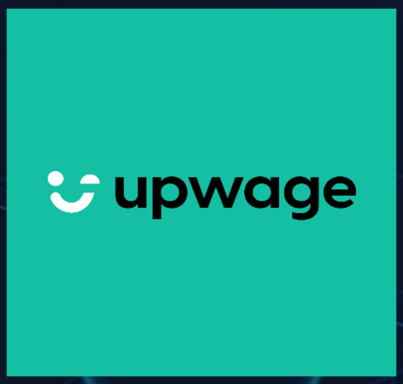
Proprietary & Confidential



SOC 2 Type 1 Report

Upwage, Inc.

System and Organization
Controls Relevant to Security

As of August 9, 2024

Table of Contents

SECTION 1 UPWAGE'S MANAGEMENT'S ASSERTION

September 19, 2024

Assertion of the Management of Upwage, Inc.

We have prepared the accompanying description of Upwage's system about Upwage as of August 9, 2024 based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)*, in AICPA, *Description Criteria*.

The description is intended to provide report users with information about the Upwage system that may be useful when assessing the risks arising from interactions with Upwage's system, particularly information about system controls that Upwage 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*.

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

1) The description presents Upwage system that was designed and implemented as of August 9, 2024, in accordance with the description criteria.
2) The controls stated in the description were suitably designed as of August 9, 2024, to provide reasonable assurance that Upwage's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period.
3) The controls stated in the description operated effectively as of August 9, 2024, to provide reasonable assurance that Upwage's service commitments and system requirements were achieved based on the applicable trust services criteria.

Gregory Call
Co-Founder and COO
Upwage, Inc.

SECTION 2 INDEPENDENT SERVICE AUDITOR REPORT

Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls Relevant to the Principle of Security

To: Upwage, Inc.

Scope

We have examined Upwage's accompanying description of its Upwage system found in Section 3 titled System Description as of August 9, 2024 based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022, in AICPA, Description Criteria, and the suitability of the design and operating effectiveness of controls stated in the description as of August 9, 2024, to provide reasonable assurance that Upwage'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.

Service Organization's Responsibilities

Upwage is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Upwage's service commitments and system requirements were achieved. In Section 1, Upwage has provided the accompanying assertion titled "Assertion of the Management of Upwage" about the description and the suitability of design and operating effectiveness of controls stated therein. Upwage is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

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

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 Tests of Controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in Section 4, "Trust Services Category, Criteria, Related Controls, and Tests of Controls" of this report.

Opinion

In our opinion, in all material respects—

a. The description presents Upwage's system that was designed and implemented as of August 9, 2024 in accordance with the description criteria.
b. The controls stated in the description were suitably designed as of August 9, 2024, to provide reasonable assurance that Upwage's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period.
c. The controls stated in the description operated effectively as of August 9, 2024 to provide reasonable assurance that Upwage's service commitments and system requirements were achieved based on the applicable trust services criteria.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Upwage, user entities of Upwage's system as of August 9, 2024, business partners of Upwage subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- 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.
- 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.

Connor Consulting Corp

San Francisco, California
September 19, 2024

SECTION 3 SYSTEM DESCRIPTION

Overview of Operations

Company Overview

Upwage Inc. is a company that focuses on streamlining the hiring process through the use of artificial intelligence. The company offers an AI-powered screening platform that significantly speeds up the candidate screening process, allowing employers to screen applicants up to 1000 times faster than traditional methods. This service aims to save recruiters considerable time and costs associated with manual screening.

Upwage is also dedicated to improving job accessibility for hourly workers, particularly those earning less than $16 per hour. Their mission includes creating substantial new wealth for these workers by making it easier and faster for them to find competitively paid hourly jobs near their location.

Description of Services Provided

Upwage Inc.'s AI-powered screening platform revolutionizes the recruitment process by significantly accelerating the screening of job applicants. Designed to cater to high-volume hiring needs, this platform uses advanced AI to screen candidates up to 1000 times faster than traditional methods, saving recruiters substantial time and costs.

Wagemap by Upwage Inc. is a cutting-edge tool designed to help hourly workers find better-paying jobs close to their location. It leverages AI and big data to provide users with a map-based interface that displays competitively paid job opportunities in various cities.

AI-Powered Screening Platform Works:

- Role Setup - Recruiters add role-specific qualifying and behavioral questions to the platform.
- AI Screening - Candidates receive an invitation to complete an AI-powered screening, which evaluates their responses in minutes.
- Instant Analysis - The AI analyzes and scores candidate responses 24/7, providing immediate transcripts and evaluations to recruiters.
- Integration - Results are seamlessly integrated with the company's ATS and communication tools like Slack.
- Review and Hiring - Recruiters review AI-generated insights and push qualified candidates through the hiring pipeline. This process significantly reduces the time and cost of candidate screening, ensuring quick and efficient hiring decisions.

Components of the System

Infrastructure

Primary infrastructure used to provide Upwage's Screener services includes the following:

Hardware	Type	Purpose
AWS ECS (Elastic Container Service)	Container Orchestration	Managed container service for running Docker containers, allowing for scalable and flexible application deployment.
AWS RDS Instances	Database	Managed relational database services for storing and managing data securely and efficiently.
AWS S3 Buckets	Storage	Scalable object storage for data such as logs, media, and backups.
AWS VPC	Networking	Virtual Private Cloud for creating isolated network environments.
AWS Route 53	Domain Name System (DNS)	Scalable DNS web service for routing end users to Internet applications.
New Relic	Monitoring and Analytics	Consolidates logs from CloudWatch and CloudTrail, providing real-time monitoring, diagnostics, and analytics.

Hardware	Type	Purpose
Cloudflare	DNS and Security	Provides DNS services, content delivery optimization, and security features such as DDoS protection.
Vercel	Frontend Hosting	Hosts frontend code

Software

Primary software used to provide Upwage's Screener Services includes the following:

Software	Operating System	Purpose
GitHub	Cloud Based Solution	GitHub is our platform for secure code storage and version control. It allows us to manage and track code changes collaboratively, with built-in security features such as branch protections and access controls.
Terraform	Cloud Based Solution	We use Terraform for automated infrastructure deployments. Terraform enables us to manage our infrastructure as code, ensuring consistency, repeatability, and secure deployments across our cloud environment.
AWS CloudWatch and New Relic	Cloud Based Solution	These tools are used for comprehensive monitoring and alerting across our infrastructure and applications. These tools provide real-time insights and logging for AWS services, application performance monitoring and alerting help us quickly identify and resolve issues.
AWS RDS Snapshots	Cloud Based Solution	This service is used for daily automated backups of our relational databases, ensuring that data is securely stored and can be quickly restored if necessary.
Jira	Cloud Based Solution	Our incident management and ticketing platform. Jira helps us track, manage, and resolve incidents and service requests efficiently, ensuring that all issues are documented and addressed in a timely manner.
Slack and Email	Cloud Based Solution	We use Slack and email for real-time alerts and notifications from New Relic and CloudWatch. This setup ensures that our team is immediately informed of any critical issues or performance anomalies, allowing for prompt action.

People

Upwage staff involved in the setup, management and termination of IT services are the following:

Executive Management – Provides general oversight and strategic planning of operations, ensuring alignment with company goals and vision.

Production team – Responsible for delivering a responsive system that fully complies with the functional specifications. This includes coding, debugging, and implementing new features, as well as verifying that the system complies with the functional specifications through rigorous testing procedures. Engineers conduct functional testing to ensure the system is reliable and meets user needs. They are also responsible for effective provisioning, installation/configuration, operation, and maintenance of systems hardware and software relevant to the system, ensuring optimal performance and security of the IT infrastructure.

Customer Support – Serves customers by providing product and service information, including resolving product and service issues. They act as the primary point of contact for user inquiries and troubleshooting.

Audit and Compliance – Performs regularly scheduled audits relative to defined standards, provides continuous improvement feedback, and assesses legal and regulatory requirements. They ensure that Upwage.inc adheres to industry standards and best practices.

Data

Customer data at Upwage is managed, processed, and stored in accordance with relevant data protection regulations and the specific requirements outlined in our policies. This data is essential for delivering Upwage's AI-powered screening platform and related services. The types of customer data handled by Upwage include, but are not limited to, the following:

Screening Results and Candidate Evaluations: Data generated by the AI platform during the candidate screening process, including metrics, transcripts, and analysis reports.

User Interactions: Data from user interactions, such as logins, form submissions, and activity logs, is captured and analyzed to improve user experience and any platform performance disruptions, managed through Upwage's ticketing system (e.g., Jira).

Processes, Policies and Procedures

At Upwage, we have established a comprehensive set of IT policies and procedures to manage physical security, logical access, computer operations, change control, and data communication standards across our organization. These procedures are designed to ensure the delivery of reliable services while adhering to the highest standards of security and efficiency.

- Logical Access Control: Access to our systems and data is strictly controlled through a formalized access control policy. This policy ensures that access is granted based on the principle of least privilege and is regularly reviewed and amended to address the changing needs of our business and security environment.
- Change Control Procedures: Changes to system configurations, software installations, and other critical components are managed through a structured change management process. This ensures that all changes are reviewed, approved, and documented before implementation, minimizing the risk of unplanned downtime or security vulnerabilities.
- Data Protection and Privacy: Our data protection policies rigorously define how data must be handled, stored, and transmitted. To safeguard sensitive information, data is classified and managed according to its level of sensitivity, and robust encryption methods are employed both at rest and in transit.
- Security Monitoring and Incident Response: We actively monitor our systems for security threats using advanced tools like AWS CloudWatch and New Relic. Our logging and monitoring policy outlines the procedures for recording and analyzing security events, ensuring rapid detection and response to potential security incidents.
- Employee Training and Compliance: All team members are expected to adhere to our documented IT policies and procedures. These documents are easily accessible on our company's intranet, and we conduct regular training sessions to ensure all employees understand their responsibilities related to our system operational procedures.

Our operational procedures are continuously assessed and improved to adapt to new challenges and technologies, ensuring that we remain compliant with industry standards and regulation. By maintaining strict controls and fostering a culture of security and compliance, Upwage effectively manages risks and delivers dependable, secure services to our users.

Upwage performs automatic backups of all customer and system data to protect against catastrophic loss due to unforeseen events that impact the entire system. By default, data will be backed up daily.

Upwage employs AWS CloudWatch, CloudTrail, and New Relic for comprehensive monitoring of all systems, including backend services, databases, and frontend/website logs. We have configured alerts to notify relevant teams when any system metrics deviate from predefined thresholds. These metrics include service uptime, API throughput, external service availability, database performance (CPU, memory, and storage), and messaging queue health (e.g., stale messages).

Alerts are promptly routed to designated Gmail groups and Slack channels to ensure timely response and resolution.

- Change Request and Initiation Processes: All changes are initiated through a formal change request process, documented within Jira. Each request is logged, reviewed, and prioritized based on its impact and urgency. Jira serves as the primary tool for tracking the lifecycle of each change request, from initiation through to resolution.
- Documentation Requirements: Every change must be thoroughly documented in Jira, detailing the rationale, the expected impact, and the steps required for implementation. This documentation ensures transparency and accountability, enabling all stakeholders to understand the changes being made.
- Development Practices: Development and configuration management are handled using GitHub and Terraform. GitHub is used for secure code storage and version control, allowing for collaborative development and tracking of changes. Terraform is employed for managing infrastructure as code, ensuring that infrastructure changes are consistent, repeatable, and easily auditable.
- Quality Assurance Testing (QA): Quality Assurance (QA) testing is a crucial step before any changes are promoted to production. The QA team uses automated testing frameworks integrated with GitHub to verify that all changes meet the required functional and non-functional specifications.
- User Acceptance Testing (UAT): UAT is conducted in an environment that closely mirrors the production setup. This ensures that the changes align with user expectations and business requirements. The results of UAT are documented in Jira, and any necessary adjustments are made based on feedback.
- Approval Procedures: Changes must undergo a multi-tier approval process before being deployed. Approvals are tracked in Jira, ensuring that all changes are authorized by the appropriate management personnel, including relevant stakeholders from the development, operations, and security teams.
- Version Control: GitHub is used to maintain a detailed history of code changes, which allows for auditing, tracking, and, if necessary, rollback of changes. This version control practice is critical for maintaining the integrity of the system and supporting compliance with regulatory requirements.
- Firewall Systems: Upwage uses advanced firewall systems to filter unauthorized inbound and outbound network traffic. These firewalls are configured to deny any network connections that are not explicitly authorized, thereby protecting the system from external threats. Network Address Translation (NAT) functionality is also utilized to manage internal IP addresses, adding an additional layer of security.
- Redundant Infrastructure: To ensure high availability and reliability, Upwage's data communication infrastructure is designed with redundancy at multiple levels. This includes redundant firewalls, routers, and servers. In the event of a primary system failure, the redundant systems are configured to take over seamlessly, minimizing downtime and maintaining service continuity.
- Penetration Testing: Regular penetration testing is conducted by a third-party vendor to assess the security posture of the data communication systems. These tests follow industry-standard methodologies to identify vulnerabilities that could be exploited by malicious actors. The scope of penetration testing includes both network and application layers, as well as the controls and processes that support these systems.
- Vulnerability Scanning: Upwage performs quarterly vulnerability scans, using industry-standard tools provided by third-party vendors. These scans are designed to identify potential security vulnerabilities within the network and communication systems. Scans are scheduled during non-peak times to minimize any impact on system performance. Retests and on-demand scans are conducted as needed, and all findings are documented and addressed promptly.
- Secure Communication Channels: All data communications within Upwage are encrypted using industry-standard protocols such as SSL/TLS. This ensures that data in transit is protected from eavesdropping and tampering. Additionally, communication between critical systems is routed through secure, isolated network segments to further safeguard sensitive data.

Boundaries of the System

The scope of this review includes Upwage's AI-powered screening platform, encompassing the infrastructure, software, and processes that directly support the delivery of these services.

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

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Upwage's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Upwage's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Commitment to Competence

The effectiveness of our controls is tightly linked to the competence of our employees. At Upwage, competence is recognized as the acquisition and maintenance of the necessary skills and knowledge to perform designated roles and responsibilities effectively.

Management's Philosophy and Operating Style

Upwage's management philosophy is centered around proactive engagement and strategic foresight, reflecting a committed adherence to regulatory compliance and industry best practices.

Specific Control Activities Implemented:

- Periodic Briefings on Regulatory and Industry Changes:
- Objective: Ensure management is always informed and responsive to the dynamic regulatory environment and industry trends.
- Activity: Regularly scheduled briefings are held, where updates on regulatory changes and their potential impact on service delivery are discussed. This includes reviews of updates from regulatory bodies relevant to Upwage's operations.
- Outcome: Decisive and informed adjustments to Upwage's operational strategies to remain compliant and competitive.
- Executive Management Meetings:
- Objective: Facilitate strategic discussions on broad organizational initiatives and pertinent issues affecting the company.
- Activity: Executive meetings focus on evaluating the company's performance, discussing significant initiatives, and addressing comprehensive challenges. Topics often include strategic planning, financial forecasts, risk management, and technology advancements.
- Outcome: Strategic decisions that align with Upwage's long-term goals and immediate operational needs, ensuring a cohesive approach to management and corporate governance.

Organizational Structure and Assignment of Authority and Responsibility

Executive Management:

- CEO (Chief Executive Officer): Diana Tsai oversees the entire company, providing strategic direction and leadership.
- COO (Chief Operating Officer): Greg Call is responsible for managing daily operations and ensuring that the company's activities align with strategic goals.

Marketing:

- Head of Marketing: Elliot Manson leads marketing strategies to promote Upwage's products and services.
- Senior Business Operations Manager: Julia Wang oversees business operations, ensuring efficiency and productivity.
- Talent Acquisition & Customer Success: Phil Maligsa manages recruitment processes and customer satisfaction initiatives.

Technology and Product Development:

- CTO (Chief Technology Officer): Nate Babbel is in charge of the company's technological direction and innovation.
- Product Manager: Santiago Leon oversees product development and lifecycle management.
- Head of Data and Data Protection Officer: Sameer Saadi manages data strategy, ensuring data integrity and security. He also ensures compliance with data protection regulations and oversees the implementation of data privacy measures.
- Head of Integrations: Mike Dee leads the integration of Upwage's systems with other platforms.
- Senior Frontend Engineers: Justen Phelps and Ryan Walsh are responsible for developing and maintaining the user interface and experience.
- Senior Backend Engineer: Tamas Kalman ensures the robustness and efficiency of the server-side logic and database management.

This organizational structure allows Upwage Inc. to efficiently manage its operations, maintain strong customer relationships, and drive technological innovation. Each role is essential in ensuring that the company meets its strategic objectives and delivers high-quality services to its clients.

Human Resources Policies and Procedures

Upwage’s commitment to excellence is embodied in our Human Resources policies, which are foundational to our success. These policies ensure that we hire, retain, and develop top-quality personnel who drive our company’s efficiency and uphold our high ethical standards.

Specific Control Activities:

- Recruitment and Hiring:
  - Objective: Attract and select candidates who align with Upwage’s values of integrity and professionalism.
  - Activity: Utilize robust screening processes including competency tests and integrity checks. Leverage both internal referrals and external recruiting agencies that adhere to our ethical standards.
  - Outcome: Recruitment of personnel who are not only skilled but also committed to our values.
- Orientation and Training:
  - Objective: Ensure new employees understand Upwage’s operations, culture, and expectations.
  - Activity: Comprehensive orientation programs that cover company policies, data security protocols, and role-specific responsibilities. Ongoing training sessions are held to keep skills updated.
  - Outcome: Well-informed employees who are prepared to contribute effectively from the start.
- Performance Evaluation:
  - Objective: Regularly assess employee performance to ensure alignment with organizational goals.
  - Activity: Annual performance reviews combined with continuous feedback mechanisms.

    - Outcome: Identification of high performers for promotions and targeted development plans for those needing improvement.
- Employee Counseling and Support:
    - Objective: Support employee well-being and professional growth.
    - Activity: Access to professional counseling services and career development programs.
    - Outcome: A resilient workforce that feels valued and supported.
- Compensation and Promotions:
    - Objective: Reward and motivate employees based on merit and contribution to the organization.
    - Activity: Compensation assessment is based on a combination of performance evaluations, market rate analyses, and individual contributions to company goals. Criteria for career advancement are informed by managerial assessments and alignment with organizational needs, which are communicated to employees through one-on-one reviews.
    - Outcome: Fair and motivating compensation and promotion practices that encourage longevity and loyalty.
- Disciplinary Actions:
    - Objective: Address and rectify behaviors or practices that are against company policies.
    - Activity: Formal disciplinary procedures that ensure fair treatment and due process.
    - Outcome: Maintenance of high ethical and professional standards across the organization.

Risk Assessment Process

Upwage's risk assessment process is pivotal in managing risks that may impact the organization's ability to deliver reliable services to user organizations. This comprehensive process engages management across various departments to identify significant risks inherent in the offerings and operations under their charge. The process is structured as follows:

- Identification of Assets and Associated Risks: Initially, all assets within the scope of Upwage's information security program are identified. These include, but are not limited to, documents, applications, IT equipment, and external services which impact confidentiality, integrity, and/or availability of information within the organization.
- Threat and Vulnerability Assessment: Each asset is then analyzed to determine associated threats and vulnerabilities, capturing these in a detailed risk assessment table. This helps in understanding the potential threats and the weaknesses they may exploit.
- Risk Evaluation: For each identified risk, the likelihood of occurrence and the potential impact on the organization are assessed. This quantitative analysis involves scoring risks based on predefined criteria, thus helping in prioritizing the risks based on their probable impact and frequency.
- Risk Treatment: Following evaluation, suitable treatment options are identified for each risk. These treatment options might involve mitigating the risk, transferring it to a third party (e.g., through insurance), avoiding the risk, or accepting it based on cost-benefit analysis. This helps in reducing the risks to acceptable levels as determined by the organization’s risk appetite.
- Monitoring and Review: The risk assessment process is ongoing, with regular reviews and updates necessary to account for new assets, changing threats, and external environmental changes. This dynamic approach ensures that the organization remains vigilant and responsive to emerging risks, thereby safeguarding its operational capabilities and business continuity.

This structured and strategic approach aligns Upwage’s operations closely with its key stakeholders’ expectations, effectively manages uncertainty, minimizes threats, and leverages opportunities in the rapidly evolving market. Through continuous communication and collaboration across leadership teams, Upwage actively identifies, assesses, manages, and mitigates significant risks, thereby enhancing resilience and operational excellence.

Information and Communication Systems Overview

Our company operates as a fully remote organization, leveraging a combination of automated and manual systems to ensure efficient identification, capture, and exchange of information. The primary communication tools include Zoom, Slack, and email, which are supplemented by other platforms and processes to facilitate seamless communication and collaboration across all teams.

Monitoring

Upwage's management is actively involved in monitoring controls to ensure they operate as intended and are modified to adapt to changing conditions. This ongoing process is crucial for maintaining the integrity and reliability of our services.

- Ongoing Monitoring Activities: Upwage management engages regularly in quality assurance monitoring. This involves frequent review and testing of existing controls to assess their effectiveness in real-world scenariosUse of Automated Tools: Upwage employs advanced monitoring tools such as AWS CloudWatch and Elastic Cloud, which help in real-time monitoring of operational performance and system health. These tools alert key personnel in case of system failures or any anomalous activities, ensuring rapid response and minimization of potential disruptions.
- Security Vulnerability Assessments: Regular penetration testing, and vulnerability assessments are conducted to identify and address security weaknesses. These tests are performed bi-annually by independent third-party service providers, ensuring an unbiased evaluation of our security posture.
- Tracking and Remediation: Any security vulnerabilities identified during assessments are tracked and managed through Jira, a project management tool. This system helps Upwage to efficiently prioritize and address vulnerabilities based on their severity and potential impact on the organization.
- Employee Training and Awareness: Continuous training programs are provided for employees based on the results of monitoring activities. These trainings are designed to address any identified weaknesses and to enhance understanding and compliance with company policies and procedures.
- Reporting and Escalation: A robust incident response plan allows for the prompt detection and management of security incidents. Vulnerabilities or incidents that are identified are escalated according to their severity, with high-risk issues being addressed immediately.
- Evaluation of Control Variances: Management continually assesses the operation of Upwage's internal controls through close monitoring of security and system logs, which are comprehensively recorded and analyzed. This helps in identifying any significant deviations from expected control operations which may necessitate adjustments to policies or procedures.
- Corrective Actions: Necessary corrective actions are implemented to address any deviations or deficiencies found during monitoring activities. These actions ensure compliance with company standards and legal requirements, enhancing the overall security and performance of Upwage's operations.

Significant Changes in the Last 12 Months

Since Upwage's Screener-AI product was launched less than 12 months ago, there have been no significant changes to the services during this period. The focus during the initial months post-launch has been on ensuring stability, gathering user feedback, and making minor enhancements based on early user experiences.

Any updates or changes implemented during this period were part of the planned post-launch refinements and were aimed at improving the user experience and performance of the platform. These changes were incremental and did not constitute significant modifications to the core functionality or service architecture of the Screener-AI product.

As the product matures, Upwage will continue to monitor and document any significant changes as part of its commitment to maintaining a robust and compliant service.

Incidents in the last 3 months

We can confirm that during the SOC Report Period (AICPA DC4), there have been no significant incidents reported. All operations have proceeded as expected, with no disruptions or security breaches affecting our systems or services.

Criteria Not Applicable to the System

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.

Subservice Organizations

Subservice Organization	Nature	Category	Criteria	Control
AWS	AWS provides cloud computing infrastructure, including storage, compute, and networking resources.	Common Criteria – Security	CC1.1 - CC6.1	• Physical security controls (e.g., data center access) • Environmental controls (e.g., fire suppression, power management) • Network security controls (e.g., firewalls, DDoS protection)
Cloudflare	Cloudflare offers content delivery network (CDN) services, DDoS protection, and security solutions for web traffic.	Common Criteria – Security	CC1.1 - CC6.1	• Web application firewall (WAF) configurations • DDoS mitigation strategies • Network security controls
Vercel	Vercel provides a platform for front-end development, hosting, and deployment of web applications.	Common Criteria – Security	CC1.1 - CC6.1	• Access control for deployment pipelines • Application security monitoring • Data encryption in transit and at rest
Pusher	Pusher provides real-time communication APIs for web and mobile applications, including WebSockets and push notifications.		CC1.1 - CC6.1	• Encryption of communication channels • Authentication and authorization mechanisms for API access • Monitoring of service availability
OpenAI	OpenAI offers AI and machine learning services, including APIs for natural language processing and other AI functionalities.		CC1.1 - CC6.1	• Access controls for AI models and data • Monitoring of data usage and access • Encryption and privacy controls for sensitive data processed by AI model

For each organization, the carveout method allows the primary service organization to rely on the subservice organization's controls related to applicable Trust Services Criteria. However, the primary organization assumes that the subservice organization is effectively managing controls related to security, availability, confidentiality, and other relevant criteria. These assumed controls often include physical security, network security, access control, data encryption, and monitoring.

Complimentary User Entity Control Considerations

Upwage was designed with the assumption that certain controls would be implemented by user entities. These controls are essential to complement Upwage's controls and ensure that service commitments and system requirements are achieved. The user-entity controls outlined below should not be regarded as a comprehensive list, but rather as examples of the types of controls that should be employed by all user entities:

- User Authentication Controls: Ensure that robust user authentication mechanisms are in place, such as multi-factor authentication (MFA) and strong password policies, to prevent unauthorized access to Upwage's services.
- Access Management: Implement access controls that restrict access to Upwage's services based on user roles and responsibilities. Regularly review and update access permissions to ensure that only authorized personnel have access to critical systems and data.
- Data Protection Policies: Establish and enforce data protection policies that align with legal and regulatory requirements. This includes data encryption, secure data storage, and proper handling of sensitive information when using Upwage's services.
- Incident Response Plan: Develop and maintain an incident response plan that includes procedures for responding to security incidents or breaches that may involve Upwage's services. Ensure that this plan is regularly tested and updated as needed.
- Regular Security Awareness Training: Conduct regular security awareness training for all users to ensure they understand their responsibilities in protecting the integrity and confidentiality of data when using Upwage's services.
- Secure Configuration of End-User Devices: Ensure that all end-user devices accessing Upwage's services are securely configured, including the use of up-to-date antivirus software, firewalls, and device encryption.
- Data Backup and Recovery: Implement regular data backup procedures to ensure that critical data can be restored in the event of a system failure or data loss incident. Ensure that backups are securely stored and regularly tested for integrity.
- Monitoring and Logging: Establish monitoring and logging mechanisms to detect and respond to unauthorized access, unusual activity, or potential security threats related to the use of Upwage's services.

By implementing these controls, user entities will complement the controls established by Upwage, thereby enhancing the overall security and reliability of the services provided.

SECTION 4 TRUST SERVICES CATEGORY, CRITERIA, AND TESTS OF CONTROLS

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

Connor's examination of the controls of Upwage was limited to the Trust Services Criteria, related criteria and control activities specified by the management of Upwage and did not encompass all aspects of operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205 and ISAE 3000.

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

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of the service organization's personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control environment and corroborate policy and procedure documentation.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether the report meets the criteria, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the service commitments and system requirements based on the applicable trust services criteria
- Understand the infrastructure, software, procedures, and data that are designed, implemented and operated by the service organization
- Determine whether the criteria are relevant to the user entity's assertions
- Determine whether the service organization's controls are suitably designed to provide reasonable assurance that its service commitments and system were achieved based on the applicable trust services criteria

TRUST SERVICES CRITERIA - SECURITY

Security The trust services criteria relevant to security address the need for information and system to be protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the service organization's ability to achieve its service commitments and system requirements.

Security refers to the protection of:

i. information during its collection or creation, use, processing, transmission, and storage and
ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft, or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, altercation, destruction, or disclosure of information.

In the table that follows, the columns have the following meaning:

a. **SOC 2 Criteria** – This column contains, for each criterion evaluated, the reference citation. Each criterion sources from a requirement of the Trust Services Criteria.

b. **Requirement(s)** – This column contains the text of the criterion (requirement) directly from the Trust Services Criteria.

c. **Reference –** This column contains the reference to the control activities in Section III, *Upwage,* which are relevant to the achievement of the criterion. Control activities are found in the subsection **CONTROLS SPECIFIED BY SERVICE ORGANIZATION, TESTING PROCEDURES AND RESULT OF TESTS.**

The purpose of this table is to demonstrate that all SOC 2 control criteria in scope were assessed and that the control activities described in Section III, *Upwage Description* address the SOC 2 control criteria.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CONTROL ENVIRONMENT		
CC1.0	**Criteria**	**Control Activity Specified by the Organization**
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Background checks are conducted on eligible personnel (employees and third parties as deemed necessary by the organization) prior to hire as permitted by local laws. Upwage maintains a documented code of conduct. Eligible personnel are required to acknowledge Upwage's code of conduct during onboarding and annually thereafter. Upwage has a defined disciplinary sanctions process to be enacted when a member of the workforce violates the company's policies or causes a security or privacy incident. Management retains documentation of instances when the disciplinary process was enacted. Personnel responsibilities for information security (including confidentiality, legal, and data-handling requirements), including responsibilities that remain after employment, are communicated to and acknowledged by personnel (e.g., through employment contracts, etc.) Internal communication channels are in place for employees to report failures, events, incidents, policy violations, concerns, and other issues to company management, including anonymous reporting channels if applicable. Management conducts performance evaluations for eligible personnel at least annually. Personnel, including employees and contractors, are required to sign an agreement that outlines confidentiality requirements (e.g., non-disclosure agreements) prior to hiring. Company policies are accessible to all employees and as appropriate, third parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control. The company's board of directors or a relevant subcommittee meets at least annually with management to discuss company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies. Management has established and documented roles and responsibilities for personnel, including responsibilities for implementation of the risk management and compliance program (e.g., security, privacy, AI, etc.) and oversight activities. The board of directors includes members independent from management who are not involved in performing controls or company operations.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CONTROL ENVIRONMENT		
CC1.0	**Criteria**	**Control Activity Specified by the Organization**
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control. Management has established and documented roles and responsibilities for personnel, including responsibilities for implementation of the risk management and compliance program (e.g., security, privacy, AI, etc.) and oversight activities. Upwage has appointed and documented the responsibilities of an individual (e.g., data protection officer) responsible for developing, implementing, maintaining and monitoring an organization-wide governance and privacy program and acting as a point of contact with authorities and data subjects to ensure compliance with all applicable laws and regulations regarding the processing of PII. Personnel responsibilities for information security (including confidentiality, legal, and data-handling requirements), including responsibilities that remain after employment, are communicated to and acknowledged by personnel (e.g., through employment contracts, etc.) An organizational chart is in place to describe the organizational structure and reporting lines. The chart is available to all employees (e.g., through the company's HRMS, intranets, etc.) and is updated upon changes to the organizational structure.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CONTROL ENVIRONMENT		
CC1.0	**Criteria**	**Control Activity Specified by the Organization**
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Upwage maintains a documented code of conduct. Eligible personnel are required to acknowledge Upwage's code of conduct during onboarding and annually thereafter. Management evaluates candidates for employment through a formal screening process. The process may include verification of academic and professional qualifications, identity verifications, validation of personal or professional references, technical interviews, or other steps as deemed applicable by the organization. Upwage has documented job descriptions for each position at the company, which include roles and responsibilities as well as required qualifications, skills, and experience for the role. Management conducts performance evaluations for eligible personnel at least annually. Upwage has established training programs to help personnel understand their obligations and responsibilities for information security. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding and annually thereafter. Upwage has established training programs to help personnel understand their obligations and responsibilities for the protection of personally identifiable information (PII) and associated regulatory requirements. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding and annually thereafter.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Upwage maintains a documented code of conduct. Eligible personnel are required to acknowledge Upwage's code of conduct during onboarding and annually thereafter. Upwage has a defined disciplinary sanctions process to be enacted when a member of the workforce violates the company's policies or causes a security or privacy incident. Management retains documentation of instances when the disciplinary process was enacted. Internal communication channels are in place for employees to report failures, events, incidents, policy violations, concerns, and other issues to company management, including anonymous reporting channels if applicable. An organizational chart is in place to describe the organizational structure and reporting lines. The chart is available to all employees (e.g., through the company's HRMS, intranets, etc.) and is updated upon changes to the organizational structure. Management conducts performance evaluations for eligible personnel at least annually.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
COMMUNICATION AND INFORMATION		
CC2.0	**Criteria**	**Control Activity Specified by the Organization**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Upwage uses compliance automation software to identify, select, and continuously monitor internal controls. Upwage has established a data classification policy in order to identify the types of information stored or processed by the entity and the protection measures that are required for each. A dataflow diagram is maintained to show all account data flows across systems and networks. The diagram is reviewed and approved by management at least annually and updated as necessary when there are changes to the environment. Upwage has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control. A documented network diagram is in place to document system boundaries and connections to external networks. The diagram is reviewed and approved by management at least annually and updated as necessary when there are changes to the environment. Management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary based on changes to business objectives or risks to the environment. Company policies are accessible to all employees and as appropriate, third parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
COMMUNICATION AND INFORMATION		
CC2.0	**Criteria**	**Control Activity Specified by the Organization**
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.	Upwage maintains a documented code of conduct. Eligible personnel are required to acknowledge Upwage's code of conduct during onboarding and annually thereafter. Upwage uses compliance automation software to identify, select, and continuously monitor internal controls. Management has defined company objectives, including operational objectives at the entity and functional levels, financial performance goals, and other objectives as appropriate to serve as the basis for risk assessment activities (e.g., objectives related to security, compliance, risk mitigation, etc.). Management communicates its objectives and any changes to those objectives to personnel. Personnel responsibilities for information security (including confidentiality, legal, and data handling requirements), including responsibilities that remain after employment, are communicated to and acknowledged by personnel (e.g., through employment contracts, etc.) Internal communication channels are in place for employees to report failures, events, incidents, policy violations, concerns, and other issues to company management, including anonymous reporting channels if applicable. Upwage has documented job descriptions for each position at the company, which include roles and responsibilities as well as required qualifications, skills, and experience for the role. Upwage's security awareness program includes multiple methods of communicating awareness and educating personnel, such as newsletters, web-based training, in-person training, team meetings, phishing simulations, etc. Periodic security updates are provided to personnel through these multiple methods of communication. An organizational chart is in place to describe the organizational structure and reporting lines. The chart is available to all employees (e.g., through the company's HRMS, intranets, etc.) and is updated upon changes to the organizational structure. Management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary based on changes to business objectives or risks to the environment. Upwage has established training programs to help personnel understand their obligations and responsibilities for information security. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding and annually thereafter. Upwage has established training programs to help personnel understand their obligations and responsibilities for the protection of personally identifiable information (PII) and associated regulatory requirements. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding and annually thereafter. Upwage has an established and documented record of processing activity (ROPA), which includes descriptions of the of lawful collection and use of PII, including the specific purposes for which PII is processed. Company policies are accessible to all employees and as appropriate, third parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter. Upwage provides user guides, help articles, system documentation or other mechanisms to users to share information about the design and operation of the system and its boundaries. The information provided includes functional and nonfunctional requirements related to system processing and information specifications required to support the use of the system.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
COMMUNICATION AND INFORMATION		
CC2.0	**Criteria**	**Control Activity Specified by the Organization**
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company's board of directors or a relevant subcommittee meets at least annually with management to discuss company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies. Upwage communicates service commitments and system requirements to customers and other external parties, as appropriate, through contracts, agreements, company website, etc. Upwage provides notification to relevant parties of any changes to service commitments and system requirements. Upwage notifies customers of any intended changes (including additions and replacements) in subprocessors that process PII so that customers have an opportunity to object to such changes. Upwage communicates system changes via release notes posted on the company's website or via periodic communications. Upwage provides external communication mechanisms to customers (e.g., communication features, support portal, external ticketing system, etc.) to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. Customer support tickets are responded by the support team within defined SLAs. Master service agreements outlining specific requirements are executed with enterprise customers or when the standard terms of service may not apply. Personnel, including employees and contractors, are required to sign an agreement that outlines confidentiality requirements (e.g., non-disclosure agreements) prior to hiring. Upwage provides a contact mechanism for data subjects to submit privacy-related requests or report privacy incidents (e.g., email address, customer portal). Upwage shares information with vendors and third parties only when an executed agreement (e.g., service agreements, business associate agreements, data processing agreements, etc.) is in place that includes security, confidentiality, and privacy requirements for the transfer and processing of information. Upwage maintains a publicly available privacy policy or privacy notice. Upwage maintains a publicly available terms of service for use of the system. All users must agree to the terms of service prior to using the system. Upwage communicates to customers any use of subprocessors to process PII (e.g., through a list of subprocessors in the company website or data processing agreement, etc.). Upwage obtains authorization from customers for the use of subprocessors (e.g., through executed data processing agreements, accepting the terms on the website, etc.). Upwage provides user guides, help articles, system documentation or other mechanisms to users to share information about the design and operation of the system and its boundaries. The information provided includes functional and nonfunctional requirements related to system processing and information specifications required to support the use of the system.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
RISK ASSESSMENT		
CC3.0	**Criteria**	**Control Activity Specified by the Organization**
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Upwage communicates service commitments and system requirements to customers and other external parties, as appropriate, through contracts, agreements, company website, etc. Upwage provides notification to relevant parties of any changes to service commitments and system requirements. Management has defined company objectives, including operational objectives at the entity and functional levels, financial performance goals, and other objectives as appropriate to serve as the basis for risk assessment activities (e.g., objectives related to security, compliance, risk mitigation, etc.). Management communicates its objectives and any changes to those objectives to personnel. Upwage conducts risks assessments periodically as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented. Upwage has defined a formal risk management process that outlines the process for identifying risks and assigning risk owners, the risk tolerance (risk acceptance criteria), and the process for evaluating and treating risks based on the defined tolerance. Upwage's management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
RISK ASSESSMENT		
CC3.0	**Criteria**	**Control Activity Specified by the Organization**
CC3.2	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.	Upwage uses compliance automation software to identify, select, and continuously monitor internal controls. Management has defined company objectives, including operational objectives at the entity and functional levels, financial performance goals, and other objectives appropriate to serve as the basis for risk assessment activities (e.g., objectives related to security, compliance, risk mitigation, etc.). Management communicates its objectives and any changes to those objectives to personnel. Upwage conducts risks assessments periodically as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented. Upwage has defined a formal risk management process that outlines the process for identifying risks and assigning risk owners, the risk tolerance (risk acceptance criteria), and the process for evaluating and treating risks based on the defined tolerance. Upwage's management has documented a risk treatment plan to formally manage risks identified in risk assessment activities. Upwage obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third parties' compliance with industry frameworks, regulations, standards (e.g., SOC 2, ISO, PCI DSS, etc.) and Upwage's requirements. Results of the review and action items, if any, are documented. Upwage performs due diligence activities prior to engaging with a new service provider or vendor (e.g., review of security questionnaires and compliance reports, review of vendor-provided policies, procedures or other documents, analysis of delegated or shared responsibilities with the prospective vendor, etc). Results of the due diligence activities including action items are documented. Upwage maintains a vendor/third party register that includes a description for each of the services provided, vendor risk ratings, results of vendor risk management activities, etc. Agreements with vendors and service providers involved in accessing, processing, storing or managing information assets are reviewed to validate they address all relevant requirements prior to execution. Upwage conducts vulnerability scans of the production environment as dictated by company policy and compliance requirements. Results are reviewed by company personnel and vulnerabilities are tracked to resolution in accordance with company policies.

TRUST SERVICE CRITERIA FOR THE SECURITY CATEGORY		
RISK ASSESSMENT		
CC3.0	**Criteria**	**Control Activity Specified by the Organization**
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Upwage uses compliance automation software to identify, select, and continuously monitor internal controls. Upwage performs an evaluation of fraud risks at least annually, either as a separate evaluation or as part of the overall enterprise risk assessment. The evaluation of fraud risk is performed in accordance with the company's risk assessment methodology. Upwage conducts risks assessments periodically as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented. Upwage has defined a formal risk management process that outlines the process for identifying risks and assigning risk owners, the risk tolerance (risk acceptance criteria), and the process for evaluating and treating risks based on the defined tolerance. Upwage's management has documented a risk treatment plan to formally manage risks identified in risk assessment activities. Upwage has implemented secure login procedures for in-house developed systems to deter enumeration or brute-force attacks (e.g., displaying limited information in login error messages without indicating which data is correct or incorrect, etc.)
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Upwage uses compliance automation software to identify, select, and continuously monitor internal controls. Upwage conducts risks assessments periodically as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented. Upwage has defined a formal risk management process that outlines the process for identifying risks and assigning risk owners, the risk tolerance (risk acceptance criteria), and the process for evaluating and treating risks based on the defined tolerance. Upwage's management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
MONITORING ACTIVITIES		
CC4.0	**Criteria**	**Control Activity Specified by the Organization**
CC4.1	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.	Upwage uses compliance automation software to identify, select, and continuously monitor internal controls. Production resources are monitored through operational tools that send automated alerts to personnel when specific thresholds are crossed. Events are evaluated to determine if they constitute an incident and escalated per policy if necessary. An external penetration test of production environments is performed by an independent third party periodically or after any significant infrastructure or application changes. Results are reviewed by management and vulnerabilities are tracked to resolution in accordance with company policies. Management performs user access reviews periodically (as defined by policy and compliance requirements) to validate user accounts, including third party or vendor accounts, and their associated privileges remain appropriate based on job function. The review includes validation of logical and physical access as necessary. Changes resulting from the review, if any, are documented and implemented. Upwage conducts vulnerability scans of the production environment as dictated by company policy and compliance requirements. Results are reviewed by company personnel and vulnerabilities are tracked to resolution in accordance with company policies.
CC4.2	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.	The company's board of directors or a relevant subcommittee meets at least annually with management to discuss company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies. Upwage uses compliance automation software to identify, select, and continuously monitor internal controls. Upwage conducts risks assessments periodically as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented. Upwage has defined a formal risk management process that outlines the process for identifying risks and assigning risk owners, the risk tolerance (risk acceptance criteria), and the process for evaluating and treating risks based on the defined tolerance. Upwage's management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CONTROL ACTIVITIES		
CC5.0	**Criteria**	**Control Activity Specified by the Organization**
CC5.1	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.	Access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles. Upwage uses compliance automation software to identify, select, and continuously monitor internal controls. Upwage conducts risks assessments periodically as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented. Access to deploy changes to production is restricted to authorized personnel in accordance with segregation of duties principles. Upwage's management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CONTROL ACTIVITIES		
CC5.0	**Criteria**	**Control Activity Specified by the Organization**
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles. Upwage uses compliance automation software to identify, select, and continuously monitor internal controls. An external penetration test of production environments is performed by an independent third party periodically or after any significant infrastructure or application changes. Results are reviewed by management and vulnerabilities are tracked to resolution in accordance with company policies. Upwage conducts risks assessments periodically as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented. Upwage has established training programs to help personnel understand their obligations and responsibilities for information security. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding and annually thereafter. Administrative or privileged access to systems and resources is restricted to authorized personnel. Changes to all system components in the production environment (including software, code, infrastructure, network, configuration changes, etc.) are made according to established procedures that include documentation (change description, justification, evaluation of security impact, approval by authorized parties, rollback procedures) and testing (including security impact testing and code vulnerability testing for custom development changes). Upwage's management has documented a risk treatment plan to formally manage risks identified in risk assessment activities. Company policies are accessible to all employees and as appropriate, third parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter. Upwage conducts vulnerability scans of the production environment as dictated by company policy and compliance requirements. Results are reviewed by company personnel and vulnerabilities are tracked to resolution in accordance with company policies.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CONTROL ACTIVITIES		
CC5.0	**Criteria**	**Control Activity Specified by the Organization**
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Upwage has a documented acceptable use policy that outlines requirements for personnel to use the company's assets. Upwage has documented a policy that establishes requirements for the management of organizational assets. Upwage has a defined business continuity plan those outlines strategies for maintaining operations during a disruption. Upwage maintains a documented code of conduct. Eligible personnel are required to acknowledge Upwage's code of conduct during onboarding and annually thereafter. Upwage has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. Upwage has a documented policy that establishes requirements for the use of cryptographic controls. Upwage has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control. Management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary based on changes to business objectives or risks to the environment. Upwage has defined a formal risk management process that outlines the process for identifying risks and assigning risk owners, the risk tolerance (risk acceptance criteria), and the process for evaluating and treating risks based on the defined tolerance. Company policies are accessible to all employees and as appropriate, third parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter. Upwage has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloging, and assigning risk ratings to vulnerabilities to prioritize remediation efforts.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
LOGICAL AND PHYSICAL ACCESS CONTROLS		
CC6.0	**Criteria**	**Control Activity Specified by the Organization**
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.	System and physical access are revoked within one business day of effective termination date for terminated users (including employees, third parties and vendors, and other personnel). Access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles. Invalid authentication attempts are limited by locking out the user ID after no more than 10 failed attempts. A centralized asset register is maintained for physical, cloud, and other information assets and includes business description, owner, and other attributes deemed relevant by the organization. Upwage uses tags to assign metadata to cloud resources to facilitate identification, inventory, and classification of virtual assets. Upwage has documented policies and procedures for authentication that are communicated to all personnel. These documents include guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc. Upwage has implemented processes to change credentials (secrets, access keys, etc.) periodically based on a defined schedule. Upwage has implemented processes to change cryptographic keys periodically based on a defined schedule. Upwage has implemented segregation mechanisms so that customers cannot impact or access data or resources of other customers. Remote access to production systems is only available through an encrypted connection (e.g., encrypted virtual private network, SSH, etc.) Data at rest is encrypted using strong cryptographic algorithms. Data in transit is encrypted using strong cryptographic algorithms. Upwage has a documented policy that establishes requirements for the use of cryptographic controls. Hard-disk encryption is enabled on all company-managed devices. Upwage retires, replaces or destroys cryptographic keys that are no longer used or needed or when the key expires, the integrity of the key has been weakened, or the key is known or suspected to be compromised, in accordance with documented company policies and procedures. Retired or replaced keys are not used for encryption operations. Upwage has configured account lockout duration following a set number of invalid authentication attempts to a minimum of 30 minutes or until the identity of the user is confirmed (for example, by a system administrator). Authentication to systems requires the use of multi-factor authentication.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
LOGICAL AND PHYSICAL ACCESS CONTROLS		
CC6.0	**Criteria**	**Control Activity Specified by the Organization**
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.	Upwage limits access to system components storing sensitive data (e.g., databases, tables, file folders, etc.) to only those individuals whose job requires such access. Network security controls are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied. System configuration settings are in place to prevent password reuse. Individuals are not allowed to submit a new password that is the same as any of the last four passwords used, at a minimum. A password manager is installed on all company-managed devices. Upwage has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy. Administrative or privileged access to systems and resources is restricted to authorized personnel. Cloud resources are configured to deny public access. Root password authentication to production resources (e.g., virtual machines, containers, etc.) is disabled and only allowed for under exceptional circumstances for a limited time duration based on documented business justification and approval from management. Access to the root account in the cloud infrastructure provider is monitored. Login activity for the root account is investigated and validated for appropriateness. Upwage has implemented technical measures to protect stored user passwords for the system (e.g., encryption, hashing, salting, etc.). Upwage uses network segmentation and/or other techniques to isolate portions of the environment and to control traffic between them based on security and business needs. Group, shared, or generic account usage is prevented unless strictly necessary and supported by documented business justification and management approval. Mechanisms are in place to confirm individual user identity before access to the account is granted and to trace every action to an individual user. Key-management policies and procedures are documented and implemented including generation of strong cryptographic keys, secure distribution, and secure storage of cryptographic keys used to protect sensitive data. Upwage has documented baseline security configuration standards for all system components in accordance with industry-accepted system hardening standards or vendor hardening recommendations. These standards are updated as needed when vulnerabilities are identified and verified to be in place before or immediately after a system component is connected to a production environment. Unique user IDs are used for authentication to systems.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
LOGICAL AND PHYSICAL ACCESS CONTROLS		
CC6.0	**Criteria**	**Control Activity Specified by the Organization**
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.	Access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles. Management performs user access reviews periodically (as defined by policy and compliance requirements) to validate user accounts, including third party or vendor accounts, and their associated privileges remain appropriate based on job function. The review includes validation of logical and physical access as necessary. Changes resulting from the review, if any, are documented and implemented.
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.	Upwage has developed and documented a policy that outlines requirements for access control. System and physical access are revoked within one business day of effective termination date for terminated users (including employees, third parties and vendors, and other personnel). Access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles. Management performs user access reviews periodically (as defined by policy and compliance requirements) to validate user accounts, including third party or vendor accounts, and their associated privileges remain appropriate based on job function. The review includes validation of logical and physical access as necessary. Changes resulting from the review, if any, are documented and implemented. Upwage assigns permissions through groups or roles based on the principle of least privilege and limits the use of wild-card permissions or broad-access patterns.
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.	Management performs user access reviews periodically (as defined by policy and compliance requirements) to validate user accounts, including third party or vendor accounts, and their associated privileges remain appropriate based on job function. The review includes validation of logical and physical access as necessary. Changes resulting from the review, if any, are documented and implemented. Upwage has a documented policy that outlines requirements for physical security. Upwage tracks and documents the return of all electronic and physical assets upon termination as part of the offboarding process. Access mechanisms such as keys, access cards, MFA tokens, are disabled or collected by IT or HR personnel.
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.	Upwage disposes of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures. When Upwage disposes of hard copy materials, it does so through secure means such as cross-cut shredding, incinerating, or pulping, so that sensitive data cannot be reconstructed. Upwage has documented policies and procedures for erasure or destruction of information that has been identified for disposal.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
LOGICAL AND PHYSICAL ACCESS CONTROLS		
CC6.0	**Criteria**	**Control Activity Specified by the Organization**
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Network security controls are in place to restrict public access to remote server administration ports (e.g., SSH, RDP) to authorized IP addresses or address ranges only. Remote access to production systems is only available through an encrypted connection (e.g., encrypted virtual private network, SSH, etc.) Data at rest is encrypted using strong cryptographic algorithms. Data in transit is encrypted using strong cryptographic algorithms. Upwage's systems are configured to automatically log users out after a predefined period of inactivity and/or closure of the system or internet browser. An intrusion detection system (IDS)/intrusion prevention system (IPS) or equivalent is in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected. All remote access to the entity€™s network (including that of users, administrators, and third parties or vendors) requires multi-factor authentication. Authentication to systems requires the use of multi-factor authentication. Network security controls are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied. Upwage has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy. Cloud resources are configured to deny public access. Company-managed devices are configured to enforce a screensaver lock with a timeout of 15 minutes or less. Upwage uses network segmentation and/or other techniques to isolate portions of the environment and to control traffic between them based on security and business needs. A threat detection system is in place to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary. A web application firewall is in place to protect public-facing web applications from outside threats.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
LOGICAL AND PHYSICAL ACCESS CONTROLS		
CC6.0	**Criteria**	**Control Activity Specified by the Organization**
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.	Automated operating system (OS) updates are enabled on company-managed devices to install security patches. Upwage has implemented data leakage prevention mechanisms to systems that process, store or transmit sensitive information. These mechanisms are configured to prevent data leakage and generate audit logs and alerts. Upwage has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. Data in transit is encrypted using strong cryptographic algorithms. Hard-disk encryption is enabled on all company-managed devices. All media with sensitive data is encrypted and/or physically secured to prevent unauthorized persons from gaining access to the data.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The deployed anti-malware solution is configured to detect all known types of malwares and to remove, block, or contain all known types of malware, and is kept current via automatic updates. The implemented anti-malware solutions are configured to perform automatic scans or continuous behavioral analysis of systems or processes when removable electronic media is inserted, connected, or logically mounted within the environment. The implemented anti-malware solutions are configured to perform periodic scans and active or real-time scans or perform continuous behavioral analysis of systems or processes. Antimalware software is installed on all company-managed devices. Upwage has implemented automated mechanisms (e.g., unattended upgrades, automated patching tools, etc.) to install security fixes to systems. Changes to all system components in the production environment (including software, code, infrastructure, network, configuration changes, etc.) are made according to established procedures that include documentation (change description, justification, evaluation of security impact, approval by authorized parties, rollback procedures) and testing (including security impact testing and code vulnerability testing for custom development changes). A threat detection system is in place to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary.

CC7.0 Common Criteria Related to System Operations

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
SYSTEM OPERATIONS		
CC7.0	**Criteria**	**Control Activity Specified by the Organization**
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.	Antimalware software is installed on all company-managed devices. Automated operating system (OS) updates are enabled on company-managed devices to install security patches. An intrusion detection system (IDS)/intrusion prevention system (IPS) or equivalent is in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected. Production resources are monitored through operational tools that send automated alerts to personnel when specific thresholds are crossed. Events are evaluated to determine if they constitute an incident and escalated per policy if necessary. An external penetration test of production environments is performed by an independent third party periodically or after any significant infrastructure or application changes. Results are reviewed by management and vulnerabilities are tracked to resolution in accordance with company policies. Upwage maintains secure and supported configuration standards for application and platform runtimes. Upwage checks software components and libraries for policy and license compliance, security risks, and supported versions (e.g. using software composition analysis (SCA) tools in development pipeline, etc.). If vulnerabilities in these software components or libraries are identified, fixes are implemented in accordance with the company's vulnerability management policies. Upwage uses static application security testing (SAST) or equivalent tool as part of the CI/CD pipeline to detect vulnerabilities in the code base. When vulnerabilities are identified, corrections are implemented prior to release as appropriate based on the nature of vulnerability. Storage buckets that contain sensitive data have versioning enabled to preserve, retrieve, and restore versions of objects. Upwage has documented baseline security configuration standards for all system components in accordance with industry-accepted system hardening standards or vendor hardening recommendations. These standards are updated as needed when vulnerabilities are identified and verified to be in place before or immediately after a system component is connected to a production environment. A threat detection system is in place to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary. Upwage has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloging, and assigning risk ratings to vulnerabilities to prioritize remediation efforts. Upwage conducts vulnerability scans of the production environment as dictated by company policy and compliance requirements. Results are reviewed by company personnel and vulnerabilities are tracked to resolution in accordance with company policies.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
SYSTEM OPERATIONS		
CC7.0	**Criteria**	**Control Activity Specified by the Organization**
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.	Audit logs are enabled and active for all system components and sensitive data in accordance with company policies. Upwage has configured audit logs to trace each action to an individual user. Audit logs contain user identification, type of event, date and time, success and failure indication, origination of event, identity or name of affected data, and system component, resource, or service. Automated audit trails or logs are implemented to capture all changes to identification and authentication credentials (e.g., creation of new accounts, elevation of privileges, changes, additions, or deletions to accounts with administrative access, etc.). Automated audit trails or logs are implemented for all system components to capture all invalid access attempts. Automated audit trails or logs are implemented for all system components to capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts. Automated audit trails or logs are implemented for all system components to capture all creation and deletion of system-level objects. An intrusion detection system (IDS)/intrusion prevention system (IPS) or equivalent is in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected. Upwage has a documented policy that outlines requirements for audit logging and monitoring of system activity at the company. Upwage uses a system that collects and stores logs of system activity and sends alerts to personnel based on pre-configured rules. Access to logs is restricted to authorized personnel. Production resources are monitored through operational tools that send automated alerts to personnel when specific thresholds are crossed. Events are evaluated to determine if they constitute an incident and escalated per policy if necessary. Access to the root account in the cloud infrastructure provider is monitored. Login activity for the root account is investigated and validated for appropriateness. A threat detection system is in place to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary. A web application firewall is in place to protect public-facing web applications from outside threats.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
SYSTEM OPERATIONS		
CC7.0	**Criteria**	**Control Activity Specified by the Organization**
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.	Upwage documents a post-mortem review for identified incidents that includes root-cause analysis, documentation of evidence, and lessons learned as applicable per company policies and procedures. The incident response plan is modified and evolved according to lessons learned and to incorporate industry developments. Upwage has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, classify, and respond to incidents. Upwage has identified and documented incident response team members who have the responsibility and authority to coordinate and execute incident response procedures. Upwage performs a test of all components of the incident response plan and procedures at least annually through different mechanisms including simulated events. The documented plan and procedures are updated if necessary based on the results of the test. Upwage provides notices of breaches and incidents to affected parties and authorities in accordance with company policies and procedures and contractual and legal obligations. Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents and operational issues through an on-call rotation schedule.
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.	Upwage documents a post-mortem review for identified incidents that includes root-cause analysis, documentation of evidence, and lessons learned as applicable per company policies and procedures. The incident response plan is modified and evolved according to lessons learned and to incorporate industry developments. Upwage has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, classify, and respond to incidents. Upwage has identified and documented incident response team members who have the responsibility and authority to coordinate and execute incident response procedures. Upwage performs a test of all components of the incident response plan and procedures at least annually through different mechanisms including simulated events. The documented plan and procedures are updated if necessary based on the results of the test. Upwage provides notices of breaches and incidents to affected parties and authorities in accordance with company policies and procedures and contractual and legal obligations. Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents and operational issues through an on-call rotation schedule. Upwage evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, documented, tracked, and resolved in accordance with company policies and procedures.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
SYSTEM OPERATIONS		
CC7.0	**Criteria**	**Control Activity Specified by the Organization**
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Upwage documents a post-mortem review for identified incidents that includes root-cause analysis, documentation of evidence, and lessons learned as applicable per company policies and procedures. The incident response plan is modified and evolved according to lessons learned and to incorporate industry developments. Upwage has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, classify, and respond to incidents. Upwage has identified and documented incident response team members who have the responsibility and authority to coordinate and execute incident response procedures. Upwage performs a test of all components of the incident response plan and procedures at least annually through different mechanisms including simulated events. The documented plan and procedures are updated if necessary based on the results of the test. Upwage provides notices of breaches and incidents to affected parties and authorities in accordance with company policies and procedures and contractual and legal obligations. Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents and operational issues through an on-call rotation schedule. Upwage evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, documented, tracked, and resolved in accordance with company policies and procedures.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CHANGE MANAGEMENT		
CC8.0	**Criteria**	**Control Activity Specified by the Organization**
CC8.1	The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Access to deploy changes to production is restricted to authorized personnel in accordance with segregation of duties principles. Changes to all system components in the production environment (including software, code, infrastructure, network, configuration changes, etc.) are made according to established procedures that include documentation (change description, justification, evaluation of security impact, approval by authorized parties, rollback procedures) and testing (including security impact testing and code vulnerability testing for custom development changes). Pre-production environments (e.g., development, testing, etc.) are separated from production environments and the separation is enforced with access controls. Upwage has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating software development changes. Upwage has implemented a software update management process where critical patches and application updates are installed for all authorized software within priority SLAs established in company policies. Upwage uses static application security testing (SAST) or equivalent tool as part of the CI/CD pipeline to detect vulnerabilities in the code base. When vulnerabilities are identified, corrections are implemented prior to release as appropriate based on the nature of the vulnerability. Test data is used in testing and development environments to prevent sensitive information from being copied to non-production environments. Changes are tested in an environment separate from production prior to deployment in accordance with the nature of the change. Documented evidence of testing criteria and testing results is retained. Upwage uses a version control system to manage source code, change documentation and tracking, release labeling, and other change management tasks. Access to the version control system is restricted to authorized personnel.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
RISK MITIGATION		
CC9.0	**Criteria**	**Control Activity Specified by the Organization**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Upwage has a defined business continuity plan that outlines strategies for maintaining operations during a disruption. Upwage maintains cybersecurity insurance to mitigate the financial impact of security incidents and business disruptions. Upwage has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. Upwage has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, classify, and respond to incidents. Business-critical resources are deployed or replicated across multiple availability zones or regions.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Upwage has data processing agreements (DPAs) in place with sub-processors that include the minimum technical and organizational measures that the third parties need to implement to meet the objectives of Upwageâ€™s privacy program. Upwage shares information with vendors and third parties only when an executed agreement (e.g., service agreements, business associate agreements, data processing agreements, etc.) is in place that includes security, confidentiality, and privacy requirements for the transfer and processing of information. Upwage obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third parties' compliance with industry frameworks, regulations, standards (e.g., SOC 2, ISO, PCI DSS, etc.) and Upwage's requirements. Results of the review and action items, if any, are documented. Upwage performs due diligence activities prior to engaging with a new service provider or vendor (e.g., review of security questionnaires and compliance reports, review of vendor-provided policies, procedures or other documents, analysis of delegated or shared responsibilities with the prospective vendor, etc). Results of the due diligence activities including action items are documented. Upwage has a documented policy that outlines requirements for managing vendors and third-party relationships through their entire life cycle. Upwage maintains a vendor/third party register that includes a description for each of the services provided, vendor risk ratings, results of vendor risk management activities, etc. Agreements with vendors and service providers involved in accessing, processing, storing or managing information assets are reviewed to validate they address all relevant requirements prior to execution.

SECTION 5 MISCELLANEOUS

Connor noted that client “Upwage” is reliant on Drata as a software SOC2 tool for evidence collection of key internal controls.