to physical security and environmental safeguards are the responsibility of the cloud provider, AWS.		
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.	Procedures are in place to identify data and software stored on equipment to be disposed of and to render such data and software unreadable.	Inspected the Information Security Policy to determine that procedures were in place to identify data and software stored on equipment to be disposed of and to render such data and software unreadable.	This control is suitably designed; however, there were no instances of data destruction during the review period to test the operating effectiveness of the control. No deviations noted.

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
		Procedures are in place to erase or destroy decommissioned hardware containing potentially sensitive data.	Inspected the Information Security Policy to determine that the procedures were in place to erase or destroy decommissioned hardware containing potentially sensitive data.	This control is suitably designed; however, there were no instances of hardware decommissioning during the review period to test the operating effectiveness of the control. No deviations noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Access to the applications requires a user name, password, and dual factor authentication.	Inspected the applications' multi-factor authentication to determine that access to the applications required a username, password, and dual factor authentication.	No deviations noted.
		Firewall and an intrusion detection system are used to log access events and is available for review by authorized personnel.	Inspected the firewall ruleset, the intrusion detection dashboard, the firewall administrators and a sample of intrusion detection logs to determine that firewall and an intrusion detection system were used to log access events and was available for review by authorized personnel.	No deviations 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,	Firewall and an intrusion detection system are deployed to monitor and restrict inbound Internet traffic.	Inspected the firewall ruleset, the intrusion detection dashboard, and the firewall administrators to determine that firewall and an intrusion detection system were deployed to monitor and restrict inbound Internet traffic.	No deviations noted.

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
	or removal to meet the entity’s objectives.	Web-based traffic is protected by industry standard encryption protocols. Remote connections to the Company's network are provided through an SSL-based connection.	Inspected the SSL certificates to determine that web-based traffic was protected by industry standard encryption protocols and remote connections to the Company's network were provided through an SSL-based connection.	No deviations noted.
		The Company employs full-device hard drive encryption to protect the confidentiality and integrity of information on approved mobile devices.	Inspected the Information Security Policy and the encryption configuration for a sample of mobile devices to determine that the Company employed full-device hard drive encryption to protect the confidentiality and integrity of information on approved mobile devices.	No deviations 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.	The ability to install applications on systems is restricted to software preapproved by Company management.	Inquired of the CISO regarding software installation and inspected the Information Security Policy to determine that the ability to install applications on systems was restricted to software preapproved by Company management.	No deviations noted.
		File integrity monitoring is in place to detect and alert authorized personnel of any unauthorized changes to software and configuration parameters.	Inquired of the CISO regarding file integrity monitoring and inspected the Information Security Policy, the file integrity monitoring tool, sample of alerts, AWS rule details, and the list of users that receive the alerts to determine that file integrity monitoring was in place to detect and alert authorized personnel of any unauthorized changes to software and configuration parameters.	No deviations noted.

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
		The Company follows a change process to deploy, maintain, and modify third-party software.	Inspected the information security policy and a sample of application changes to determine that the Company followed a change process to deploy, maintain, and modify third-party software.	No deviations noted.
		Antivirus is installed on the Company’s systems and are required to be updated regularly.	Inspected the antivirus configuration on a sample of current employees' laptops to determine that antivirus was installed on the Company’s systems and were required to be updated regularly.	No deviations noted.

CC7.0 – Common Criteria Related to System Operations

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	System configuration standards are documented by the Company.	Inspected the Information Security Policy and baseline configurations repository dashboard to determine that system configuration standards were documented by the Company.	No deviations noted.
		Network scanning and testing is performed by the Company on an at least annual basis.	Inspected the vulnerabilities dashboard, a sample of vulnerability logs, penetration test reports, and the firewall rules to determine that network scanning and testing was performed by the Company on an at least annual basis.	No deviations noted.
		File Integrity Monitoring (FIM) is in place to detect unauthorized modifications of critical system files, configuration files, or content files.	Inspected the Information Security Policy and the file integrity monitoring tool to determine that File Integrity Monitoring (FIM) was in place to detect unauthorized modifications of critical system files, configuration files, or content files.	No deviations 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.	Policies and procedures are in place to guide personnel in identifying and mitigating security events.	Inspected the Incident Management Policy and a sample of closed incident tickets to determine that policies and procedures were in place to guide personnel in identifying and mitigating security events.	This control is suitably designed; however, there were no instances of significant security events during the review period to test the operating effectiveness of the control. No deviations noted.

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
		The Company utilizes system monitoring tools to identify and evaluate ongoing system performance, security threats, and unusual system activity.	Inspected the firewall ruleset and the intrusion detection dashboard to determine that the Company utilized system monitoring tools to identify and evaluate ongoing system performance, security threats, and unusual system activity.	No deviations noted.
		Security incidents and alerts are documented and retained by the Company.	Inspected the Incident Management Policy and a sample of incidents to determine that security incidents and alerts were documented and retained by the Company.	No deviations noted.
		The Company has implemented processes to monitor the effectiveness of detection tools.	Inspected the vulnerabilities dashboard, a sample of vulnerability logs, the penetration test reports, Security Review Board meetings and the firewall rules to determine that the Company had implemented processes to monitor the effectiveness of detection tools.	No deviations noted.
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.	Policies and procedures are documented to guide personnel in identifying and mitigating security breaches and other incidents.	Inspected the Incident Management Policy, Security Incident and Breach Notification Policy, and a sample of incidents to determine that policies and procedures were documented to guide personnel in identifying and mitigating security breaches and other incidents.	No deviations noted.
		IT personnel follow defined protocols for resolving and escalating reported events.	Inspected the Incident Management Policy and a sample of incidents to determine that IT personnel followed defined protocols for resolving and escalating reported events.	No deviations noted.

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
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.	Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are assigned.	Inspected the Security Incident and Breach Notification Policy and the Incident Management Policy to determine that roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program were assigned.	No deviations noted.
		Policies and procedures are documented to guide personnel in identifying and mitigating security breaches and other incidents.	Inspected the Security Incident and Breach Notification Policy to determine that policies and procedures were documented to guide personnel in identifying and mitigating security breaches and other incidents.	This control is suitably designed; however, there were no instances of significant security events during the review period to test the operating effectiveness of the control. No deviations noted.
		Procedures are in place to end the threats posed by security incidents through closure of the vulnerability, removal of unauthorized access, and other remediation actions.	Inspected the Incident Management Policy and a sample of incident tickets to determine that procedures were in place to end the threats posed by security incidents through closure of the vulnerability, removal of unauthorized access, and other remediation actions.	No deviations noted.
		Daily backups are performed using an automated system.	Inspected the completed backups for a sample of days to determine that daily backups were performed using an automated system.	No deviations noted.

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
		Protocols for communicating security incidents and actions taken to affected parties are developed and implemented.	Inspected the Incident Management Policy, Security Incident and Breach Notification Policy, and a sample of incidents to determine that protocols for communicating security incidents and actions taken to affected parties were developed and implemented.	No deviations noted.
		Procedures are in place to understand the nature of the incident and the severity.	Inspected the Incident Management Policy and a sample of incident tickets to determine that procedures were in place to understand the nature of the incident and the severity.	No deviations noted.
		Procedures are in place to remediate vulnerabilities through the development and execution of remediation activities.	Inspected the penetration test reports and the associated remediation ticket to determine that procedures were in place to remediate vulnerabilities through the development and execution of remediation activities.	No deviations noted.
		The design of incident response activities is evaluated for effectiveness at least annually.	Inspected the Business Continuity Plan, the Disaster Recovery Plan, the business continuity testing, and the lessons learned appendix to determine that the design of incident response activities was evaluated for effectiveness at least annually.	No deviations noted.
		Management reviews incidents related to security and confidentiality and identifies the need for system changes based on incident patterns and root causes.	Inspected the Incident Management Policy and a sample of closed incident tickets to determine that management reviewed incidents related to security and confidentiality and identified the need for system changes based on incident patterns and root causes.	No deviations noted.

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Procedures are in place to restore the affected environment to functional operation by rebuilding systems, updating software, installing patches, and changing configurations, as needed.	Inspected the completed backups for a sample of days to determine that procedures were in place to restore the affected environment to functional operation by rebuilding systems, updating software, installing patches, and changing configurations, as needed.	No deviations noted.
		Procedures are in place to communicate the nature of the incident, recovery actions taken, and activities required for the prevention of future security events are made to management and others as appropriate.	Inspected the Incident Management Policy and a sample of closed incident tickets to determine that procedures were in place to communicate the nature of the incident, recovery actions taken, and activities required for the prevention of future security events were made to management and others as appropriate.	This control is suitably designed; however, there were no instances of security events during the review period to test the operating effectiveness of the control. No deviations noted.
		Procedures are in place to analyze the root cause of an event.	Inspected the Incident Management Policy and sample of closed incident tickets to determine that procedures were in place to analyze the root cause of an event.	No deviations noted.
		Procedures are in place to implement changes to preventive controls, detective controls, or both, to prevent and detect recurrences on a timely basis.	Inspected the Business Risk and Business Impact Assessment to determine that procedures were in place to implement changes to preventive controls, detective controls, or both, to prevent and detect recurrences on a timely basis.	No deviations noted.

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
		Procedures are in place to analyze lessons learned and improve the business continuity plan and recovery procedures.	Inspected the Disaster Recovery Plan and the BCP and DRP walkthrough presentation to determine that procedures were in place to analyze lessons learned and improved the business continuity plan and recovery procedures.	No deviations noted.
		Procedures are in place to test the incident response plan and business continuity plan on an annual basis.	Inspected the Business Continuity Plan, the Disaster Recovery Plan, the business continuity testing, and the lessons learned appendix to determine that procedures were in place to test the incident response plan and business continuity plan on an annual basis.	No deviations noted.

CC8.0 – Common Criteria Related to Change Management

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Uplevel has a documented change control policies and procedures which defines the procedures for change management review, testing, and approval of scheduled software and hardware changes migrated into the production environment.	Inspected the Information Security Policy to determine that Uplevel had a documented change control policies and procedures which defined the procedures for change management review, testing, and approval of scheduled software and hardware changes migrated into the production environment.	No deviations noted.
		System change requests are reviewed and approved by management prior to work commencing on the requested change.	Inspected the Information Security Policy and a sample of application and infrastructure changes to determine that system change requests were reviewed and approved by management prior to work commencing on the requested change.	No deviations noted.
		A process is in place to design and develop system changes.	Inspected the Information Security Policy and a sample of application changes to determine that a process was in place to design and develop system changes.	No deviations noted.
		A process is in place to document system changes to support ongoing maintenance of the system and to support system users in performing their responsibilities.	Inspected the Information Security Policy and a sample of application and infrastructure changes to determine that a process was in place to document system changes to support ongoing maintenance of the system and to support system users in performing their responsibilities.	No deviations noted.
		A change management tracking system is utilized to maintain and track application change requests.	Inspected the ticketing system and a sample of application changes and infrastructure changes to determine that a change management tracking system was utilized to maintain and track application change requests.	No deviations noted.

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
		Application quality assurance testing validates key processing for the application during the change management process.	Inspected the Information Security Policy, the ticketing system, and a sample of application changes to determine that application quality assurance testing validated key processing for the application during the change management process.	No deviations noted.
		A process is in place to approve system changes prior to implementation.	Inspected the Information Security Policy, the branch protection rules, and a sample of closed pull requests to determine a process was in place to approve system changes prior to implementation.	No deviations noted.
		Approval is systematically required prior to a change being deployed into production.	Inspected the branch protection rules to determine that approval was systematically required prior to a change being deployed into production.	No deviations noted.
		A baseline configuration of IT and control systems is created and maintained.	Inspected the baseline configurations repository dashboard to determine that a baseline configuration of IT and control systems was created and maintained.	No deviations noted.
		A process is in place for authorizing, designing, testing, approving, and implementing changes necessary in emergency situations.	Inspected the Information Security Policy and the sample of emergency changes to determine that a process was in place for authorizing, designing, testing, approving, and implementing changes necessary in emergency situations.	No deviations noted.
		The Company's virtual systems are segmented to permit unrelated portions of the information system to be isolated from each other	Inquired of the CISO regarding separate environments and inspected the separate environments to determine that the Company's virtual systems were segmented to permit unrelated portions of the information system to be isolated from each other.	No deviations noted.

CC9.0 – Common Criteria Related to Risk Mitigation

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	An annual risk assessment process is in place and performed by the Company.	Inspected the Information Security Policy and the risk assessment to determine that an annual risk assessment processed was in place and performed by the Company.	No deviations noted.
		The risk management activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the Company to meet its objectives.	Inspected the insurance policies to determine that the risk management activities considered the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the Company to meet its objectives.	No deviations noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Uplevel reviews the terms of service for each of its vendors to ensure scope of services and compliance requirements are documented.	Inspected the vendor management policy and the terms of service for a sample of key vendors to determine that Uplevel reviewed the terms of service for each of its vendors to ensure scope of services and compliance requirements are documented.	No deviations noted.
		Due diligence procedures are documented and performed annually on key vendors.	Inspected the Vendor Management Policy and the vendor risk assessment to determine that due diligence procedures were documented and performed annually on key vendors.	No deviations noted.
		Senior management members have been assigned the responsibility and accountability for the management of risks associated with vendors and business partners.	Inspected the Vendor Management Policy and management job description to determine that senior management members had been assigned the responsibility and accountability for the management of risks associated with vendors and business partners.	No deviations noted.

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
		The Company establishes communication and resolution protocols for service or product issues related to vendors and business partners.	Inspected the Vendor Management Policy to determine that the Company established communication and resolution protocols for service or product issues related to vendors and business partners.	No deviations noted.
		The Company establishes exception handling procedures for service or product issues related to vendors and business partners.	Inspected the Vendor Management Policy to determine that the Company established exception handling procedures for service or product issues related to vendors and business partners.	This control is suitably designed; however, there were no instances of exception handling with vendors during the review period to test the operating effectiveness of the control. No deviations noted.
		Critical third parties and service providers are utilized by the Company, and vendor risk assessments are performed to help ensure compliance with service level agreements.	Inspected the vendor risk assessment to determine that critical third parties and service providers were utilized by the Company, and vendor risk assessments were performed to help ensure compliance with service level agreements.	No deviations noted.
		The Company implements procedures for terminating vendor and business partner relationships.	Inspected the Vendor Management Policy to determine that the Company implemented procedures for terminating vendor and business partner relationships.	This control is suitably designed; however, there were no instances of vendor terminations during the review period to test the operating effectiveness of the control. No deviations noted.

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
		Uplevel obtained confidentiality commitments that are consistent with Uplevel's confidentiality commitments and requirements from vendors and business partners who has access to confidential information.	Inspected a sample statement of work for a business partner to determine that Uplevel obtained confidentiality commitments that were consistent with Uplevel's confidentiality commitments and requirements from vendors and business partners who have access to confidential information.	This control is suitably designed; however, there were no instances of onboarded vendors during the review period to test the operating effectiveness of the control. No deviations noted.
		The Company monitors confidentiality commitments provided by their vendors and where applicable independent auditor's reports from the third parties are obtained as an aspect of monitoring vendor MSAs.	Inspected the vendor risk assessment and evidence of review of vendor third party audit reports to determine that the Company monitored confidentiality commitments provided by their vendors and where applicable independent auditor's reports from the third parties were obtained as an aspect of monitoring vendor MSAs.	No deviations noted.

C1.0 – Additional Criteria Related to Confidentiality

No.	Criteria	Control Activity Specified by the Service Organization	Tests Applied by the Service Auditor	Test Results
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Procedures are in place to identify and designate confidential information when it is received or created and to determine the period over which the confidential information is to be retained.	Inspected the Information Security Policy, the data flow diagram, an example confidential document, and a sample of internal documents to determine that procedures were in place to identify and designate confidential information when it was received or created and to determine the period over which the confidential information was to be retained.	No deviations noted.
		Procedures are in place to protect confidential information from erasure or destruction during the specified retention period of the information.	Inspected the Information Security Policy, completed backups, and the database encryption configuration to determine that procedures were in place to protect confidential information from erasure or destruction during the specified retention period of the information.	No deviations noted.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Procedures are in place to identify confidential information requiring destruction when the end of the retention period is reached.	Inspected the Information Security Policy to determine that procedures were in place to identify confidential information requiring destruction when the end of the retention period was reached.	This control is suitably designed; however, there were no instances of data destruction during the review period to test the operating effectiveness of the control No deviations noted.
		Procedures are in place to erase or destroy decommissioned hardware containing potentially sensitive data.	Inspected the Information Security Policy to determine that procedures were in place to erase or destroy decommissioned hardware containing potentially sensitive data.	This control is suitably designed; however, there were no instances of hardware decommissioning during the review period to test the operating effectiveness of the control. No deviations noted.