System and Organization Controls Report (SOC 2® TYPE 2)

Report on Uplevel Inc.'s Description of Its Engineering Intelligence Platform and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security Throughout the Period November 16, 2022, to November 15, 2023

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' or 'the Service Organization') description of its Engineering Intelligence Platform found in Section 3 titled "Uplevel Inc.'s description of its Engineering Intelligence Platform" throughout the period November 16, 2022, to November 15, 2023 ("description") based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* in 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, 2022, to November 15, 2023, to provide reasonable assurance that Uplevel's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA, *Trust Services Criteria.*

Uplevel uses Amazon Web Services (AWS) to provide 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 certain 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 designing, implementing, and operating effective controls within the system to provide reasonable assurance

that Uplevel's service commitments and system requirements were achieved. In Section 2, Uplevel has provided the accompanying assertion titled "Uplevel's Management Assertion" (assertion) about the description and the suitability of the 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 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.

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

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

- 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 meet our other ethical responsibilities in accordance with ethical requirements relating to the examination engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Test 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,

- the description presents Uplevel's Engineering Intelligence Platform that was designed and implemented throughout the period November 16, 2022, to November 15, 2023, in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the period November 16, 2022, to November 15, 2023, 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.
- the controls stated in the description operated effectively throughout the period November 16, 2022, to November 15, 2023, 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 user entity controls assumed in the design of Uplevel's controls operated effectively throughout that period.

Restricted Use

This report is intended solely for the information and use of Uplevel, user entities of Uplevel's Engineering Intelligence Platform throughout the period November 16, 2022, to November 15, 2023, and business partners of Uplevel subject to risks arising from interactions with the Engineering Intelligence Platform, 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, 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 the specified parties.

Insight Assurance LLC

Tampa, Florida
January 19, 2024

SECTION 2: UPLEVEL INC.'S MANAGEMENT ASSERTION

UPLEVEL INC.'S MANAGEMENT ASSERTION

We have prepared the description of Uplevel Inc.'s ('Uplevel' or 'the Service Organization') Engineering Intelligence Platform entitled "Uplevel Inc.'s description of its Engineering Intelligence Platform" throughout the period November 16, 2022, to November 15, 2023 ("description") based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* in AICPA, *Description Criteria*, (description criteria) The description is intended to provide report users with information about the Engineering Intelligence Platform 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 (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy With Revised Points of Focus—2022)* in AICPA, *Trust Services Criteria.*

Uplevel uses Amazon Web Services (AWS) to provide 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 organizations.

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 the subservice organization 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-

- the description presents Uplevel's Engineering Intelligence Platform that was designed and implemented throughout the period November 16, 2022, to November 15, 2023, in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the period November 16, 2022, to November 15, 2023, to provide reasonable assurance that Uplevel's service commitments and system requirements would be achieved based on the applicable trust services criteria, and if the subservice organization and user entities applied the complementary controls assumed in the design of Uplevel's controls

- the controls stated in the description operated effectively throughout the period November 16, 2022, to November 15, 2023, 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.

Uplevel Inc.

January 19, 2024

SECTION 3: UPLEVEL INC.'S DESCRIPTION OF ITS ENGINEERING INTELLIGENCE PLATFORM

UPLEVEL INC.'S DESCRIPTION OF ITS ENGINEERING INTELLIGENCE PLATFORM

COMPANY BACKGROUND

Uplevel Inc. ("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 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 the summer of 2019 and has raised $7.5M in seed funding from Madrona, Norwest Venture Partners, and Voyager Capital. It raised additional financing in a Series "A" round during the summer of 2022 with Madrona, Norwest Venture Partners, Voyager Capital, and Cota Capital participating. As of September 2023, the company has just under 30 full-time employees and many live customers. Key customers include Avalara, Nubank, Accolade, and others.

DESCRIPTION OF SERVICES OVERVIEW

Uplevel is an Engineering Intelligence 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.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Uplevel designs its processes and procedures related to the Engineering Intelligence 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 Multi-tenant 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 offered online.

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

- Security principles within the fundamental designs of the Engineering Intelligence 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 Intelligence Platform.

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

The System description is comprised of the following components:

- **Infrastructure** – The collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the service organization used to provide the services.
- **Software** - The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use mobile applications or desktop or laptop applications are.
- **People** - The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- **Data** – The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- **Procedures** – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

INFRASTRUCTURE

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

Data is first collected on-prem in the client's environment, 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, or Github is required.

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

Uplevel Network Data Flow
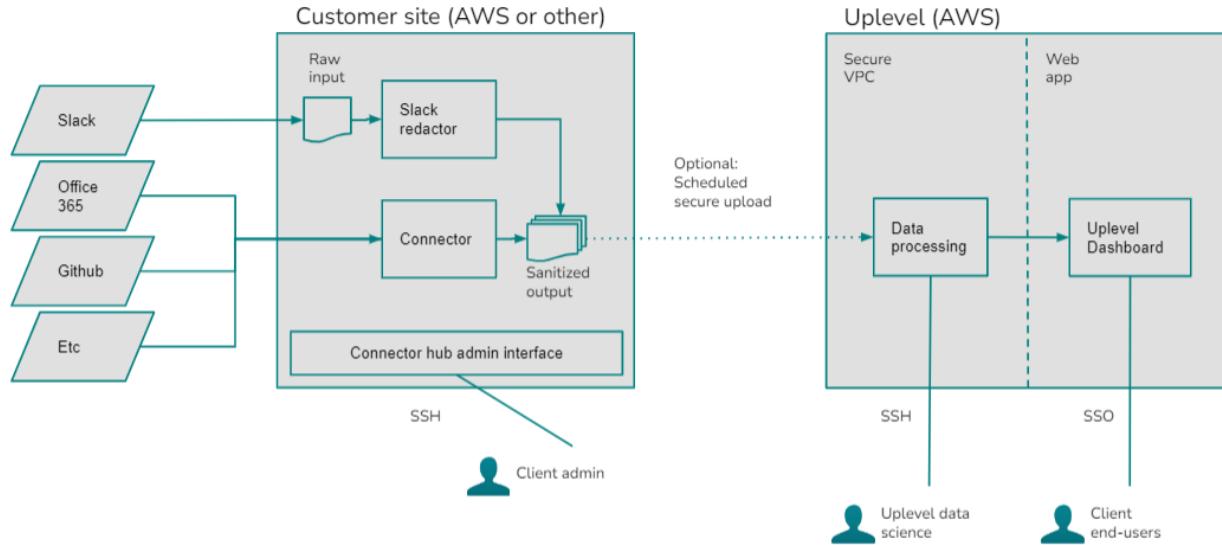
Uplevel maintains a system inventory that includes virtual machines (EC2 instances), computers (desktops and laptops), and networking devices (switches and routers). The inventory documents the device name, device type, vendor function, OS, location, and notes. To outline the topology of its network, the organization maintains the following network diagrams.

The Uplevel application infrastructure is hosted in AWS (across several US regions). AWS acts as a hosting subservice organization for the company. The subservice organization provides physical security and environmental protection controls, as well as managed services for Uplevel's infrastructure.

AWS network security uses hardware and software-based intrusion prevention, advanced content filtering, anti-malware, and anti-spam modules.

In addition to the firewall, Uplevel uses anti-virus and anti-spyware applications to protect systems from viruses.

Uplevel's Information Security Policy and security procedures ensure that all computer devices (including servers, desktops, printers, etc.) connected to the Uplevel network have proper virus protection software, current virus definition libraries, and the most recent operating system and security patches installed. The Engineering department verifies that all known and reasonable defenses are in place to reduce network vulnerabilities while keeping the network operating. In the event of a virus threat, the anti-virus system will attempt to delete or quarantine the infected file. If the virus cannot be deleted or quarantined, the infected machine will be disconnected from the network and cleaned manually.

Multiple controls are installed to monitor traffic that could contain malicious programs or code. External perimeter scans are performed annually by a third-party vendor to expose potential vulnerabilities to the production environment and corporate data. Email is scanned at the gateway and in the hosted email environment. Server operating systems utilize anti-virus and anti-spyware programs. All employee workstation computers have a minimum standard hardware and software

configuration. Employees are not allowed to install any software on Uplevel-owned computers. The IT staff maintains several replacement computers that can replace workstations in need of repair or maintenance, thereby disrupting the employee's workday as little as possible.

SOFTWARE

Uplevel maintains a list of critical software in use within its environment. The organization also retains appropriate software license documentation. Critical software in use includes the following:

- Amazon Web Services (AWS)
- Datadog
- GitHub
- Google Workspace
- HubSpot
- Jira
- Notion
- PagerDuty
- Vanta
- Sentry
- Slack
- Zoom

PEOPLE

The Uplevel staff provides support to the above services. Uplevel employs dedicated team members to handle all major product functions, including operations, and support. The Engineering Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep Uplevel and its data secure.
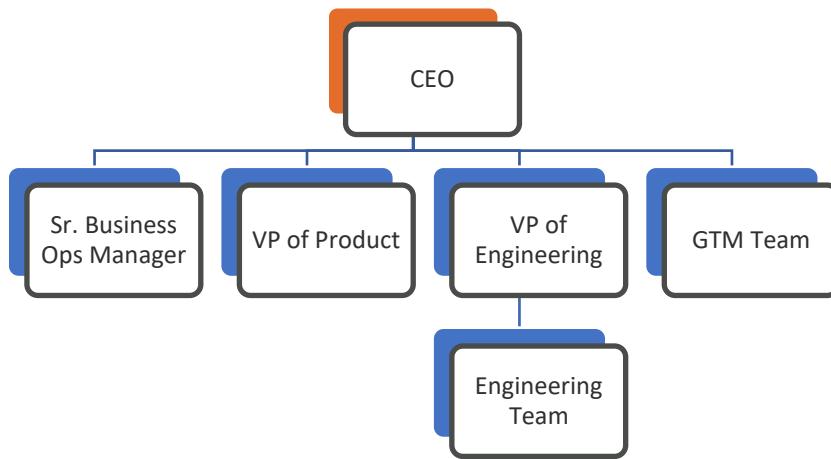
Uplevel's corporate structure includes the following roles:

Chief Executive Officer (CEO) – Handles the strategic direction of the organization. The CEO assigns authority and responsibility to key management personnel with the skills and experience necessary to carry out their assignments.

Go to Market Team – Responsible for the outward communication of company initiatives. Primary role responsible for exposing new programs to prospects and existing customers and furthering the public reach of Uplevel.

Customer Success – This role is responsible for customer relations and working closely with the Sales and Marketing team to ensure there is transparency between marketing and sales efforts. This role also includes the support team and crosses over to the engineering team. It is primarily responsible for daily support aspects of the business. This includes but is not limited to the support of end-users with day-to-day issues, as well as assisting in the onboarding, implementation, and migrations of new and existing customers as part of their ongoing maintenance.

Sales - Primary role for outbound reach to prospects and completing sales. They are also responsible for the maintenance and renewal of existing customer contracts.

VP of Engineering & VP of Product – Responsible for the technological direction and advancements of the organization. Directs the operations, engineering, and support teams to efficiently create/present new services, maintain existing ones, and help support the Uplevel customer-based use of the service. These roles are responsible for the operations of the day-to-day items to maintain the integrity of the environment. This role is also responsible for the provisioning and research and development of new and upcoming services within the company.

DATA

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements. Customer data is captured which is utilized by Uplevel and delivered through the product.

The information takes many forms. It may be stored on computers, transmitted across networks, printed or written on paper, and spoken in conversations. All employees of Uplevel are obligated to respect and, in all cases, to protect confidential and private data. Customer information, employment-related records, and other intellectual property-related records are, subject to limited exceptions, confidential as a matter of law. Many other categories of records, including company and other personnel records, and records relating to Uplevel's business and finances are, as a matter of Uplevel policy, treated as confidential. Responsibility for guaranteeing appropriate security for data, systems, and networks is shared by the Client Services and IT Departments. IT is responsible for designing, implementing, and maintaining security protection and retains responsibility for ensuring compliance with the policy. In addition to management and the technology staff, individual users are responsible for the equipment and resources under his or her control.

Uplevel has policies and procedures in place to ensure prior retention and disposal of confidential and private data. The retention and data destruction policies define the retention periods and proper destruction procedures for the disposal of data. These policies are reviewed at least annually. The destruction of data is a multi-step process. Client data is deleted upon termination of the contract. A ticket is created and assigned to the product team and system engineering team to coordinate the deletion of the data. First, all files received or generated from the client are identified and deleted by the system engineering team then the product team deletes all user-related data.

Electronic communications are treated with the same level of confidentiality and security as physical documents. Networks are protected by enterprise-class firewalls and appropriate

enterprise-class virus protection is in place. Password protection with assigned user rights is required for access to the network, application, and databases. Access to the network, application, and databases is restricted to authorized internal and external users of the system to prohibit unauthorized access to confidential data. Additionally, access to data is restricted to authorized applications to prevent unauthorized access outside the boundaries of the system.

Summary of Uplevel Data Sanitization

To calculate the building block metrics and provide our insights, Uplevel requires access to a sanitized copy of our customers' data. We realize this is super sensitive and have built several procedures and safeguards to ensure the data is safely and securely managed.

Uplevel describes how they functionally process and sanitize customer data. Separately, Uplevel has several security safeguards such as encryption, single sign-on, and 3rd party audits that we review and get approval from the customer's information security team. Uplevel also has many legal safeguards such as requirements for controlled access, background checks, and liability coverage that are 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 that your IT department can run to download the data locally first, audit it, 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 them 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.

All data presented to the customer is aggregated at the team level, typically similar to HR engagement results. No manager can directly identify information about a specific employee based on Uplevel insights. For example, "Ashley's team had a lot of time to focus last week" which would be based on aggregated analysis of calendars, Slack, Jira, and Bitbucket. No individual is identified.

Sanitization of Slack:

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

The 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 with certain Slack channels that, while marked as private, are effectively public to that team and are valuable sources of work information. These are commonly larger private channels for people discussing non-sensitive technical topics. We can discuss ways of ingesting these channels as well.

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 emails are 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.

PROCEDURES

Formal IT policies and procedures exist that describe logical access, computer operations, change management, incident management, and data communication standards to obtain the stated objectives for network and data security, data privacy, and integrity for both the company and its clients and define how services should be delivered. These are communicated to employees and are located within the organization's intranet.

Reviews and changes to these policies and procedures are performed annually and are approved by senior management.

Physical Security and Environmental Controls

Uplevel's production servers are maintained by Amazon Web Services.

Physical and environmental security protections are the responsibility of Amazon Web Services. Uplevel reviews the attestation reports and performs a risk analysis of Amazon Web Services on at least an annual basis.

Logical Access

AWS handles the network, physical host, and virtual server infrastructure. Uplevel handles the administrative responsibilities involved in supporting the web, application, and database components of the platform Uplevel has full access to log into their servers remotely using secure shell (SSH) or Windows Remote Desktop, depending on the platform. Dedicated firewalls are used to restrict administrative access to servers. Appropriate firewall rules are in place to restrict access to customer data and to limit the possibility of disruptions to customer operations from unauthorized users.

Logical access to Uplevel's networks, applications, and data is limited to properly authorized individuals. For both the client-hosted network and the Uplevel local network, logical access is controlled via standard user authentication credentials (user ID and password). No other outside access is permitted.

Change Management

For internally developed software platforms/solutions, Uplevel uses an agile-based SDLC process, which includes research and planning, analysis and design, initial development, and quality assurance (QA) testing before the final release. All software development activities follow the internal project-related business process model.

Uplevel has a Change Management Policy in place to control information resources that require an outage for planned upgrades, maintenance, or fine-tuning. Additionally, unplanned outages may occur that may result in upgrades, maintenance, or fine-tuning. The purpose of the Change Management Policy is to manage changes rationally and predictably so that staff and clients can plan accordingly. Changes require forethought, monitoring, and follow-up evaluation to reduce the negative impact on the user community and to increase the value of Information Resources. The Uplevel Change Management Policy applies to all individuals who install, operate, or maintain Information Resources.

Patch Management

Uplevel takes a proactive approach to patch management. The VP of Engineering and engineers regularly monitor various websites, message boards, and mailing lists where advanced notifications of bug-related patches are often disclosed before a public announcement by the vendor. This allows the company to plan for upcoming patches.

The networking team reviews the availability of patches and independently determines if it is necessary to deploy within the production environment. Approved patches are scheduled for installation in the test environment weekly as applicable. If there are no issues in the test

environment after a week, the patch will be applied to the production environment. The patching process is tracked via a Jira ticket.

Backup and Recovery

Uplevel uses several different managed AWS services (RDS, ECS) that provide ongoing reliability and recovery of the system and backup of critical data. Databases have automatic full snapshots that run daily. The retention period for these jobs is 7 days. Jobs are run nightly on a regular schedule with schedules distributed based on specific database use cases. Alerts are generated if any errors are encountered with the backup. Testing of the snapshots is done quarterly. All backups are encrypted and stored within S3.

Problem Management

Uplevel maintains an Incident Response Policy that describes the process for identifying and addressing potential security incidents. The policy details exactly what must occur if an incident is suspected and covers both electronic and physical security incidents. Plans for detecting, responding to, and recovering from incidents are included in the policy and post-incident activity requirements are defined. To ensure responsible employees are prepared to respond to incidents, the organization provides formal security breach training.

The organization provides a customer service request form where clients can report potential security breaches, and clients are also provided with an email and phone number for this same purpose. Internal users are directed to report incidents through an internal portal for documentation and tracking purposes.

System Monitoring

The Network Security and Vulnerability Management Policy describes the organization's policies and procedures related to network logging and monitoring as well as vulnerability identification and remediation. The organization uses CloudWatch for system logging within the AWS environment, and the organization collects logs from the OpenVPN router. CloudWatch logs and the OpenVPN router logs document source IP, destination IP, destination port, protocol type, and timestamp. The organization monitors system capacity using CloudWatch.

AWS Guard Duty is used for threat detection purposes, and the tool generates logs, VPC flow logs, and DNS logs for intrusion detection.

The vulnerability assessment process involves the execution of CIS testing, implementation of antivirus software, and system patching. The organization uses Avast antivirus and has configured the software to run updates daily and prohibit end-users from disabling or altering the software. Alerts are sent immediately when a potential virus is detected, and logs are generated and retained for at least one year with at least three months readily available. Github Dependabot and AWS Inspector are used to identify newly emerging vulnerabilities, and the organization monitors vendors for patch updates to correct vulnerabilities.

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 the Customer within 30 days of completion, planned for annually during Q4.

Vendor Management

The organization maintains a Vendor Management Policy that includes requirements for interacting with vendors/service providers. The policy includes requirements for performing due diligence measures before engaging with a new provider. Due diligence procedures include evaluating each material IT vendor's cost-effectiveness, functionality/services, risk, financial viability, compliance, and performance. The organization is required to define service levels when negotiating an arrangement with a new vendor or re-negotiating an existing arrangement, and all service levels are agreed upon and documented clearly. The organization monitors its providers' service levels to ensure each provider is providing the agreed-upon services and is compliant with all requirements. The organization executes non-disclosure agreements with third parties before any information is shared.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, CONTROL ACTIVITIES, INFORMATION AND COMMUNICATION, AND MONITORING

The security category and applicable trust services criteria were used to evaluate the suitability of the design of controls stated in the description. Security criteria and the controls designed, implemented, and operated to meet them ensure that the system is protected against unauthorized access (both physical and logical). The controls supporting the applicable trust services security criteria are included in section IV of this report. Although the applicable trust services criteria and related controls are included in section IV, they are an integral part of Uplevel's description of its system.

CONTROL ENVIRONMENT

The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across an organization. The organizational structure, separation of job responsibilities by departments and business function, documentation of policies and procedures, and internal audits are the methods used to define, implement, and assure effective operational controls. The Board of Directors and/or senior management establish the tone at the top regarding the importance of internal control and expected standards of conduct.

Management Philosophy, Integrity, and Ethical Values

Uplevel's control environment reflects the philosophy of senior management concerning the importance of the security of data. Integrity and ethical values are essential elements of Uplevel's control environment. Management is responsible for setting the tone at the top, establishing, communicating, and monitoring control policies and procedures.

Formal policies, code of conduct, and employee handbooks are documented and communicated to employees to ensure that entity values, ethics, integrity, and behavioral standards are a primary focus and risks are mitigated in daily operations. In addition, a sanctions policy is in place to address deviations from established security and personnel standards.

Management's philosophy and operating style affect the way the entity is managed, including the kinds of business risks accepted. Uplevel places a great deal of importance on working to ensure

that the integrity of processing is a primary focus and that controls are maximized to mitigate risk in daily operations. Management and specific teams are structured to ensure the highest level of integrity and efficiency in customer support and transaction processing.

Formal job descriptions departmental meetings and staff interactions ensure communication of organizational values, ethics, and behavior standards. Personnel operates under Uplevel's policies and procedures, including confidentiality agreements and security policies. Annual training is conducted to communicate regulations and the importance of privacy and security. Management is committed to being aware of regulatory and economic changes that impact lines of business and monitoring the customer base for trends, changes, and anomalies.

Commitment to Competence

Uplevel has standardized human resource policies and procedures. The result is a uniform set of practices that provide equitable hiring and advancement opportunities across the organization.

Training and development opportunities are provided to staff and performance evaluations are performed to communicate goals based on job responsibilities and address any performance issues.

Employees are trained in their specific roles and policies through on-the-job training and procedures are reviewed. Management communicates any changes to these policies on an ongoing basis and policies are updated as needed. To protect confidential internal and client information employees are prohibited from divulging any information regarding client affairs or taking action, not in the interests of the client or Uplevel.

Human Resources Policies and Procedures

Uplevel has formal hiring procedures that are designed to ensure that new team members are able to meet or exceed the job requirements and responsibilities. All candidates go through interviews and assessments of their education, professional experience, and certifications. Background checks are performed for all newly hired employees before the start date and include a review of their education and criminal records.

During the onboarding process, the new employees review the Employee Handbook, Confidentiality Agreement, and any other relevant policies and procedures relevant to their role. Newly hired employees are required to sign an acknowledgment of receipt and understanding of the Employee Handbook and Confidentiality Agreement. These policies and procedures are also available to employees through the internal policies repository. Security awareness training is also completed at least annually by all employees, including the areas of security and confidentiality to communicate the security implications around their roles and how their actions could affect the organization.

Ongoing performance feedback is provided to all employees. Formal performance reviews are completed annually by management to discuss expectations, goals, and the employee's performance for the last fiscal year.

RISK ASSESSMENT PROCESS

Uplevel regularly reviews the risks that may threaten the achievement of its service commitments and system requirements related to security, availability, and confidentiality. The Risk assessment process is performed by management to identify and manage risks and consider possible

changes in the internal and external environment to mitigate these risks. Risk mitigation activities include the prevention, mitigation, and detection of risk via the implementation of internal controls. In addition, management also transfers risk through the organization's business insurance policies.

The Uplevel management team and other members of the engineering team monitor rick on an ongoing basis using information derived from employee input, system morning, audit results, industry experience, business environment, and internal system and/or process changes.

On an annual basis, management completes a risk assessment as part of the annual risk management activities. Risks identified during the annual risk assessment process include the following:

- Operational Risk
- Strategic Risk
- Compliance Risk
- Fraud Risk
- Environmental Risk

CONTROL ACTIVITIES

Control activities are the actions established by policies and procedures to help ensure that management directives to mitigate risks to the achievement of objectives are executed. Control activities are performed at all levels of the organization and various stages within business processes, and over the technology environment.

INFORMATION AND COMMUNICATION SYSTEMS

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

Additional communication methods include department meetings to communicate company policies, procedures, industry or business issues, or other topics management deems key to the achievement of the organization's objectives. Communication is encouraged at all levels to promote the operating efficiency of Uplevel.

Uplevel also updates its website on an ongoing basis to inform clients and other external parties of company and industry-related issues that could affect their services and what steps the company is taking to reduce or avoid the impact on their operations. The organization's security, availability, and confidentiality commitments regarding the engineering effectiveness system are included in the services agreement.

MONITORING CONTROLS

In addition to daily oversight, and vulnerability assessments, management uses monitoring software to monitor the security and availability of their systems. Ongoing monitoring of internal controls is also performed by management.

Monitoring of the Subservice Organization

Uplevel uses a subservice organization to provide hosting services.

Management of Uplevel receives and reviews the SOC 2 report of AWS on an annual basis. In addition, through its daily operational activities, the management of Uplevel monitors the services performed by AWS to ensure that operations and controls expected to be implemented at the subservice organization are functioning effectively.

TRUST SERVICES CATEGORIES

The security category and applicable trust services criteria were used to evaluate the suitability of the design of controls stated in the description. Criteria and controls designed, implemented, and operated to meet them ensure that information, systems, and access (physical and logical) are protected against unauthorized access, and systems are available for operation and use.

CONTROLS ACTIVITIES AND CRITERIA

Uplevel's trust services criteria and related control activities are included in Section 4 of this report to eliminate the redundancies that would result from listing them here in Section 3 and repeating them in Section 4. Although the trust services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Uplevel's description of controls.

For specific criteria, which were deemed not relevant to the system, see Section 4 for the related explanation.

CHANGES TO THE SYSTEM DURING THE PERIOD

No significant changes have occurred to the services provided to user entities during the examination period.

SYSTEM INCIDENTS DURING THE PERIOD

No significant incidents have occurred to the service provided to user entities during the examination period.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOCs)

Uplevel's controls related to the Engineering Intelligence Platform cover only a portion of the overall internal control for each user entity of Uplevel. It is not feasible for the trust services criteria related to the Engineering Intelligence Platform to be achieved solely by Uplevel. Therefore, each user entity's internal controls should be evaluated in conjunction with Uplevel's controls and the related tests and results described in Section 4 of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

	Complementary Subservice Organization Controls (CSOC)	Related Criteria
1	AWS is responsible for maintaining physical security and environmental protection controls over the data centers hosting the Uplevel infrastructure.	CC6.4

	Complementary Subservice Organization Controls (CSOC)	Related Criteria
2	AWS is responsible for the destruction of physical assets hosting the production environment.	CC6.5

COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

Uplevel's controls related to the Engineering Intelligence Platform only cover a portion of the overall internal controls for each user entity. It is not feasible for the applicable trust service criteria related to the system to be achieved solely by Uplevel control procedures. Accordingly, user entities, in conjunction with the services, should establish their internal controls or procedures to complement those of Uplevel.

User auditors should determine whether the following controls have been in place in operation at the user organization:

- Controls to provide reasonable assurance that user access including the provisioning and de-provisioning are designed appropriately and operating effectively.
- User entities are responsible for reporting issues with Uplevel systems and platforms.
- User entities are responsible for understanding and complying with their contractual obligations to Uplevel.
- User entities are responsible for notifying Uplevel of changes made to the administrative contact information.

SECTION 4: TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS AND TEST OF CONTROLS

Trust Services Category, Criteria, Related Controls, and Test of Controls

This SOC 2 Type 2 report was prepared in accordance with the AICPA attestation standards and has been performed to examine the suitability of the design and operating effectiveness of controls to meet the criteria for the Security category set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*With Revised Points of Focus – 2022)* in AICPA, Trust Services Criteria throughout the period November 16, 2022, to November 15, 2023.

The trust services category for the Security criteria and related controls specified by Uplevel are presented in Section 4 of this report.

Test procedures performed in connection with determining the operating effectiveness of controls detailed here in section 4 are described below:

- Inquiries - Inquiry of appropriate personnel and corroboration with management
- Observation - Observation of the application, performance, or existence of the control.
- Inspection - Inspection of documents and reports indicating the performance of the control.
- Reperformance - Reperformance of the control.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

	TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
	CONTROL ENVIRONMENT		
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	The company has an approved Employee Handbook that is reviewed annually and updated as needed. Sanction policies are documented within the information security policies and procedures.	Inspected the company's Employee Handbook to determine that the company had an approved Employee Handbook that is reviewed annually and updated as needed.	No exceptions noted.
		Inspected the company's information security policies and procedures to determine that sanction policies were documented within the information security policies and procedures.	No exceptions noted.
CC1.1.2	The company requires employees to acknowledge the Employee Handbook at the time of hire and active employees to acknowledge the Employee Handbook at least annually.	Inspected the Employee Handbook acknowledgment for a sample of employees to determine that the Employee Handbook was acknowledged at the time of hire.	No exceptions noted.
		Inspected the Employee Handbook acknowledgments for a sample of active employees during the examination period to determine that the Employee Handbook was acknowledged at least annually.	No exceptions noted.
CC1.1.3	The company requires employees to review and acknowledge the information security policies at the time of hire and active employees to acknowledge the information security policies at least annually.	Inspected the information security policies acknowledgment for a sample of employees to determine that the information security policies were acknowledged at the time of hire.	No exceptions noted.
		Inspected the information security policies acknowledgment for a sample of active	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	Controls	Detailed Test of Controls	Test Results
		employees to determine that the information security policies were acknowledged at least annually.	
CC1.1.4	The company's managers are required to complete performance evaluations for direct reports at least annually.	Inspected the completed performance evaluation for a sample of employees to determine that the company's managers were required to complete performance evaluations for direct reports annually.	No exceptions noted.
CC1.1.5	The company performs background checks on new employees.	Inspected the completed background check for a sample of new employees to determine whether the company performed background checks on new employees.	No exceptions noted.
CC1.1.6	Employees are required to review and acknowledge the confidentiality agreement at the time of hire.	Inspected the signed agreements and/or non-disclosure agreements for a sample of new employees to determine that employees were required to review and acknowledge the confidentiality agreement at the time of hire.	No exceptions noted.
Criteria: COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	The company's board members have sufficient expertise to oversee management's ability to design, implement, and operate information security controls.	Inspected the board members' profiles to determine that the company's board members had sufficient expertise to oversee management's ability to design, implement, and operate information security controls.	No exceptions noted.
CC1.2.2	The company's board of directors meets annually and maintains formal meeting minutes.	Inspected the board of directors meeting minutes to determine that the company's board of	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
		directors meets annually and maintained formal meeting minutes.	
CC1.2.3	The company's board of directors has a documented Information Security Policy that outlines its oversight responsibilities for internal control.	Inspected the company's Information Security Policy to determine that the company's board of directors had a documented Information Security Policy that outlined its oversight responsibilities for internal control.	No exceptions noted.
CC1.2.4	The company's board of directors consists of members that are independent of the company.	Inspected the board of directors listing to determine that the company's board of directors consisted of members that were independent of the company.	No exceptions noted.
Criteria: COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	The company maintains an organizational chart that describes the organizational structure and reporting lines.	Inspected the company's organizational chart to determine that the company maintained an organizational chart that described the organizational structure and reporting lines.	No exceptions noted.
CC1.3.2	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Policy.	Inspected the company's Information Security Policy to determine roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in the Information Security Policy.	No exceptions noted.
CC1.3.3	The company requires employees to review and acknowledge the information security policies at	Inspected the information security policies acknowledgment for a sample of employees to	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
	the time of hire and active employees to acknowledge the information security policies at least annually.	determine that the information security policies were acknowledged at the time of hire.	
		Inspected the information security policies acknowledgment for a sample of active employees to determine that the information security policies were acknowledged at least annually.	No exceptions noted.
Criteria: COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	The company performs background checks on new employees.	Inspected the completed background check for a sample of new employees to determine whether the company performed background checks on new employees.	No exceptions noted.
CC1.4.2	The company's managers are required to complete performance evaluations for direct reports at least annually.	Inspected the completed performance evaluation for a sample of employees to determine that the company's managers were required to complete performance evaluations for direct reports annually.	No exceptions noted.
CC1.4.3	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Policy.	Inspected the company's Information Security Policy to determine roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls formally assigned in the Information Security Policy.	No exceptions noted.
CC1.4.4	The company requires new employees to complete security awareness training at the time	Inspected the security awareness training topics to determine that the security awareness training	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	Controls	Detailed Test of Controls	Test Results
	of hire and active employees to complete security training at least annually.	covered areas to educate personnel on information security topics and the latest trends to protect scontrensitive data.	
		Inspected the training records for a sample of new employees to determine that the company required employees to complete security awareness training at the time of hire.	No exceptions noted.
		Inspected the training records for a sample of active employees to determine that the company required employees to complete security awareness training annually.	No exceptions noted.
Criteria: COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	The company has an approved Employee Handbook that is reviewed annually and updated as needed. Sanction policies are documented within the information security policies and procedures.	Inspected the company's Employee Handbook to determine that the company had an approved Employee Handbook that is reviewed annually and updated as needed.	No exceptions noted.
		Inspected the company's information security policies and procedures to determine that sanction policies were documented within the information security policies and procedures.	No exceptions noted.
CC1.5.2	The company requires employees to acknowledge the Employee Handbook at the time of hire and active employees to	Inspected the Employee Handbook acknowledgment for a sample of employees to determine that the Employee Handbook was acknowledged at the time of hire.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	Controls	Detailed Test of Controls	Test Results
	acknowledge the Employee Handbook at least annually.	Inspected the Employee Handbook acknowledgments for a sample of active employees during the examination period to determine that the Employee Handbook was acknowledged at least annually.	No exceptions noted.
CC1.5.3	The company's managers are required to complete performance evaluations for direct reports at least annually.	Inspected the completed performance evaluation for a sample of employees to determine that the company's managers were required to complete performance evaluations for direct reports annually.	No exceptions noted.
CC1.5.4	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Policy.	Inspected the company's Information Security Policy to determine roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in the Information Security Policy.	No exceptions noted.
CC1.5.5	The company requires new employees to complete security awareness training at the time of hire and active employees to complete security training at least annually.	Inspected the security awareness training topics to determine that the security awareness training covered areas to educate personnel on information security topics and the latest trends to protect sensitive data.	No exceptions noted.
		Inspected the training records for a sample of new employees to determine that the company required employees to complete security awareness training at the time of hire.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	Controls	Detailed Test of Controls	Test Results
		Inspected the training records for a sample of active employees to determine that the company required employees to complete security awareness training annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
INFORMATION AND COMMUNICATION			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented and reviewed annually.	No exceptions noted.
CC2.1.2	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected the company's compliance platform to determine that control self-assessments were performed annually, and corrective actions were taken based on relevant findings.	No exceptions noted.
CC2.1.3	The company utilizes a log management tool to identify events that may potentially impact the company's ability to achieve its security objectives.	Inspected the log management tool configurations to determine that the company utilized a log management tool to identify events that may potentially impact the company's ability to achieve its security objectives.	No exceptions noted.
Criteria: CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	The company has security incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Information Security Policy and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
INFORMATION AND COMMUNICATION			
Control Number	Controls	Detailed Test of Controls	Test Results
CC2.2.2	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Policy.	Inspected the company's Information Security Policy to determine roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in the Information Security Policy.	No exceptions noted.
CC2.2.3	The company requires new employees to complete security awareness training at the time of hire and active employees to complete security training at least annually.	Inspected the security awareness training topics to determine that the security awareness training covered areas to educate personnel on information security topics and the latest trends to protect sensitive data.	No exceptions noted.
		Inspected the training records for a sample of new employees to determine that the company required employees to complete security awareness training at the time of hire.	No exceptions noted.
		Inspected the training records for a sample of active employees to determine that the company required employees to complete security awareness training annually.	No exceptions noted.
CC2.2.4	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented and reviewed annually.	No exceptions noted.
CC2.2.5	The company describes its products and services to internal and external users.	Inspected the company's website to determine that the company provided a description of its	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
INFORMATION AND COMMUNICATION			
Control Number	Controls	Detailed Test of Controls	Test Results
		products and services to internal and external users.	
CC2.2.6	The company communicates system changes to authorized internal users.	Inspected the internal communication channel/example communication to determine that the company communicated system changes to authorized internal users.	No exceptions noted.
Criteria: CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	The company's security commitments are communicated to customers in the Uplevel Software as a Service Agreement and Privacy Policy.	Inspected the company's Software as a Service Agreement and Privacy Policy to determine that the company's security commitments were communicated to customers in the Uplevel Software as a Service Agreement and Privacy Policy.	No exceptions noted.
CC2.3.2	The company provides guidelines and technical support resources relating to system operations to customers.	Inspected the company's support page/knowledge base to determine that the company provides guidelines and technical support resources relating to system operations to customers.	No exceptions noted.
CC2.3.3	The company describes its products and services to internal and external users.	Inspected the company's website to determine that the company described its products and services to internal and external users.	No exceptions noted.
CC2.3.4	The company has contact information on its website to allow users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected the company's website to determine that the company had the contact information on their website to allow users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
INFORMATION AND COMMUNICATION			
Control Number	Controls	Detailed Test of Controls	Test Results
CC2.3.5	The company has written agreements in place with vendors and related third parties. These agreements include security and confidentiality commitments applicable to that entity.	Inspected the Terms of Service for vendors to determine that security and confidentiality commitments were in place for vendors and related third parties.	No exceptions noted.
CC2.3.6	The company notifies customers of critical system changes that may affect their processing.	Inspected example communication to determine that the company notified customers of critical system changes that may affect their processing.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	Controls	Detailed Test of Controls	Test Results
Criteria: COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the annual security risk assessment to determine that the company specified its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.
CC3.1.2	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Management Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC3.1.3	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
Criteria: COSO Principle 7: 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.			
CC3.2.1	The company has a documented risk management program in place that includes guidance on the identification of potential	Inspected the company's Risk Management Policy to determine that the company had a documented risk management program in place that included	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	Controls	Detailed Test of Controls	Test Results
	threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	
CC3.2.2	The company has a third-party management program in place. Components of this program include: - critical third-party vendor inventory. - vendor's security requirements; and - annual review of critical third-party vendors	Inspected the company's Information Security Policy to determine that the company had a third-party management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the vendor listing to determine that the critical third-party vendor inventory was in place.	No exceptions noted.
		Inspected the vendor review to determine that a review of critical third-party vendors was performed annually.	No exceptions noted.
CC3.2.3	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC3.2.4	The company has a documented business continuity/disaster recovery (BC/DR) Plan and tests it at least annually.	Inspected the company's BC/DR Plan to determine that the company has a documented BC/DR plan.	No exceptions noted.
		Inspected the company's latest BC/DR Plan tabletop exercise meeting minutes to determine that the BC/DR plan was tested annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC3.3.2	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Management Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
Criteria: COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for	Inspected the annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	Controls	Detailed Test of Controls	Test Results
	fraud and how fraud may impact the achievement of objectives.		
CC3.4.2	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Management Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

	TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
	MONITORING ACTIVITIES		
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected the company's compliance platform to determine that control self-assessments were performed annually, and corrective actions were taken based on relevant findings.	No exceptions noted.
CC4.1.2	The company's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate critical and high vulnerabilities in accordance with SLAs.	Inspected the completed penetration report to determine that a penetration test was performed annually.	No exceptions noted
		Per inspection of the penetration test report, there were no critical and high vulnerabilities found during the assessment. Therefore, no testing was performed.	No testing performed.
CC4.1.3	Vulnerability scans are performed annually on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Inspected the completed vulnerability scan reported to determine that vulnerability scans were performed annually on all external-facing systems.	No exceptions noted.
		Inspected the remediation ticket/notes for a sample of vulnerabilities to determine that critical and high vulnerabilities were tracked to remediation.	No exceptions noted.
CC4.1.4	The company has a third-party management program in place. Components of this program include: - critical third-party vendor inventory. - vendor's security requirements; and - annual review of critical third-party vendors.	Inspected the company's Information Security Policy to determine that the company had a third-party management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the vendor listing to determine that the critical third-party vendor inventory was in place.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	Controls	Detailed Test of Controls	Test Results
		Inspected the vendor review to determine that a review of critical third-party vendors was performed annually.	No exceptions noted.
Criteria: COSO Principle 17: 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.			
CC4.2.1	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected the company's compliance platform to determine that control self-assessments were performed annually, and corrective actions were taken based on relevant findings.	No exceptions noted.
CC4.2.2	The company has a third-party management program in place. Components of this program include: - critical third-party vendor inventory. - vendor's security requirements; and - annual review of critical third-party vendors.	Inspected the company's Information Security Policy to determine that the company had a third-party management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the vendor listing to determine that the critical third-party vendor inventory was in place.	No exceptions noted.
		Inspected the vendor review to determine that a review of critical third-party vendors was performed annually.	No exceptions noted.
CC4.2.3	The company's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate critical and high vulnerabilities in accordance with SLAs.	Inspected the completed penetration report to determine that a penetration test was performed annually.	No exceptions noted.
		Per inspection of the penetration test report, there were no critical and high vulnerabilities found during the assessment. Therefore, no testing was performed.	No testing performed.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	Controls	Detailed Test of Controls	Test Results
CC4.2.4	Vulnerability scans are performed annually on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Inspected the completed vulnerability scan reported to determine that vulnerability scans were performed annually on all external-facing systems.	No exceptions noted.
		Inspected the remediation ticket/notes for a sample of vulnerabilities to determine that critical and high vulnerabilities were tracked to remediation.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Management Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC5.1.2	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented and reviewed annually.	No exceptions noted.
CC5.1.3	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC5.1.4	Role-based access is configured within AWS and other supporting applications to enforce	Inspected the system configuration for AWS and other supporting applications to determine that role-	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	Controls	Detailed Test of Controls	Test Results
	the segregation of duties and restrict access to confidential information.	based access was configured to enforce segregation of duties and restrict access to confidential information.	
Criteria: COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	The company's Information Security Policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company's Information Security Policy to determine that the Information Security Policy documented the requirements for adding, modifying, and removing user access.	No exceptions noted.
CC5.2.2	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's Information Security Policy to determine that the company had a formal SDLC methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.
CC5.2.3	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented and reviewed annually.	No exceptions noted.

	TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
	CONTROL ACTIVITIES		
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented and reviewed annually.	No exceptions noted.
CC5.3.2	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	Inspected the company's Information Security Policy to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
		Inspected the documentation for a sample of changes to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
CC5.3.3	The company has a formal SDLC methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's Information Security Policy to determine that the company had a formal SDLC methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance	No exceptions noted.

	TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
	CONTROL ACTIVITIES		
Control Number	Controls	Detailed Test of Controls	Test Results
		of information systems and related technology requirements.	
CC5.3.4	The company has security incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Information Security Policy and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.
CC5.3.5	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the annual security risk assessment to determine that the company specified its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.
CC5.3.6	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Management Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC5.3.7	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Policy.	Inspected the company's Information Security Policy to determine roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls formally assigned in the Information Security Policy.	No exceptions noted.
CC5.3.8		Inspected the company's Information Security Policy to determine that the company had a third-	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
	The company has a third-party management program in place. Components of this program include: - critical third-party vendor inventory. - vendor's security requirements; and - annual review of critical third-party vendors.	party management program in place that included the security requirements for vendors.	
		Inspected the vendor listing to determine that the critical third-party vendor inventory was in place.	No exceptions noted.
		Inspected the vendor review to determine that a review of critical third-party vendors was performed annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: 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.			
CC6.1.1	The company's Information Security Policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company's Information Security Policy to determine that the Information Security Policy documented the requirements for adding, modifying, and removing user access.	No exceptions noted.
CC6.1.2	The company has a Confidential Information Policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the company's Confidential Information Policy to determine that the company had a Confidential Information Policy in place to help ensure that confidential data was properly secured and restricted to authorized personnel.	No exceptions noted.
CC6.1.3	The company's databases housing sensitive customer data are encrypted at rest.	Inspected the encryption configurations to determine that the company databases housing sensitive customer data are encrypted at rest.	No exceptions noted.
CC6.1.4	The company restricts privileged access to encryption keys to authorized users with a business need.	Inspected the company's Information Security Policy and AWS user list to determine that the company restricted privileged access to encryption keys to authorized users with a business need.	No exceptions noted.
CC6.1.5	Role-based access is configured within AWS and other supporting applications to enforce the segregation of duties and restrict access to confidential information.	Inspected the system configuration for AWS and other supporting applications to determine that role-based access was configured to enforce segregation of duties and restrict access to confidential information.	No exceptions noted.

	TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
	LOGICAL AND PHYSICAL ACCESS CONTROLS		
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC6.1.6	The company restricts privileged access to the network, application, databases, and supporting cloud infrastructure to authorized users with a business need.	Inspected the list of users with privileged access to the cloud infrastructure and application to determine that the company restricted privileged access to the network, application, databases, and supporting cloud infrastructure to authorized users with a business need.	No exceptions noted.
CC6.1.7	The company restricts privileged access to the firewall to authorized users with a business need.	Inspected the list of users with privileged access to the firewall to determine that the company restricted privileged access to the firewall to authorized users with a business need.	No exceptions noted.
CC6.1.8	The firewall is configured to prevent unauthorized access to the company's network.	Inspected the firewall rules to determine that the firewall was configured to prevent unauthorized access to the company's network.	No exceptions noted.
CC6.1.9	The company ensures that user access to in-scope system components is based on job role and function.	Inspected the user access request and in-scope user listings for a sample of new employees to determine that the company ensured that user access to in-scope system components was based on job role and function.	No exceptions noted.
CC6.1.10	The company requires passwords for in-scope system components to be configured according to the company's policy.	Inspected the password configurations and written password policy to determine that the company required passwords for in-scope system components to be configured according to the company's policy.	No exceptions noted.
CC6.1.11	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Inspected the MFA configurations to determine that the company's production systems could only be remotely accessed by authorized employees possessing a valid MFA method.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC6.1.12	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company's Infrastructure as a Service provider's TLS certificate to determine that the company's production systems could only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
CC6.1.13	The company maintains a formal inventory of production system assets.	Inspected an inventory listing of information assets to determine that the company maintained a formal inventory of production system assets.	No exceptions noted.
CC6.1.14	The company's network is segmented to prevent unauthorized access to customer data.	Inspected the network diagram/network configurations to determine that the company's network was segmented to prevent unauthorized access to customer data.	No exceptions noted.
Criteria: 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.			
CC6.2.1	The company's Information Security Policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company's Information Security Policy to determine that the Information Security Policy documented the requirements for adding, modifying, and removing user access.	No exceptions noted.
CC6.2.2	The company conducts semi-annual access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the user access review documentation to determine that the company conducted semi-annual access reviews for the in-scope system components to help ensure that access was restricted appropriately.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	Controls	Detailed Test of Controls	Test Results
CC6.2.3	Logical access to systems is revoked as a component of the termination process within the company's SLAs.	Inspected the user access and offboarding checklist and in-scope user listings for a sample of terminated employees to determine that logical access to systems was revoked as a component of the termination process within the company's SLAs.	No exceptions noted.
CC6.2.4	The company ensures that user access to in-scope system components is based on job role and function.	Inspected the user access request and in-scope user listings for a sample of new employees to determine that the company ensured that user access to in-scope system components was based on job role and function.	No exceptions noted.
CC6.2.5	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company's Infrastructure as a Service provider's TLS certificate to determine that the company's production systems could only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
Criteria: CC6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.3.1	The company's Information Security Policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company's Information Security Policy to determine that the Information Security Policy documented the requirements for adding, modifying, and removing user access.	No exceptions noted.
CC6.3.2	The company conducts semi-annual access reviews for the in-scope system components to	Inspected the user access review documentation to determine that the company conducted semi-	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	Controls	Detailed Test of Controls	Test Results
	help ensure that access is restricted appropriately. Required changes are tracked to completion.	annual access reviews for the in-scope system components to help ensure that access was restricted appropriately.	
CC6.3.3	Logical access to systems is revoked as a component of the termination process within the company's SLAs.	Inspected the user access and offboarding checklist and in-scope user listings for a sample of terminated employees to determine that logical access to systems was revoked as a component of the termination process within the company's SLAs.	No exceptions noted.
CC6.3.4	The company ensures that user access to in-scope system components is based on job role and function.	Inspected the user access request and in-scope user listings for a sample of new employees to determine that the company ensured that user access to in-scope system components was based on job role and function.	No exceptions noted.
CC6.3.5	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company's Infrastructure as a Service provider's TLS certificate to determine that the company's production systems could only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
Criteria: CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
CC6.4.1	Management contracts with AWS using their Amazon Web Services (AWS) to provide physical access security of its production systems; therefore, this criterion is carved out.	This criterion is the responsibility of the subservice organization. Refer to the Subservice organization's section above for controls managed by the subservice organization.	N/A

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	Controls	Detailed Test of Controls	Test Results
Criteria: 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.			
CC6.5.1	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the data retention and disposal procedures to determine that the company had formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	No exceptions noted.
CC6.5.2	The company has electronic media containing confidential information purged or destroyed in accordance with best practices.	Inspected a data deletion record for a sample of data and media disposals to determine that the company had electronic media containing confidential information purged or destroyed in accordance with best practices.	No exceptions noted.
CC6.5.3	The destruction of physical assets hosting the production environment is the responsibility of AWS; therefore, part of this criterion is carved out.	Part of this criterion is the responsibility of the subservice organizations. Refer to the subservice organization's section above for controls managed by the subservice organizations.	N/A
Criteria: CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company's Infrastructure as a Service provider's TLS certificate to determine that the company's production systems could only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
CC6.6.2	The company's production systems can only be remotely accessed by authorized employees possessing a valid MFA method.	Inspected the MFA configurations to determine that the company's production systems could only	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	Controls	Detailed Test of Controls	Test Results
		be remotely accessed by authorized employees possessing a valid MFA method.	
CC6.6.3	The firewall is configured to prevent unauthorized access to the company's network.	Inspected the firewall rules to determine that the firewall was configured to prevent unauthorized access to the company's network.	No exceptions noted.
CC6.6.4	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the company's website and TLS certificate to determine that the company used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.
CC6.6.5	The company uses an Intrusion Detection System (IDS) to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the IDS configurations to determine that the company used an IDS to provide continuous monitoring of the company's network and early detection of potential security breaches.	No exceptions noted.
Criteria: CC6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CC6.7.1	The company encrypts portable media devices when used.	Inspected the company's Information Security Policy to determine that the company encrypted portable media devices when used.	No exceptions noted.
		Inspected the encryption configurations for a sample of devices to determine that the company encrypted portable media devices when used.	No exceptions noted.
CC6.7.2	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the company's website and TLS certificate to determine that the company used secure data transmission protocols to encrypt	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
		confidential and sensitive data when transmitted over public networks.	
Criteria: 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.			
CC6.8.1	The company deploys anti-malware technology to environments commonly susceptible to malicious attacks. The anti-malware software is configured to scan workstations daily and install updates as new updates/signatures are available.	Inspected the anti-malware configurations for a sample of workstations to determine that the company deployed anti-malware technology to environments commonly susceptible to malicious attacks.	No exceptions noted.
		Inspected the anti-malware configurations for a sample of workstations to determine that the anti-malware software was configured to scan workstations daily and install updates as new updates/signatures were available.	No exceptions noted.
CC6.8.2	The company has a formal SDLC methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's Information Security Policy to determine that the company had a formal SDLC methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	Controls	Detailed Test of Controls	Test Results
Criteria: 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.			
CC7.1.1	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	Inspected the company's Information Security Policy to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
		Inspected the documentation for a sample of changes to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
CC7.1.2	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC7.1.3	Vulnerability scans are performed annually on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Inspected the completed vulnerability scan reported to determine that vulnerability scans were performed annually on all external-facing systems.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	Controls	Detailed Test of Controls	Test Results
		Inspected the remediation ticket/notes for a sample of vulnerabilities to determine that critical and high vulnerabilities were tracked to remediation.	No exceptions noted.
CC7.1.4	The company's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate critical and high vulnerabilities in accordance with SLAs.	Inspected the completed penetration report to determine that a penetration test was performed annually.	No exceptions noted
		Per inspection of the penetration test report, there were no critical and high vulnerabilities found during the assessment. Therefore, no testing was performed.	No testing performed.
CC7.1.5	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the company's Information Security Policy to determine that the company had a configuration management procedure in place to ensure that system configurations were deployed consistently throughout the environment.	No exceptions noted.
CC7.1.6	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the company's Information Security Policy to determine that the company's formal policies outlined the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	No exceptions noted.
Criteria: 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.			
CC7.2.1	The company uses an (IDS) to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the IDS configurations to determine that the company used an IDS to provide continuous monitoring of the company's network and early detection of potential security breaches.	No exceptions noted.

	TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
	SYSTEM OPERATIONS		
Control Number	Controls	Detailed Test of Controls	Test Results
CC7.2.2	The company utilizes a log management tool to identify events that may potentially impact the company's ability to achieve its security objectives.	Inspected the log management tool configurations to determine that the company utilized a log management tool to identify events that may potentially impact the company's ability to achieve its security objectives.	No exceptions noted.
CC7.2.3	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the company's Information Security Policy to determine that the company's formal policies outlined the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	No exceptions noted.
CC7.2.4	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected the monitoring tool configurations to determine that an infrastructure monitoring tool was utilized to monitor systems, infrastructure, and performance and generated alerts when specific predefined thresholds were met.	No exceptions noted.
CC7.2.5	Vulnerability scans are performed annually on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Inspected the completed vulnerability scan reported to determine that vulnerability scans were performed annually on all external-facing systems.	No exceptions noted.
		Inspected the remediation ticket/notes for a sample of vulnerabilities to determine that critical and high vulnerabilities were tracked to remediation.	No exceptions noted.
CC7.2.6	The company's penetration testing is performed at least annually. A remediation plan is developed, and changes are	Inspected the completed penetration report to determine that a penetration test was performed annually.	No exceptions noted

	TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
	SYSTEM OPERATIONS		
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
	implemented to remediate critical and high vulnerabilities in accordance with SLAs.	Per inspection of the penetration test report, there were no critical and high vulnerabilities found during the assessment. Therefore, no testing was performed.	No testing performed.
CC7.2.7	Security incidents are reported to the IT personnel and tracked through to resolution in a ticketing system.	Inspected the incident ticket for a sample of security incidents to determine that security incidents were reported to the IT personnel and tracked through to resolution in a ticketing system.	No exceptions noted
Criteria: 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.			
CC7.3.1	The company has security incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Information Security Policy and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.
CC7.3.2	The company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the company's Information Security Policy and Information Security Policy to determine that the company's security incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
		Inspected the incident ticket for a sample of incidents to determine that the company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	Controls	Detailed Test of Controls	Test Results
Criteria: 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.			
CC7.4.1	The company has security incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Information Security Policy and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.
CC7.4.2	The company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the company's Information Security Policy and Information Security Policy to determine that the company's security incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
		Inspected the incident ticket for a sample of incidents to determine that the company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
CC7.4.3	The company tests its Incident response plan at least annually.	Inspected the company's Incident response plan to determine that the Incident response plan was in place and approved by management.	No exceptions noted
		Inspected the company's Incident response plan test notes to determine that the company tests its Incident response plan at least annually.	No exceptions noted

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	Controls	Detailed Test of Controls	Test Results
Criteria: CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	The company has security incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Information Security Policy and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.
CC7.5.2	The company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the company's Information Security Policy and Information Security Policy to determine that the company's security incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
		Inspected the incident ticket for a sample of incidents to determine that the company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
CC7.5.3	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	Controls	Detailed Test of Controls	Test Results
CC7.5.4	The company has a documented BC/DR plan and tests it at least annually.	Inspected the company's BC/DR plan to determine that the company has a documented BC/DR plan.	No exceptions noted.
		Inspected the company's latest disaster recovery plan tabletop exercise meeting minutes to determine that the BC/DR plan was tested annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CHANGE MANAGEMENT			
Control Number	Controls	Detailed Test of Controls	Test Results
Criteria: 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.			
CC8.1.1	The company has a formal SDLC methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's Information Security Policy to determine that the company had a formal SDLC methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.
CC8.1.2	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	Inspected the company's Information Security Policy to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
		Inspected the documentation for a sample of changes to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
CC8.1.3	Segregation of duties are in place to prevent developers to push changes to production.	Inspected the branch protection rule and Github user listing to determine that segregation of duties is in place to prevent developers from pushing changes to production.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CHANGE MANAGEMENT			
Control Number	Controls	Detailed Test of Controls	Test Results
CC8.1.4	The company restricts access to migrate changes to production to authorized personnel.	Inspected the in-scope user listings to production to determine that the company restricted access to production to authorized personnel.	No exceptions noted.
CC8.1.5	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC8.1.6	The company's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate critical and high vulnerabilities in accordance with SLAs.	Inspected the completed penetration report to determine that a penetration test was performed annually.	No exceptions noted
		Per inspection of the penetration test report, there were no critical and high vulnerabilities found during the assessment. Therefore, no testing was performed.	No testing performed.
CC8.1.7	Vulnerability scans are performed annually on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Inspected the completed vulnerability scan reported to determine that vulnerability scans were performed annually on all external-facing systems.	No exceptions noted.
		Inspected the remediation ticket/notes for a sample of vulnerabilities to determine that critical and high vulnerabilities were tracked to remediation.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK MITIGATION			
Control Number	Controls	Detailed Test of Controls	Test Results
Criteria: CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC9.1.2	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Management Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
Criteria: CC9.2: The entity assesses and manages risks associated with vendors and business partners			
CC9.2.1	The company has written agreements in place with vendors and related third parties. These agreements include security and confidentiality commitments applicable to that entity.	Inspected the Terms of Service for vendors to determine that security and confidentiality commitments were in place for vendors and related third parties.	No exceptions noted.
CC9.2.2		Inspected the company's Information Security Policy to determine that the company had a third-	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK MITIGATION			
Control Number	Controls	Detailed Test of Controls	Test Results
	The company has a third-party management program in place. Components of this program include: - critical third-party vendor inventory. - vendor's security requirements; and - annual review of critical third-party vendors.	party management program in place that included the security requirements for vendors.	
		Inspected the vendor listing to determine that the critical third-party vendor inventory was in place.	No exceptions noted.
		Inspected the vendor review to determine that a review of critical third-party vendors was performed annually.	No exceptions noted.