Upwage inc

SOC 2 TYPE II REPORT

For the Period November 6, 2025 to February 6, 2026

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

PREPARED BY:

accorp
ACCORP PARTNERS

Table of Contents

SECTION 1 ..... **3**

Independent Service Auditor's Report **3**

SECTION 2 ..... **7**

Management Assertion **7**

SECTION 3 ..... **11**

System Description **11**

Principal Service Commitments and System Requirements **15**

Description of Control Environment, Control Activities, Risk Assessment, Monitoring and Information and Commu **17**

SECTION 4 ..... **29**

Applicable Trust Services Criteria and Related Controls **29**

Tests of Controls and Results of Tests **69**

SECTION 5 ..... **96**

Other Information Provided by Upwage **96**

SECTION 1

Independent Service Auditor's Report

Independent Service Auditor's Report

To: Management of Upwage inc

Scope

We have examined the attached Upwage inc description of the system titled "Upwage" throughout the period November 6, 2025 to February 6, 2026 (description) included in Section 3, based on the criteria set forth in the Description Criteria DC Section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (description criteria) and the suitability of the design and operating effectiveness of controls included in the description throughout the period November 6, 2025 to February 6, 2026 to provide reasonable assurance that Upwage's service commitments and system requirements were achieved based on the trust services criteria for Security set forth in TSP Section 100, 2017 Trust Services Principles and Criteria for *Security, Availability, Processing Integrity, Confidentiality and Privacy* (applicable trust services criteria).

The information included in Section 5, "Other Information Provided by Upwage inc" is presented by the management of Upwage inc to provide additional information and is not a part of Upwage inc's description of its system made available to user entities during the period November 6, 2025 to February 6, 2026.

The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of Upwage inc controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls.

As indicated in the description, Upwage inc uses the subservice organization CLOUDFLARE, VERCEL, and AWS for data center services. The description in Section 3 includes only the controls of Upwage inc and excludes controls of the various subservice organizations. The description also indicates that certain trust service criteria can be met only if the subservice organization's controls, contemplated in the design of Upwage inc's controls, are suitably designed and operating effectively along with related controls at the service organization. Our examination did not extend to controls of various subservice organizations for data center services.

Service Organization's Responsibilities

Upwage inc is responsible for its service commitments and system requirements and for designing controls within the system to provide reasonable assurance that the service commitments and system requirements were achieved.

Upwage inc has provided the accompanying assertion titled, "Management of Upwage inc's Assertion" about the presentation of the Description based on the Description Criteria and suitability of the design of the controls described therein to provide reasonable assurance that the service commitments and system requirement

covered by the Description; (4) identifying the risks that would threaten the achievement of the service organization's service commitments and system requirements; and (5) designing, implementing, and documenting controls to meet the applicable trust services criteria stated in the Description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the presentation of the description based on the description criteria outlined in Upwage inc's assertion, on the suitability of the design of the controls to meet the applicable trust services criteria, and on the operating effectiveness of the controls to meet the applicable trust services criteria, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the description is presented in accordance with the description criteria, (2) the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period November 6, 2025 to February 6, 2026, and (3) the controls stated in the description operated effectively to meet the applicable trust services criteria throughout the period November 6, 2025 to February 6, 2026.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria, the suitability of the design of those controls to meet the applicable trust services criteria, and the operating effectiveness of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the description is not fairly presented, that the controls were not suitably designed to meet the applicable trust services criteria, and that the controls did not operate effectively to meet the applicable trust services criteria. Our examination also included testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust services criteria were met and evaluating the overall presentation of the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each user may consider important to his or her own particular needs. Because of their nature, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, conclusions about the suitability of the design of the controls to meet the applicable trust services criteria are subject to the risks that the system may change or that controls at a service organization may become ineffective.

Opinion

In our opinion, in all material respects, based on the description criteria described in Upwage inc's assertion and the applicable trust services criteria:

a. The description fairly presents the "Upwage" the period November 6, 2025 to February 6, 2026.

February 6, 2026 and if user entities applied the complementary user entity controls, and the subservice organization applied the controls contemplated in the design of Upwage inc controls throughout the period November 6, 2025 to February 6, 2026.

c. The Upwage inc controls stated in the description operated effectively to meet the applicable trust services criteria if user entities applied the complementary user entity controls, and the subservice organization applied the controls contemplated in the design of Upwage inc controls throughout the period November 6, 2025 to February 6, 2026.

Description of Tests of Controls

The specific controls we tested, and the nature, timing, and results of our tests are presented in Section 4 of our report titled "Applicable Trust Services Criteria, Related Controls, and Tests of Controls."

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4 of this report, is intended solely for the information and use of Upwage; user entities of Upwage's systems during the period November 6, 2025 to February 6, 2026; and those prospective user entities, independent auditors and practitioners providing services to such user entities, 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, subservice organizations or other parties
- Internal control and its limitations
- User entity responsibilities, complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria
- The applicable trust services criteria
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks

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

Accorp Partners CPA LLC PAC-FIRM-LIC-47383
Kalispell, Montana
March 07, 2026

SECTION 2

Management Assertion

Company Logo

https://upwage.com | security@upwage.com

Assertion by Management of Upwage inc

February 17, 2026

We have prepared the accompanying description of Upwage inc, system titled "Upwage" throughout the period November 6, 2025 to February 6, 2026 (description), based on the criteria set forth in the Description Criteria DC Section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (description criteria).

The description is intended to provide users with information about "Upwage" that may be useful when assessing the risks arising from interactions with Upwage inc system, particularly information about the suitability of design and operating effectiveness of Upwage inc controls to meet the criteria related to Security set forth in TSP Section 100, *2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy* (applicable trust services criteria).

Upwage inc uses CLOUDFLARE, VERCEL, and AWS subservice organization. The description in Section 3 includes only the controls of Upwage inc and excludes controls of the various subservice organizations. The description also indicates that certain trust services criteria can be met only if the subservice organization's controls, contemplated in the design of Upwage inc controls, are suitably designed and operating effectively along with related controls at the service organization. Our examination did not extend to controls of various subservice organizations for data center services.

The description also indicates that certain trust services criteria specified in the description can be met only if complementary user entity controls contemplated in the design of Upwage inc controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of user entities.

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

a. The description fairly presents the "Upwage" the period November 6, 2025 to February 6, 2026, based on the following description criteria:

    i. The description contains the following information:

        1. The types of services provided
        2. The components of the system used to provide the services, which are:

            a. **Infrastructure.** The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and other telecommunications networks).

c. **People.** The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).

d. **Procedures.** The automated and manual procedures.

e. **Data.** Transaction streams, files, databases, tables, and output used or processed by the system.

3. The boundaries or aspects of the system covered by the description.
4. For information provided to, or received from, subservice organizations or other parties,

   a. How such information is provided or received and the role of the subservice organization and other parties and

   b. The procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

5. The applicable trust services criteria and the related controls designed to meet those criteria, including,, the following:

   a. Complementary user entity controls contemplated in the design of the service organization's system.

   b. When the inclusive method is used to present a subservice organization, controls at the subservice organization

6. If the service organization presents the subservice organization using the carveout method,

   a. The nature of the services provided by the subservice organization and

   b. Each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria.

7. Any applicable trust services criteria that are not addressed by a control at the service organization or a subservice organization and the reasons.
8. In the case of a Type 2 report, relevant details of changes to the service organization's system during the period covered by the description.

ii. The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

b. The controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated and if user entities applied the

c. The Upwage inc controls stated in the description operated effectively throughout the period November 6, 2025 to February 6, 2026 to meet the applicable trust services criteria if user entities applied the complementary user entity controls, and the subservice organization applied the controls contemplated in the design of Upwage inc controls throughout the period November 6, 2025 to February 6, 2026.

Nate Babbel

Signed on March 7, 2026

Signing Authority Name: Nate Babbel

Designation: CTO

SECTION 3

System Description

Background and Overview of Services

Company Background

Upwage Inc. is a technology company founded in 2022 that provides a cloud-based hiring and candidate evaluation platform. Upwage serves employer customers seeking to streamline recruiting workflows and evaluate job applicants through structured, automated interview tools.

Upwage operates as a Software-as-a-Service (SaaS) provider. The platform is accessed via web application and supports employer administrators, recruiters, and hiring managers.

Upwage processes candidate-submitted information on behalf of its employer customers. Employer customers act as data controllers for candidate information, and Upwage acts as a data processor.

Candidate data processed by the system may include:

- Name and contact information
- Resume or employment history
- Interview responses and transcripts
- Structured evaluation outputs

Services provided by Upwage includes below:

Line of Products –

The Upwage platform consists of the following core functional capabilities:

1. Interview and Evaluation Platform

- Creation and configuration of structured interview workflows
- Candidate interview delivery via web interface
- Collection and storage of candidate responses
- Structured evaluation and scoring tools

2. Candidate Management

- Management of candidate records and associated documentation
- Tracking of interview completion status
- Session management and resume functionality
- Employer-directed export of candidate materials

3. Automated Communication Features

- Employer-enabled interview invitations

- Employer-enabled reminder notifications for incomplete sessions
- Controlled, user-initiated sharing of candidate materials

4. System Administration and Access Controls

- Role-based access control
- User account management
- Permission configuration by employer administrators

Subservice Organizations

Upwage utilizes the following subservice providers for data center services that are not included within the scope of this examination. However, Upwage responsibilities for the applications and services run at these cloud services are covered of the audit and in scope. Responsibility matrix is defined of the SLA and agreements with these sub-service organizations.

AWS

AWS has provided an Independent Service Auditor's Report (SOC 2).

The criteria that relate to controls at the subservice organization include all criteria related to the Trust Services Principles of Security (CC1.1 – CC6.1). The types of controls that are necessary to meet the applicable trust services criteria, either alone or in combination with controls at Upwage, include:

• The system is protected against unauthorized physical and logical access. • Environmental safeguards exist for data center facilities. • Network security controls, including firewall and DDoS protections, are implemented.

Cloudflare

Cloudflare has provided an Independent Service Auditor's Report (SOC 2).

The criteria that relate to controls at the subservice organization include all criteria related to the Trust Services Principles of Security (CC1.1 – CC6.1). The types of controls that are necessary to meet the applicable trust services criteria, either alone or in combination with controls at Upwage, include:

• Web application firewall configurations. • DDoS mitigation protections. • Network traffic filtering and monitoring controls.

Vercel

The criteria that relate to controls at the subservice organization include all criteria related to the Trust Services Principles of Security (CC1.1 – CC6.1). The types of controls that are necessary to meet the applicable trust services criteria, either alone or in combination with controls at Upwage, include:

• Access controls for deployment pipelines. • Application security monitoring. • Encryption of data in transit.

OpenAI

OpenAI provides AI model APIs used to support AI-powered features.

The criteria that relate to controls at the subservice organization include all criteria related to the Trust Services Principles of Security (CC1.1 – CC6.1). The types of controls that are necessary to meet the applicable trust services criteria, either alone or in combination with controls at Upwage, include:

• Access controls for AI models and API usage. • Encryption of communications. • Monitoring of data usage and access.

Anthropic

Anthropic provides AI model services used to support AI-powered features.

The criteria that relate to controls at the subservice organization include all criteria related to the Trust Services Principles of Security (CC1.1 – CC6.1). The types of controls that are necessary to meet the applicable trust services criteria, either alone or in combination with controls at Upwage, include:

• Access controls for model APIs. • Encryption of communications. • Monitoring of model usage and activity.

Pusher

Pusher provides real-time messaging and event delivery services.

The criteria that relate to controls at the subservice organization include all criteria related to the Trust Services Principles of Security (CC1.1 – CC6.1). The types of controls that are necessary to meet the applicable trust services criteria, either alone or in combination with controls at Upwage, include:

• Encryption of communication channels. • Authentication and authorization controls for API access. • Monitoring of service availability.

The criteria that relate to controls at the subservice organization include all criteria related to the Trust Services Principles of Security (CC1.1 – CC6.1). The types of controls that are necessary to meet the applicable trust services criteria, either alone or in combination with controls at Upwage, include:

• Secure API authentication mechanisms. • Encryption of data in transit. • Access control and monitoring of analytics data.

Langfuse

Langfuse provides LLM observability, tracing, and prompt monitoring services.

The criteria that relate to controls at the subservice organization include all criteria related to the Trust Services Principles of Security (CC1.1 – CC6.1). The types of controls that are necessary to meet the applicable trust services criteria, either alone or in combination with controls at Upwage, include:

• Access controls for observability data. • Encryption of data in transit. • Activity logging and monitoring controls.

LangSmith

LangSmith provides LLM observability, evaluation, and prompt testing services.

The criteria that relate to controls at the subservice organization include all criteria related to the Trust Services Principles of Security (CC1.1 – CC6.1). The types of controls that are necessary to meet the applicable trust services criteria, either alone or in combination with controls at Upwage, include:

• Access controls for testing environments. • Encryption of data in transit. • Monitoring of evaluation activity.

Hotjar

Hotjar provides product analytics and user behavior insights.

The criteria that relate to controls at the subservice organization include all criteria related to the Trust Services Principles of Security (CC1.1 – CC6.1). The types of controls that are necessary to meet the applicable trust services criteria, either alone or in combination with controls at Upwage, include:

• Secure transmission of analytics data. • Access control and monitoring mechanisms. • Privacy safeguards and data protection controls.

user entities are documented and communicated in customer agreements, the description of the service offering provided online.

Upwage establishes operational requirements that support the achievement of security commitments, relevant CLOUDFLARE, VERCEL, and AWS and regulations, and other system requirements. Such requirements are communicated in Upwage's system policies and procedures, system design documentation, and contracts with customers.

Information security policies define an organization-wide approach how the systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the System.

Components of the System

The System is comprised of the following components:

- Infrastructure including the logical structures, Information Technology (IT) and other hardware.
- Software including application programs and IT system software that support application programs.
- People including executives, sales and marketing, client services, product support, information processing, software development, IT, Finance and Human resources.
- Procedures (automated and manual).
- Data including transaction streams, files, databases, tables, and output used or processed by the system.

The System boundaries include the applications, databases and infrastructure required to directly support the services provided to Upwage's clients. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to Upwage's customers are not included within the boundaries of its system.

Boundaries of the System

The specific products, services and locations that are included in the scope of the report are given below. All other products, services and locations are not included.

Products and Services in Scope

Products:

Upwage Hiring and Candidate Evaluation Platform

Upwage is a web-based SaaS platform that enables employer customers to:

- Create and configure structured interview workflows
- Deliver automated candidate interviews via web interface
- Collect, store, and manage candidate responses and transcripts
- Evaluate candidate responses using structured scoring tools
- Track interview completion and session status
- Export candidate materials at employer direction
- Send employer-enabled automated interview communications

The platform is accessed by authorized employer users through secure authentication controls.

Services:

- SaaS hosting and infrastructure management
- Platform maintenance and updates
- Customer onboarding and support
- Technical support and issue resolution

Geographic Locations in Scope

No physical offices and related physical and availability specific controls are included since Upwage does not have any physical servers and all data is processed on cloud services.

Description of Control Environment, Control Activities, Risk Assessment, Monitoring and Information and Communication

Control Environment

Upwage's internal control environment reflects the overall attitude, awareness, and actions of management concerning the importance of controls, and the emphasis given to controls in the Company's policies, procedures, methods, and organizational structure.

The Chief Executive Officer, the Senior Management Team and all employees are committed to establishing and operating an effective Information Security Management System in accordance with its strategic business objectives. The Management is committed to the Information Security Management System, and ensures that IT Security policies are communicated, understood, implemented, and adhered at all levels of the organization and regularly reviewed for continual suitability.

Integrity and Ethical Values

Upwage requires directors, officers, and employees to observe high standards of business and personal ethics in conducting their duties and responsibilities. Honesty and integrity are core principles of the Company, and all employees are expected to fulfil their responsibilities based on these principles and comply with all applicable laws and regulations. Upwage promotes an environment of open communication and has created an environment where employees are protected from any kind of retaliation should a good faith report of an ethics violation occur. Executive management has the exclusive responsibility to investigate all reported violations and to take corrective action when warranted.

Board of Directors

Business activities at Upwage are under the direction of the Board of Directors. The company is governed by its Board of Directors headed by its chairperson. The chairperson is in charge of the company's operations playing a key role in strategy and client management.

Management's Philosophy and Operating Style

The Executive Management team assesses risks prior to venturing into business ventures and relationships. The Executive Management team interacts with operating management on a daily basis.

Risk Management and Risk Assessment

Risk assessments are performed annually to identify current risk levels, with recommendations to minimize those risks that are determined to pose an unacceptable level of risk to Upwage. As part of this process, security threats are identified and the risk from these threats is formally assessed.

Upwage has operationalized a risk assessment process to identify and manage risks that could adversely affect their ability to provide reliable processing for User Organizations. This process consists of an Information Security team identifying significant risks in their areas of responsibility and implementing appropriate measures to address those risks.

Following steps are involved in performing risk assessments

- Risk identification for each asset in a process and at Organizational level.
- Risk analysis & evaluation for each asset in a process & at Organizational level.
- Risk treatment & residual risk.

Company has also conducted organization-based risk assessment which is based on internal issues, needs and expectations of interested parties etc. The threats, vulnerabilities associated with every asset are evaluated along with threat impact, probability of occurrence and chances of detection (on a rating basis) of the threat. This determines the Risk Factor, which is then put into an equation to derive a risk value. The risk value is then compared to the organizational threshold (i.e., accepted risk value) which is treated appropriately (i.e., treat, transfer, avoid, accept). The identified risks will be treated (mitigated) so that risk levels are reduced. The output of a risk assessment will include a complete risk register and risk treatment plan. Any action plans are tracked to completion. Regular management meetings are held to discuss the security level, changes, technology trends, occurrence of incidents, and security initiatives.

Information Security Policies

Upwage has developed an organization-wide Information Security Policies. All the people impacting Security Policies (IS Policies) are made available to employees via an internal portal. Changes to the Information Security Policies are reviewed by the IS Team and approved by CEO/COO prior to implementation.

Monitoring

Monitoring is a critical aspect of internal control in evaluating whether controls are operating and whether they are modified for changes in business conditions. Management and Information Security personnel monitor the quality of internal control performance routine part of their activities. Performance monitoring reports cover server parameters such space, incoming/outgoing network traffic, packet loss, CPU utilization etc. These system performance reports are reviewed by management on a periodic basis. In addition, a self-assessment scan of vulnerabilities is performed prior every release to the production or on yearly basis. Vulnerabilities are evaluated and remediation actions monitored and completed. Results and recommendations for improvement are reported to management.

Information and Communication

Upwage has documented procedures covering significant functions and operations for each major work group. Policies and procedures are reviewed and updated based upon suggestions from security personnel and approval by management. Departmental managers monitor adherence to policies and procedures of their daily activities. The management holds departmental status meetings, along with strategic planning meetings, to identify and address service issues, customer problems, and project management concerns. The CEO is the focal point for communication regarding the IT environment. Additionally, there are personnel that have been designated to interface with the customer if processing or systems development issues affect customer organizations. Electronic messaging has been incorporated into many of Upwage's processes to provide timely information to employees regarding daily operating activities and to expedite management's ability to communicate with employees.

Electronic Mail (e-Mail)

Communication to Customer organizations and project teams are done through e-mail. Important corporate events, employee news, and cultural updates are some of the messages communicated using e-mail. E-mail is also a means to draw the attention of employees towards adherence to specific procedural requirements. Upwage requires two factor authentication from employees to access their e-mails.

Components of the System

Infrastructure

The infrastructure comprises cloud architecture including database, networking devices, virtual servers, etc.

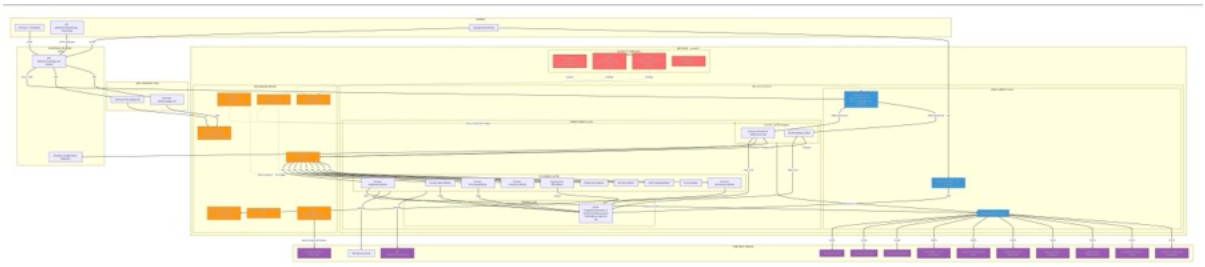
Network Segmentation Overview

The system is hosted in CLOUDFLARE, VERCEL, and AWS in a virtual private cloud (VPC) environment which protects the network from unauthorized external access. The network topology includes segmented VPCs and access control lists (ACLs). Upwage employs IDS and IPS via CLOUDFLARE, VERCEL, and AWS to identify and protect against threats in conjunction with its security policy network settings.

Upwage web-based systems are encrypted using Transport Layer Security (TLS) using certificates from an established third-party certificate authority. Remote access is done through a bastion host with a virtual private network (VPN). The hardware components that make up the aforementioned system include servers hosted, managed, and protected by CLOUDFLARE, VERCEL, and AWS. Production servers at CLOUDFLARE, VERCEL, and AWS maintain failover capabilities in the event of physical hardware or logical software failures. This infrastructure is hosted in high availability data centers with multiple availability zones.

Network Diagram

A network diagram illustrating Upwage's production infrastructure is provided below.



Network Diagram

Network & Endpoint Protection

All systems and devices are protected by the comprehensive endpoint protection system. The endpoints include antivirus, anti-malware, and Trojan protection from any source. This also includes e-mail scanning of the systems which prevents malicious scripts and viruses from e-mails. Apart from which all systems are

content filtering system routed through the proxy server.

Monitoring

Upwage has implemented adequate monitoring controls to detect unauthorized information processing activities. Critical servers and systems are configured to log user activities, Exceptions, and information security events. System administrator and system operator activities are logged and reviewed on a periodic basis.

Capacity Management

Upwage's resources are monitored to ensure system performance meets the expected service levels and minimize the risk of system failure and capacity related issues. Addition of new information systems and facilities, upgrades, new versions and changes are subject to formal system analysis, testing, and approval prior to acceptance.

Patch Management

The respective vertical team ensures that all patches to network device/servers operating systems are tested for stability & availability issues before deploying to the production environment. The patch management activity is done regularly or when any critical event occurs and required updates or patches are installed to ensure efficient working of the servers, desktops, and critical network devices. Operating system patches related and marked critical, and security are managed and applied become available, windows systems are managed through the patch management system and the network devices OS patching is managed automatically while renewing.

Vulnerability Scans & Security Audits

As per the Audit calendar, all the network devices and services are audited for vulnerabilities by doing periodic vulnerability scans. These scans are done by the internal IT Infrastructure team.

Virus Scans and Endpoint Security

An Endpoint Security Solution is installed with the feature of scanning the device automatically and log reports are reviewed by the IT Head. Anti-virus software has been installed on all desktops & laptops within the scope. Updates to the virus definition files are managed and downloaded by the software itself on a daily basis from the vendor website at specific intervals.

People

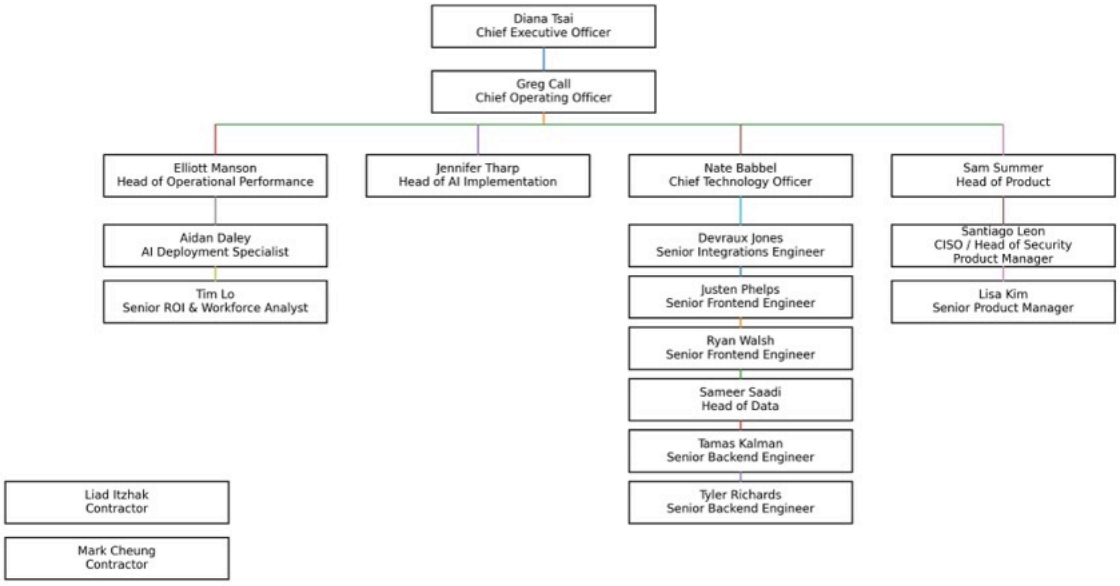
Organizational Structure

The management team meets regularly to review business unit plans and performances. Meetings with the CEO and department heads are held to review operational, security and business issues, and plans for the future.

Upwage's Information Security policies define and assign responsibility/accountabilities for information security. Regular management meetings are held to discuss the security level, changes, technology trends, occurrence of incidents, and security initiatives.

Roles and Responsibilities

The following are the responsibilities of key roles.



Organization Chart

- **Chief Executive Officer (CEO)** The CEO is responsible for overall company leadership and accountability, including setting business strategy, approving key risks and priorities, and ensuring Upwage maintains a culture of security and compliance. The CEO provides executive oversight for information security and compliance performance.
- **Chief Operations Officer (COO):** The COO is responsible for overseeing the company's day-to-day operational functions and ensuring organizational effectiveness. They coordinate across departments to streamline business operations, implement strategic initiatives, and optimize organizational processes. Working closely with the CEO and other executives, the COO translates the company's strategic vision into executable plans, manages resource allocation, and drives operational excellence.
- **Chief Technology Officer (CTO):** The CTO is responsible for technical strategy and delivery, including security architecture, engineering operations, and implementation of security controls within Upwage systems. The CTO ensures secure development practices are followed, that production systems are

- **Head of Data:** The Head of Data is responsible for the governance, integrity, and security of data within Upwage systems. This includes oversight of data architecture, data access controls, data processing workflows, and analytics infrastructure. The Head of Data ensures that data handling practices align with Upwage's security policies, privacy commitments, and retention requirements. This role partners with Engineering and Security to implement appropriate safeguards for customer and candidate data, monitor data quality and integrity, and support audit evidence related to data management controls.
- **Chief Information Security Officer (CISO) / Head of Security:** The CISO is responsible for Upwage's information security program and security governance. This includes maintaining security policies and standards, overseeing risk management, driving SOC 2 control ownership and evidence readiness, coordinating security reviews for new features, and leading incident response coordination. The CISO partners with Engineering and Operations to ensure controls operate effectively and remain audit ready.

Assignment of Authority and Responsibility

Management is responsible for the assignment of responsibility and delegation of authority within Upwage.

Human Resources Policies and Procedures

Upwage maintains written Human Resources Policies and Procedures. The policies and procedures describe practices relating to hiring, training and development, performance appraisal and advancement and the termination. Human Resource ("HR") policies and practices are intended to inform employees on topics such levels of integrity, ethical behaviour, and competence.

The CEO reviews these policies and procedures on a periodic basis to ensure they are updated to reflect changes in the organization and the operating environment. Employees are informed of these policies and procedures upon their hiring during Induction. Personnel policies and procedures are documented in the Human Resources Policy at HRMS Portal.

New Hire Procedures

New employees are required to read and accept HR corporate policies and procedures and are provided online access to these policies. Hiring procedures require that the proper educational levels have been attained along with required job-related certifications, if applicable, and industry experience. If a candidate is qualified, interviews are conducted with various levels of management and staff.

Reference checks are completed for prospective employees. Employees are required to sign Employee Confidentiality Agreement which forms an integral part of the employee file. Discrepancies noted in background investigations are documented and investigated by the CEO, COO, or Head of Operations. Any discrepancies found in background investigations result in disciplinary actions, up to and including employee termination.

New Joiner Trainings

Employees are required to complete security awareness training at the time of joining. Training is documented, monitored, and tracked by management.

Employee Terminations

Termination or change in employment is processed extant HR related procedures. There are clearly identified and assigned responsibilities with regard to termination or change in employment.

Access privileges are revoked upon termination of employment, contract, or agreement. In case of change of employment/role, rights associated with prior roles are removed and new access privileges are created for the current job roles and responsibilities.

Code of Conduct and Disciplinary Action

Upwage has put forward a Code of Conduct and Disciplinary Process in order to encourage and maintain standards of conduct and ensure consistent and fair treatment for all. An employee whose conduct does not comply with an element of the code of conduct and has been found to have breached the same is prosecuted defined process and policies.

Procedures

IT policies and operating instructions are documented. Procedures described cover server management, server hardening, workstation security system, network management, security patch management, user creation, system audit, ID card activation, etc. Additionally, production and training standard operating procedures are available.

Help Desk

Upwage has put in place a helpdesk function to handle problems and support requirements of users, support users in case of incidents and manage them without disruption to business and ensures that changes to any component of Upwage's information assets and infrastructure are controlled and managed in a structured manner. All requests are logged through helpdesk and resolved within the maximum resolution time.

Change Management

Upwage has implemented a well-defined Change Management process to ensure that all changes to the information processing facilities, including equipment, supporting facilities and utilities, networks, application software, systems software and security devices are managed and controlled. The Change Management process describes a methodical approach to handle the changes that are to be made. All the changes need to be subjected to a formal Change Management process.

Every change to such base lined components is governed by the change control and management procedures in the Change Management and Incident Response procedure. Upwage's change management process requires all security patches and system and software configuration changes to be tested before deployment into Stage or Production environments.

All changes are recorded, approved, implemented, tested and versioned before moving to the production environment. The impact of implementing all significant changes are analysed and approved by the IS team before such implementation. A sign-off obtained from the personnel who had requested for the change after implementation of the change.

Incident Response and Management

Procedures for the incident response including identification and escalation of security breaches and other incidents are included in the policy. Users or any other person log all incidents to the Helpdesk. For Network incidents, IT teams receive incident tickets via email and are resolved by them.

The help desk personnel or IT team study and escalate all security incidents to the designated team for further escalation/resolution. All security incidents are reviewed and monitored by the IT Team. Corrective and preventive actions are completed for incidents.

When an incident is detected or reported, a defined incident response process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures and the actions proposed are approved by CTO.

Logical Access

Security Authorization and Administration

Email is sent from HR to the IT helpdesk for all new employees for a new workstation configured with minimum default access to company resources/applications required by an employee to perform the job duty. The default access levels for different departments are defined and documented in HR/Admin policy and IS policies. Any additional access is recommended by the line manager and Head of Engineering. The company has a standard configuration that is implemented across Desktops & laptops individually.

Access to resources is granted to an authenticated user based on the user's identity through a unique login ID that is authenticated by an associated password. Assets are assigned owners who are responsible for evaluating the appropriateness of access based on job roles.

Roles are periodically reviewed and updated by asset owners regularly. Privileged access to sensitive resources is restricted to the IT team and authorized users of the DevOps team. Access to storage, backup data, systems, and media is limited to the IT team through the use of logical access controls.

Security Configuration

Employees establish their identity to the local network and remote systems through the use of a valid unique user ID that is authenticated with the associated password. Passwords are controlled through Password policy of CLOUDFLARE, VERCEL, and AWS and include periodic forced changes, password expiry and complexity requirements. User accounts are disabled after a limited number of unsuccessful logon attempts; the user is required to contact the IT Support team to

reset the password. Local users do not have access to modify password rules. Guest and anonymous logins are not allowed on any machines. Unattended desktops are locked within a time of inactivity. Users are required to provide their password or biometrics to unlock the desktop.

Administrative Level Access

Administrative rights and access to administrative accounts are granted to individuals that require that level of access in order to perform their jobs. All administrative level access, other than to the IT team, must be justified to and approved by the IT team.

Confidentiality

Secure procedures are established to ensure safe and secure disposal of media when no longer required. The level of destruction or disposal of media would depend on the information or data stored in the media and the criticality of the information the information classification guideline.

Backup and Recovery of Data

Upwage has developed formal policies and procedures relating to backup and recovery. Backup procedures are defined in the Backup Policy. Suitable backups are taken and maintained. The backup processes are approved by the business owners and comply with the requirements for business continuity, and legal & regulatory requirements. All backup and restoration logs are maintained for retention periods in the Backup Policy.

Applicable Trust Services Criteria and related Controls

The Security trust services category and related controls are included in section 4 of this report, "Independent Service Auditor's Description of Tests of Controls and Results."

Upwage has determined that Processing Integrity & Privacy trust services Categories are not relevant to the system.

Upwage has determined that the following criteria are not included in the system description.

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. CLOUDFLARE, VERCEL, and AWS is responsible for ensuring the physical security of its data center and accordingly, the physical security controls under this criterion are not in scope.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives. Upwage does not have an office or operates from a working space which is managed by the building management. All environmental security controls are managed by the building management / CLOUDFLARE, VERCEL, and AWS.

User-Entity Control Considerations

Services provided by Upwage to user entities and the controls of Upwage cover only a portion of the overall controls of each user entity. Upwage controls were designed with the assumption that certain controls would be implemented by user entities. In certain situations, the application of specific controls at user entities is necessary to achieve relating to the services outlined in this report to be achieved solely by Upwage. This section highlights those internal control responsibilities that Upwage believes should be present for each user entity and has considered in developing the controls described in the report. This list does not purport to be and should not be considered a complete listing of the controls relevant to user entities. Other controls may be required at user entities.

- User Organizations are responsible for ensuring that complete, accurate and timely information is provided to Upwage for processing.
- User Organizations are ultimately responsible to limit access to only those Upwage employees who are required to perform their job responsibilities and that all users are assigned unique accounts.
- User Organizations are responsible for monitoring and reviewing their business processes.
- User Organizations are responsible for ensuring end customer privacy.
- User Entity should establish confidentiality procedures to ensure that all inputs have been authorized, have been accepted for processing, and are accounted for. Any missing or unaccounted source documents or input files have been identified and investigated. These processes require that exceptions be resolved within a specified time period.
- User Organizations are responsible for defining criteria for processing and rejecting items input into their systems.

- User Organizations are responsible for initiating and implementing changes to the applications managed by User Organizations.

SECTION 4

Applicable Trust Services Criteria& Related Controls

CC1.0 Common Criteria Related to Control Environment			
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	CC1.1.1	At the time of hire, company employees and contractors are required to read and accept the Employee Confidentiality Agreement that includes an intellectual property clause, code of business conduct, ethical standards, and Information Security Policy that includes appropriate use of information technology. The company maintains an up-to-date Employee Handbook and an (including) up-to-date Sanctions Policy. The sanctions policy mentions that a non compliance with the code of business conduct can lead to termination of employees. Personnel, including contractors, are required to formally reaffirm the understanding of the code of conduct and ethical standards on an annual basis.
		CC1.1.2	Established goals and performance objectives for senior employees are reviewed on an annual basis and approved by Executive Management. Management performs annual performance evaluations based on established and approved measurable goals, Key Performance Indicators (KPIs), competency requirements and performance evaluation criteria for employees. During the annual performance evaluation the employees and their supervisor discuss the performance of the employee, their competence, skill matrix gaps and relevant training needs. The training plan is then incorporated within employees' next year's goals. Based on the annual performance evaluation, management identifies employees that are required to go through a performance improvement program. For employees that have not met the objectives or KPIs, management monitors the progress of the performance improvement program.

CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	CC1.2.1	The Board of Directors' oversight responsibilities is defined and documented within the board of directors charter and is acknowledged by the board members on an annual basis. At least annually, the Board of Directors meet to review corporate governance issues, the company strategy, business objectives, capabilities and executions.
		CC1.4.1	Management and the board of directors of organization meet on an annual basis to review the following: - Evaluate the need for additional people, processes, tools, and technologies to achieve the business objectives. - Evaluate the results of annual risk assessment and relevant information resulting from assessments conducted by internal and external parties - Evaluate the business contingency plans - Evaluate succession plans for assignment of responsibility for key roles - Approve the budgets for the organization and - Review the Organization's compensation and performance evaluation programs to retain competent individuals and to identify potential incentives and pressures for employees to commit fraud. - Access the need for a subcommittee, expert or consultant. - Evaluate the skill and expertise of board members.

CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	CC1.3.1	The organization has established an organization chart that defines organizational roles, reporting lines, and authorities relates to development, quality assurance, and security operations of its services. The organization structure is reviewed and updated on an as-needed basis or at least annually.
		CC1.3.2	Roles and responsibilities of senior management and information security employees/contractors are defined in written job descriptions or contractual agreements. For senior management and security related roles, the job description includes duties such oversight, management, and monitoring of security activities, and are communicated to the employees/contractors during the onboarding process. The job descriptions are reviewed and updated on an basis or at least annually.

CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	CC1.1.2	Established goals and performance objectives for senior employees are reviewed on an annual basis and approved by Executive Management. Management performs annual performance evaluations based on established and approved measurable goals, Key Performance Indicators (KPIs), competency requirements and performance evaluation criteria for employees. During the annual performance evaluation the employees and their supervisor discuss the performance of the employee, their competence, skill matrix gaps and relevant training needs. The training plan is then incorporated within employees' next year's goals. Based on the annual performance evaluation, management identifies employees that are required to go through a performance improvement program. For employees that have not met the objectives or KPIs, management monitors the progress of the performance improvement program.
		CC1.4.1	Management and the board of directors of organization meet on an annual basis to review the following: - Evaluate the need for additional people, processes, tools, and technologies to achieve the business objectives. - Evaluate the results of annual risk assessment and relevant information resulting from assessments conducted by internal and external parties - Evaluate the business contingency plans - Evaluate succession plans for assignment of responsibility for key roles - Approve the budgets for the organization and - Review the Organization's compensation and performance evaluation programs to retain competent individuals and to identify potential incentives and pressures for employees to commit fraud. - Access the need for a subcommittee, expert or consultant. - Evaluate the skill and expertise of board members.

CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	CC1.4.3	Management utilizes a pre-hire checklist to ensure that the hiring manager has assessed the qualification of candidates during the hiring process to confirm that they can perform the necessary job requirements.
		CC2.2.1	The organization has policies and procedures for information security, business code of conduct and operating practices. Internal policy and procedure documents relating to security are maintained and made available to employees. The policies and procedure documents are reviewed and approved by management annually or during significant changes.

CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	CC1.1.1	At the time of hire, company employees and contractors are required to read and accept the Employee Confidentiality Agreement that includes an intellectual property clause, code of business conduct, ethical standards, and Information Security Policy that includes appropriate use of information technology. The company maintains an up-to-date Employee Handbook and an (including) up-to-date Sanctions Policy. The sanctions policy mentions that a non compliance with the code of business conduct can lead to termination of employees. Personnel, including contractors, are required to formally reaffirm the understanding of the code of conduct and ethical standards on an annual basis.
		CC1.1.2	Established goals and performance objectives for senior employees are reviewed on an annual basis and approved by Executive Management. Management performs annual performance evaluations based on established and approved measurable goals, Key Performance Indicators (KPIs), competency requirements and performance evaluation criteria for employees. During the annual performance evaluation the employees and their supervisor discuss the performance of the employee, their competence, skill matrix gaps and relevant training needs. The training plan is then incorporated within employees' next year's goals. Based on the annual performance evaluation, management identifies employees that are required to go through a performance improvement program. For employees that have not met the objectives or KPIs, management monitors the progress of the performance improvement program.

CC2.0 Common Criteria Related to Information and Communication			
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	CC2.1.3	The company maintains an inventory of production information assets including details on asset ownership, data classification and location. The asset inventory listing is reviewed and updated by management on an as-needed basis.
		CC2.2.1	The organization has policies and procedures for information security, business code of conduct and operating practices. Internal policy and procedure documents relating to security are maintained and made available to employees. The policies and procedure documents are reviewed and approved by management annually or during significant changes.
		CC2.2.2	The company has established communication channels that allow employees to securely and anonymously report issues related to fraud, harassment and other issues impacting the organization's ethical and integrity requirements.
		CC2.3.2	The company posts a contact form and office locations on its website for customers and other external users to communicate/report system information on failures, incidents, concerns, and other complaints to appropriate personnel. A ticket-tracking system is used for managing customer issues. Reported incidents are addressed by the organization's support staff and tracked to resolution.

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.	CC1.3.2	Roles and responsibilities of senior management and information security employees/contractors are defined in written job descriptions or contractual agreements. For senior management and security related roles, the job description includes duties such oversight, management, and monitoring of security activities, and are communicated to the employees/contractors during the onboarding process. The job descriptions are reviewed and updated on an basis or at least annually.
		CC1.4.1	Management and the board of directors of organization meet on an annual basis to review the following: - Evaluate the need for additional people, processes, tools, and technologies to achieve the business objectives. - Evaluate the results of annual risk assessment and relevant information resulting from assessments conducted by internal and external parties - Evaluate the business contingency plans - Evaluate succession plans for assignment of responsibility for key roles - Approve the budgets for the organization and - Review the Organization's compensation and performance evaluation programs to retain competent individuals and to identify potential incentives and pressures for employees to commit fraud. - Access the need for a subcommittee, expert or consultant. - Evaluate the skill and expertise of board members.
		CC2.2.1	The organization has policies and procedures for information security, business code of conduct and operating practices. Internal policy and procedure documents relating to security are maintained and made available to employees. The policies and procedure documents are reviewed and approved by management annually or during significant changes.

CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	CC2.2.2	The company has established communication channels that allow employees to securely and anonymously report issues related to fraud, harassment and other issues impacting the organization's ethical and integrity requirements.
		CC2.2.3	Significant changes to people, roles and responsibilities for key personnel are internally communicated to all personnel via e-mail or the internal communication tool.
		CC2.2.4	Employees are required to complete information security and awareness training upon hire and at least annually.
		CC2.2.5	The organization has developed documentation and user guides that describe relevant system components purpose and design of the system. These documents are made available to both internal and external users and updated. The documentation also describes the organization and the product/service delivered.
		CC8.1.5	A communication procedure is maintained that describes how employees and customers are notified of a potential application outage, planned or unplanned downtime, changes to application and its functionality, security events and major releases. The communication procedure is reviewed and updated, however at minimum the procedure is updated annually. Internal and external system users are notified through email or internal communication tools for releases prior to system changes which will affect job responsibilities and commitments to the customers.

CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	CC1.4.1	Management and the board of directors of organization meet on an annual basis to review the following: - Evaluate the need for additional people, processes, tools, and technologies to achieve the business objectives. - Evaluate the results of annual risk assessment and relevant information resulting from assessments conducted by internal and external parties - Evaluate the business contingency plans - Evaluate succession plans for assignment of responsibility for key roles - Approve the budgets for the organization and - Review the Organization's compensation and performance evaluation programs to retain competent individuals and to identify potential incentives and pressures for employees to commit fraud. - Access the need for a subcommittee, expert or consultant. - Evaluate the skill and expertise of board members.
		CC2.2.2	The company has established communication channels that allow employees to securely and anonymously report issues related to fraud, harassment and other issues impacting the organization's ethical and integrity requirements.
		CC2.2.5	The organization has developed documentation and user guides that describe relevant system components purpose and design of the system. These documents are made available to both internal and external users and updated. The documentation also describes the organization and the product/service delivered.

CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	CC2.3.1	The organization has formal agreements in place with customers which acknowledges compliance on security commitments by both parties. The customers' responsibilities including security commitments are documented within the formal agreement and agreed with the customers during the onboarding process. An up-to-date version of the company's Master Service Agreements (MSA) or Terms of services (TOS) agreement with customers is maintained and reviewed at least annually.
		CC2.3.2	The company posts a contact form and office locations on its website for customers and other external users to communicate/report system information on failures, incidents, concerns, and other complaints to appropriate personnel. A ticket-tracking system is used for managing customer issues. Reported incidents are addressed by the organization's support staff and tracked to resolution.
		CC8.1.5	A communication procedure is maintained that describes how employees and customers are notified of a potential application outage, planned or unplanned downtime, changes to application and its functionality, security events and major releases. The communication procedure is reviewed and updated, however at minimum the procedure is updated annually. Internal and external system users are notified through email or internal communication tools for releases prior to system changes which will affect job responsibilities and commitments to the customers.

CC3.0 Common Criteria Related to Risk Assessment

CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	CC1.2.1	The Board of Directors' oversight responsibilities is defined and documented within the board of directors charter and is acknowledged by the board members on an annual basis. At least annually, the Board of Directors meet to review corporate governance issues, the company strategy, business objectives, capabilities and executions.
		CC1.4.1	Management and the board of directors of organization meet on an annual basis to review the following: - Evaluate the need for additional people, processes, tools, and technologies to achieve the business objectives. - Evaluate the results of annual risk assessment and relevant information resulting from assessments conducted by internal and external parties - Evaluate the business contingency plans - Evaluate succession plans for assignment of responsibility for key roles - Approve the budgets for the organization and - Review the Organization's compensation and performance evaluation programs to retain competent individuals and to identify potential incentives and pressures for employees to commit fraud. - Access the need for a subcommittee, expert or consultant. - Evaluate the skill and expertise of board members.
		CC2.1.2	Management and the board of directors of organization meet on an annual basis to review and evaluate the key internal control measures such and approval of the organization's policies, performance of internal controls assessment, identification of any opportunities for improvements, review resources and budget needs related to information security and compliance frameworks, review assessments conducted by internal and external parties, approve new controls ensuring appropriate mix of both manual and automated controls and preventive and detective controls and consider various ways that fraud and misconduct can occur within the organization, measures to mitigate the risk of fraud.

CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	CC2.3.3	The company has defined a Risk Management Policy, which identifies and determines the risk of meeting operational, reporting and compliance objectives that align with organization's mission. Management performs a formal risk assessment (which includes risks related to security, fraud, legal, regulatory, economic, physical and business environment, competition, customer, vendor relationship, technology changes and information security) on an annual basis or in the event of significant changes. Identified risks along with mitigation strategies are documented and implemented by the organization's executive management within the risk register which includes an inventory of "high" and "critical "risks that relate to the company, operating model, employees, and customers. Appropriate remediations are suggested and follow ups are performed to ensure that internal controls have been established to mitigate such risks. The status of all deficiencies along with residual risks that have been rated or critical for the organization are tracked until satisfactorily resolved.
		CC3.1.1	Management reviews and evaluates activities and processes that are key in meeting an organization's security commitment. On an annual basis management reviews operations, issues relating to internal controls and delivery on key performance metrics.

CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks basis for determining how the risks should be managed.	CC2.3.3	The company has defined a Risk Management Policy, which identifies and determines the risk of meeting operational, reporting and compliance objectives that align with organization's mission. Management performs a formal risk assessment (which includes risks related to security, fraud, legal, regulatory, economic, physical and business environment, competition, customer, vendor relationship, technology changes and information security) on an annual basis or in the event of significant changes. Identified risks along with mitigation strategies are documented and implemented by the organization's executive management within the risk register which includes an inventory of "high" and "critical "risks that relate to the company, operating model, employees, and customers. Appropriate remediations are suggested and follow ups are performed to ensure that internal controls have been established to mitigate such risks. The status of all deficiencies along with residual risks that have been rated or critical for the organization are tracked until satisfactorily resolved.
		CC7.1.2	An automated tool is implemented to perform vulnerability assessment on infrastructure and applications. Vulnerability scans are performed monthly with the scan frequency adjusted,, to meet ongoing and changing commitments and requirements. Management reviews the vulnerabilities and takes necessary actions on vulnerabilities identified and critical. A remediation plan is developed, and changes are implemented to remediate critical and high vulnerabilities at a minimum. The resolution of such vulnerabilities follows the incident response plan.

CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks basis for determining how the risks should be managed.	CC9.2.1	The company has a vendor management policy in place. The policy requires management to maintain critical third-party vendor inventory, baseline of vendor security requirements and periodic evaluation of the performance of critical third-party vendors. On an annual basis, management performs reviews of SOC reports from service providers/vendors to review the appropriateness of scope, impact of identified exceptions and applicable complementary user entity controls. For critical vendors that do not have a SOC report and have access to data or impact the security of the system, a quarterly vendor risk assessment is performed. During this assessment performance, service delivery and compliance with security commitments is also assessed. Corrective actions are taken based on the results of the assessments.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	CC2.3.3	The company has defined a Risk Management Policy, which identifies and determines the risk of meeting operational, reporting and compliance objectives that align with organization's mission. Management performs a formal risk assessment (which includes risks related to security, fraud, legal, regulatory, economic, physical and business environment, competition, customer, vendor relationship, technology changes and information security) on an annual basis or in the event of significant changes. Identified risks along with mitigation strategies are documented and implemented by the organization's executive management within the risk register which includes an inventory of "high" and "critical "risks that relate to the company, operating model, employees, and customers. Appropriate remediations are suggested and follow ups are performed to ensure that internal controls have been established to mitigate such risks. The status of all deficiencies along with residual risks that have been rated or critical for the organization are tracked until satisfactorily resolved.

CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	CC1.4.1	Management and the board of directors of organization meet on an annual basis to review the following: - Evaluate the need for additional people, processes, tools, and technologies to achieve the business objectives. - Evaluate the results of annual risk assessment and relevant information resulting from assessments conducted by internal and external parties - Evaluate the business contingency plans - Evaluate succession plans for assignment of responsibility for key roles - Approve the budgets for the organization and - Review the Organization's compensation and performance evaluation programs to retain competent individuals and to identify potential incentives and pressures for employees to commit fraud. - Access the need for a subcommittee, expert or consultant. - Evaluate the skill and expertise of board members.
		CC2.1.2	Management and the board of directors of organization meet on an annual basis to review and evaluate the key internal control measures such and approval of the organization's policies, performance of internal controls assessment, identification of any opportunities for improvements, review resources and budget needs related to information security and compliance frameworks, review assessments conducted by internal and external parties, approve new controls ensuring appropriate mix of both manual and automated controls and preventive and detective controls and consider various ways that fraud and misconduct can occur within the organization, measures to mitigate the risk of fraud.

CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	CC2.3.3	The company has defined a Risk Management Policy, which identifies and determines the risk of meeting operational, reporting and compliance objectives that align with organization's mission. Management performs a formal risk assessment (which includes risks related to security, fraud, legal, regulatory, economic, physical and business environment, competition, customer, vendor relationship, technology changes and information security) on an annual basis or in the event of significant changes. Identified risks along with mitigation strategies are documented and implemented by the organization's executive management within the risk register which includes an inventory of "high" and "critical "risks that relate to the company, operating model, employees, and customers. Appropriate remediations are suggested and follow ups are performed to ensure that internal controls have been established to mitigate such risks. The status of all deficiencies along with residual risks that have been rated or critical for the organization are tracked until satisfactorily resolved.
		CC9.2.1	The company has a vendor management policy in place. The policy requires management to maintain critical third-party vendor inventory, baseline of vendor security requirements and periodic evaluation of the performance of critical third-party vendors. On an annual basis, management performs reviews of SOC reports from service providers/vendors to review the appropriateness of scope, impact of identified exceptions and applicable complementary user entity controls. For critical vendors that do not have a SOC report and have access to data or impact the security of the system, a quarterly vendor risk assessment is performed. During this assessment performance, service delivery and compliance with security commitments is also assessed. Corrective actions are taken based on the results of the assessments.

CC4.0 Common Criteria Related to Monitoring Activities			
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.	CC2.1.2	Management and the board of directors of organization meet on an annual basis to review and evaluate the key internal control measures such and approval of the organization's policies, performance of internal controls assessment, identification of any opportunities for improvements, review resources and budget needs related to information security and compliance frameworks, review assessments conducted by internal and external parties, approve new controls ensuring appropriate mix of both manual and automated controls and preventive and detective controls and consider various ways that fraud and misconduct can occur within the organization, measures to mitigate the risk of fraud.
		CC4.1.1	External penetration testing is conducted annually by an independent third-party. The results of the test are reviewed by the IT management. If applicable, all high and / or critical findings of penetration tests are remediated in a timely manner added to risk register along with risk treatment plan. High risk items are tracked to resolution following the incident management process.
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,.	CC2.1.2	Management and the board of directors of organization meet on an annual basis to review and evaluate the key internal control measures such and approval of the organization's policies, performance of internal controls assessment, identification of any opportunities for improvements, review resources and budget needs related to information security and compliance frameworks, review assessments conducted by internal and external parties, approve new controls ensuring appropriate mix of both manual and automated controls and preventive and detective controls and consider various ways that fraud and misconduct can occur within the organization, measures to mitigate the risk of fraud.
		CC3.1.1	Management reviews and evaluates activities and processes that are key in meeting an organization's security commitment. On an annual basis management reviews operations, issues relating to internal controls and delivery on key performance metrics.

CC5.0 Common Criteria Related to Control Activities			
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.	CC2.1.2	Management and the board of directors of organization meet on an annual basis to review and evaluate the key internal control measures such and approval of the organization's policies, performance of internal controls assessment, identification of any opportunities for improvements, review resources and budget needs related to information security and compliance frameworks, review assessments conducted by internal and external parties, approve new controls ensuring appropriate mix of both manual and automated controls and preventive and detective controls and consider various ways that fraud and misconduct can occur within the organization, measures to mitigate the risk of fraud.
		CC8.1.3	Source code changes are logged, time-stamped, and attributed to their author in a source code management tool. Access to the source code tool is restricted to authorized users using multi-factor authentication.

CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	CC2.1.3	The company maintains an inventory of production information assets including details on asset ownership, data classification and location. The asset inventory listing is reviewed and updated by management on an as-needed basis.
		CC3.1.1	Management reviews and evaluates activities and processes that are key in meeting an organization's security commitment. On an annual basis management reviews operations, issues relating to internal controls and delivery on key performance metrics.
		CC5.2.1	The IT team continuously monitors system capacity and performance through the use of monitoring tools to identify and detect anomalies that could compromise availability of the system operations. Additionally, the monitoring tool generates alerts when specific predefined thresholds are met. Incident management process is invoked for confirmed events and anomalies. Logs and alerts are tracked until resolved within the change-management/ticketing application.
		CC5.2.2	Access to privileged and generic administrator accounts on the network, databases and servers supporting the application is restricted to authorized personnel based on a role-based access scheme.

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.	CC2.1.2	Management and the board of directors of organization meet on an annual basis to review and evaluate the key internal control measures such and approval of the organization's policies, performance of internal controls assessment, identification of any opportunities for improvements, review resources and budget needs related to information security and compliance frameworks, review assessments conducted by internal and external parties, approve new controls ensuring appropriate mix of both manual and automated controls and preventive and detective controls and consider various ways that fraud and misconduct can occur within the organization, measures to mitigate the risk of fraud.
		CC2.2.1	The organization has policies and procedures for information security, business code of conduct and operating practices. Internal policy and procedure documents relating to security are maintained and made available to employees. The policies and procedure documents are reviewed and approved by management annually or during significant changes.

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

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.	CC2.1.3	The company maintains an inventory of production information assets including details on asset ownership, data classification and location. The asset inventory listing is reviewed and updated by management on an as-needed basis.
		CC2.3.4	A formal network diagram outlining boundary protection mechanisms (e.g. firewalls, IDS, etc.) is maintained for all network connections and reviewed annually by IT management.
		CC5.2.2	Access to privileged and generic administrator accounts on the network, databases and servers supporting the application is restricted to authorized personnel based on a role-based access scheme.
		CC6.1.1	Multi-factor authentication (MFA) is enforced for user accounts with administrative access to the company's production platform.
		CC6.1.2	Unique user IDs and passwords are required to gain access to the application production environment and infrastructure supporting the application (i.e., Active Directory, server, and database accounts). Password settings for applications that store, or handle business critical systems are in accordance with the corresponding password requirements defined in the policy.
		CC6.1.3	System components are configured such that the company and its customers' access is appropriately segmented from other customer accounts.
		CC6.1.4	Management notifies security administrators of terminations of employees or consultants resulting in respective user accounts being disabled within one business day upon termination of employment the offboarding procedures. Management utilizes an employee termination checklist to ensure that the termination process is consistently executed, and access is revoked for terminated employees within one business day.

CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	CC6.1.5	The organization uses its cloud provider key management service to encrypt data at rest and to store and manage encryption keys. Access to the production environment's access keys is restricted to authorized individuals.
		CC6.1.6	Encryption technologies are used to protect communication and transmission of data over public networks.
		CC6.2.1	A ticketing system and/or access request form is used to record granting of new or modified access to the system account based on authorization by the management.
		CC7.1.1	Production systems and servers have been hardened to ensure an appropriate level of security against an established entity standard. Baseline configurations are retained within the infrastructure code and a configuration management tool is used for implementation and for rollback capability anytime an approved configuration change is made. Baseline configurations are reviewed and updated annually or when required due to reviews and system changes, and anytime integral system components are added.

CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	CC6.1.4	Management notifies security administrators of terminations of employees or consultants resulting in respective user accounts being disabled within one business day upon termination of employment the offboarding procedures. Management utilizes an employee termination checklist to ensure that the termination process is consistently executed, and access is revoked for terminated employees within one business day.
		CC6.2.1	A ticketing system and/or access request form is used to record granting of new or modified access to the system account based on authorization by the management.
		CC6.2.2	Management performs a quarterly user access review for all user accounts (including users with administrative privileges) for in-scope system components to ensure that access is restricted appropriately and to identify unauthorized or terminated users. Access is modified or removed in a timely manner based on the results of the review and are tracked to completion.

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.	CC5.2.2	Access to privileged and generic administrator accounts on the network, databases and servers supporting the application is restricted to authorized personnel based on a role-based access scheme.
		CC6.1.4	Management notifies security administrators of terminations of employees or consultants resulting in respective user accounts being disabled within one business day upon termination of employment the offboarding procedures. Management utilizes an employee termination checklist to ensure that the termination process is consistently executed, and access is revoked for terminated employees within one business day.
		CC6.2.1	A ticketing system and/or access request form is used to record granting of new or modified access to the system account based on authorization by the management.
		CC6.2.2	Management performs a quarterly user access review for all user accounts (including users with administrative privileges) for in-scope system components to ensure that access is restricted appropriately and to identify unauthorized or terminated users. Access is modified or removed in a timely manner based on the results of the review and are tracked to completion.

CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	CC6.1.4	Management notifies security administrators of terminations of employees or consultants resulting in respective user accounts being disabled within one business day upon termination of employment the offboarding procedures. Management utilizes an employee termination checklist to ensure that the termination process is consistently executed, and access is revoked for terminated employees within one business day.
		CC6.2.1	A ticketing system and/or access request form is used to record granting of new or modified access to the system account based on authorization by the management.
		CC6.2.2	Management performs a quarterly user access review for all user accounts (including users with administrative privileges) for in-scope system components to ensure that access is restricted appropriately and to identify unauthorized or terminated users. Access is modified or removed in a timely manner based on the results of the review and are tracked to completion.
		CC6.4.1	All production systems are hosted in a cloud environment which is equipped with appropriate physical security controls and is the responsibility of subservice organization. Physical security and environmental controls have been implemented to protect systems inside the server room by the subservice organization. The SOC 2 report of subservice organization is reviewed on an annual basis to evaluate the effectiveness of the controls at the subservice organization.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	CC6.5.1	Formal data retention and disposal policy and procedure are in place to guide the secure retention and disposal of information. After termination of contract, all customer data is retained in accordance with the contractual agreement between the organization and customer.

CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	CC6.1.1	Multi-factor authentication (MFA) is enforced for user accounts with administrative access to the company's production platform.
		CC6.1.6	Encryption technologies are used to protect communication and transmission of data over public networks.
		CC6.6.1	The company uses firewalls and intrusion detection tools and configures them to prevent unauthorized access and detect external security threats. System firewalls are configured on the application gateway and production network to limit unnecessary ports, protocols and services. Firewall rules are reviewed on an annual basis by IT management.

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.	CC5.2.2	Access to privileged and generic administrator accounts on the network, databases and servers supporting the application is restricted to authorized personnel based on a role-based access scheme.
		CC6.1.5	The organization uses its cloud provider key management service to encrypt data at rest and to store and manage encryption keys. Access to the production environment's access keys is restricted to authorized individuals.
		CC6.1.6	Encryption technologies are used to protect communication and transmission of data over public networks.
		CC6.8.1	Anti-virus and Malware protection software is installed and configured on all production servers to prevent or detect and act upon the introduction of unauthorized or malicious software. The Anti-virus is set up to automatically scan on a continuous basis For production servers, the Anti-virus definitions are updated on a weekly basis. Anti-virus and Malware protection software is installed and configured for Mac based workstations and laptops.
		CC7.2.1	Logging is enabled to monitor activities such activities, logon attempts, data deletions at the application and infrastructure level, changes to functions, security configurations, permissions, and roles. Automated alerts are configured to notify IT management of high and critical risk events. The issues identified are resolved in a timely manner through the incident management process. Access to change the log configuration and access to modify logs is restricted.

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.	CC5.2.2	Access to privileged and generic administrator accounts on the network, databases and servers supporting the application is restricted to authorized personnel based on a role-based access scheme.
		CC6.8.1	Anti-virus and Malware protection software is installed and configured on all production servers to prevent or detect and act upon the introduction of unauthorized or malicious software. The Anti-virus is set up to automatically scan on a continuous basis For production servers, the Anti-virus definitions are updated on a weekly basis. Anti-virus and Malware protection software is installed and configured for Mac based workstations and laptops.
		CC8.1.1	A formal change management policy is established that governs the development, implementation, changes, and maintenance of application(s) and supporting infrastructure. System development lifecycle documentation also addresses regular and emergency change processes. The change management process requires that: • Change requests are authorized • Changes are tested prior to migration to production • Changes are reviewed and approved prior to promotion to the production environment. All changes are documented in the internal tool and tracked from initiation through deployment and validation. Emergency changes follow an accelerated timeline and prior to initiating an emergency change, appropriate approval is obtained and documented.
		CC8.1.3	Source code changes are logged, time-stamped, and attributed to their author in a source code management tool. Access to the source code tool is restricted to authorized users using multi-factor authentication.

CC7.0 Common Criteria Related to System Operations

CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	CC7.1.2	An automated tool is implemented to perform vulnerability assessment on infrastructure and applications. Vulnerability scans are performed monthly with the scan frequency adjusted,, to meet ongoing and changing commitments and requirements. Management reviews the vulnerabilities and takes necessary actions on vulnerabilities identified and critical. A remediation plan is developed, and changes are implemented to remediate critical and high vulnerabilities at a minimum. The resolution of such vulnerabilities follows the incident response plan.
		CC7.2.1	Logging is enabled to monitor activities such activities, logon attempts, data deletions at the application and infrastructure level, changes to functions, security configurations, permissions, and roles. Automated alerts are configured to notify IT management of high and critical risk events. The issues identified are resolved in a timely manner through the incident management process. Access to change the log configuration and access to modify logs is restricted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	CC7.3.1	A formal incident management process has been established and implemented which requires incidents to be tracked, documented and resolved in a complete, accurate and timely manner. The process document is reviewed by management on an annual basis and updated. All critical security (including data breaches) incidents are logged and tracked in the ticketing system and communicated to affected parties. Communication is also conducted with senior management for each security incident, to evaluate the root causes, remediation steps, and lessons learned to be able to prevent similar incidents in the future. Incidents are resolved in a timely manner in accordance with the formal incident management process to meet organization's commitments.

CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents,.	CC2.1.4	The company management has established defined roles and responsibilities to oversee the design and implementation of information security policies and controls including incident response and have assigned such roles to the Chief Information Security Officer.
		CC7.3.1	A formal incident management process has been established and implemented which requires incidents to be tracked, documented and resolved in a complete, accurate and timely manner. The process document is reviewed by management on an annual basis and updated. All critical security (including data breaches) incidents are logged and tracked in the ticketing system and communicated to affected parties. Communication is also conducted with senior management for each security incident, to evaluate the root causes, remediation steps, and lessons learned to be able to prevent similar incidents in the future. Incidents are resolved in a timely manner in accordance with the formal incident management process to meet organization's commitments.
		CC7.4.1	A BCDR (Business Continuity and Disaster Recovery) policy, Business Continuity plan and Disaster Recovery plan is documented and reviewed annually. The plan includes the alternative working plans, the roles and responsibilities of key personnel in executing the continuity strategy. There are communication plans in the policy in order to notify of any disaster. The plan also includes the incident response plan. The company conducts testing of the BCDR (Business Continuity and Disaster Recovery) plans, per the defined testing schedule for different loss scenarios. Each loss scenario is tested at least annually. Test results are reviewed and consequently contingency plans are updated. Issues identified during testing are resolved and plans are updated accordingly.

CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	CC7.3.1	A formal incident management process has been established and implemented which requires incidents to be tracked, documented and resolved in a complete, accurate and timely manner. The process document is reviewed by management on an annual basis and updated. All critical security (including data breaches) incidents are logged and tracked in the ticketing system and communicated to affected parties. Communication is also conducted with senior management for each security incident, to evaluate the root causes, remediation steps, and lessons learned to be able to prevent similar incidents in the future. Incidents are resolved in a timely manner in accordance with the formal incident management process to meet organization's commitments.
		CC7.4.1	A BCDR (Business Continuity and Disaster Recovery) policy, Business Continuity plan and Disaster Recovery plan is documented and reviewed annually. The plan includes the alternative working plans, the roles and responsibilities of key personnel in executing the continuity strategy. There are communication plans in the policy in order to notify of any disaster. The plan also includes the incident response plan. The company conducts testing of the BCDR (Business Continuity and Disaster Recovery) plans, per the defined testing schedule for different loss scenarios. Each loss scenario is tested at least annually. Test results are reviewed and consequently contingency plans are updated. Issues identified during testing are resolved and plans are updated accordingly.

CC8.0 Common Criteria Related to Change Management

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.	CC7.1.1	Production systems and servers have been hardened to ensure an appropriate level of security against an established entity standard. Baseline configurations are retained within the infrastructure code and a configuration management tool is used for implementation and for rollback capability anytime an approved configuration change is made. Baseline configurations are reviewed and updated annually or when required due to reviews and system changes, and anytime integral system components are added.
		CC7.5.1	A patch management process exists to confirm that operating system level vulnerabilities are remediated in a timely manner. Chief Technology Officer (CTO) / Management has set up automatic patch management and performs monthly patch management reviews. Workstations are configured to receive automatic updates. In addition, workstations are scanned to test patch compliance on a daily basis.
		CC8.1.1	A formal change management policy is established that governs the development, implementation, changes, and maintenance of application(s) and supporting infrastructure. System development lifecycle documentation also addresses regular and emergency change processes. The change management process requires that: • Change requests are authorized • Changes are tested prior to migration to production • Changes are reviewed and approved prior to promotion to the production environment. All changes are documented in the internal tool and tracked from initiation through deployment and validation. Emergency changes follow an accelerated timeline and prior to initiating an emergency change, appropriate approval is obtained and documented.

CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	CC8.1.3	Source code changes are logged, time-stamped, and attributed to their author in a source code management tool. Access to the source code tool is restricted to authorized users using multi-factor authentication.
		CC8.1.4	Changes to application and system infrastructure are developed and tested in a separate development or test environment before implementation.
CC9.0 Common Criteria Related to Risk Mitigation			
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	CC7.4.1	A BCDR (Business Continuity and Disaster Recovery) policy, Business Continuity plan and Disaster Recovery plan is documented and reviewed annually. The plan includes the alternative working plans, the roles and responsibilities of key personnel in executing the continuity strategy. There are communication plans in the policy in order to notify of any disaster. The plan also includes the incident response plan. The company conducts testing of the BCDR (Business Continuity and Disaster Recovery) plans, per the defined testing schedule for different loss scenarios. Each loss scenario is tested at least annually. Test results are reviewed and consequently contingency plans are updated. Issues identified during testing are resolved and plans are updated accordingly.

CC9.2	The entity assesses and manages risks associated with vendors and business partners.	CC9.2.1	The company has a vendor management policy in place. The policy requires management to maintain critical third-party vendor inventory, baseline of vendor security requirements and periodic evaluation of the performance of critical third-party vendors. On an annual basis, management performs reviews of SOC reports from service providers/vendors to review the appropriateness of scope, impact of identified exceptions and applicable complementary user entity controls. For critical vendors that do not have a SOC report and have access to data or impact the security of the system, a quarterly vendor risk assessment is performed. During this assessment performance, service delivery and compliance with security commitments is also assessed. Corrective actions are taken based on the results of the assessments.
		CC9.2.2	A vendor management process has been implemented whereby management performs risk assessments of potential new vendors prior to their onboarding. The vendors' responsibilities, which includes security commitments and responsibilities are documented and agreed with the vendors during the onboarding process.
		CC9.2.3	Vendor management process has been implemented that includes security procedures to be followed in case of vendor terminations. The Company has clauses in its agreements with vendors and service providers to terminate relationships when necessary. Vendor and service provider access is removed upon termination through a termination checklist and access is revoked of the termination process.

Tests of Controls and Results of Tests

Control	Description of Controls	Tests of Controls	Test Results
CC1.1.1	Employees are required to acknowledge the Code of Conduct at least annually, which is enforced to ensure ethical behavior and compliance with organizational policies. Moreover, a Sanctions Policy mentions that non-compliance with the Code of Conduct can lead to termination of employees.	Inquired of the control owner to ascertain the appropriateness of the control performed. Selected a sample of active employees. For the selected samples inspected evidence to observe that employees are required to acknowledge the Code of Conduct at least annually, which is enforced to ensure ethical behavior and compliance with organizational policies. Further inspected evidence to observe that the Sanctions Policy mentions that non-compliance with the Code of Conduct can lead to termination of employees.	No exceptions noted.
CC1.1.2	Contractors are required to acknowledge and sign a confidentiality agreement to ensure the protection of sensitive information.	Inquired of the control owner to ascertain the appropriateness of the control performed. Selected a sample of new contractors. For the selected samples, inspected evidence to observe that contractors are required to acknowledge and sign a confidentiality agreement to ensure the protection of sensitive information.	No exceptions noted.

CC1.1.3	Contractors are required to acknowledge the Code of Conduct at least annually, which is enforced to ensure ethical behavior and compliance with organizational policies. Moreover, a Sanctions Policy mentions that non-compliance with the Code of Conduct can lead to termination of contractors.	Inquired of the control owner to confirm the requirements for contractors regarding the acknowledgment of the Code of Conduct. Selected a sample of active contractors. For the selected samples, inspected evidence to observe that contractors are required to acknowledge the Code of Conduct at least annually, which is enforced to ensure ethical behavior and compliance with organizational policies. Further, inspected evidence to observe that the Sanctions Policy mentions that non-compliance with the Code of Conduct can lead to termination of contractors.	No exceptions noted.
CC1.1.4	Employees are required to acknowledge and sign a confidentiality agreement to ensure the protection of sensitive information.	Inquired of the control owner to ascertain the appropriateness of the control performed. Selected a sample of new employees. For the selected samples, inspected evidence to observe that employees are required to acknowledge and sign a confidentiality agreement to ensure the protection of sensitive information.	No exceptions noted.

CC1.2.2	Board meetings are conducted regularly to review and oversee the entity's strategic direction, risk management, and compliance with regulatory requirements.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that the Board meetings are conducted regularly to review and oversee the entity's strategic direction, risk management, and compliance with regulatory requirements.	No exceptions noted.
CC1.4.1	The board of directors possesses the necessary expertise to oversee and guide the entity's information security and compliance programs effectively.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that the board of directors possesses the necessary expertise to oversee and guide the entity's information security and compliance programs effectively.	No exceptions noted.
CC1.4.2	The board of directors is regularly briefed on the status of the entity's information security program, including risk management, compliance, and incident response activities.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that the board of directors is regularly briefed on the status of the entity's information security program, including risk management, compliance, and incident response activities.	No exceptions noted.
CC1.3.1	The organization has established and documented its structure, including roles, responsibilities, and reporting lines, to support the achievement of its objectives and compliance with relevant requirements.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that the organization has established and documented its structure, including roles, responsibilities, and reporting lines, to support the achievement of its objectives and compliance with relevant requirements.	No exceptions noted.

CC1.3.2	Roles and responsibilities for the security of systems and data are clearly defined, documented, and communicated to relevant personnel, which includes all employees with security-related roles.	Inquired of the control owner to ascertain the appropriateness of the control performed. Selected a sample of employees. For the selected samples, inspected evidence to observe that roles and responsibilities for the security of systems and data are clearly defined, documented, and communicated to relevant personnel, which includes all employees with security-related roles.	No exceptions noted.
CC1.3.3	Management roles and responsibilities are established, documented, and communicated to ensure accountability and proper execution of tasks related to the entity's information, infrastructure, and software.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that management roles and responsibilities are established, documented, and communicated to ensure accountability and proper execution of tasks related to the entity's information, infrastructure, and software.	No exceptions noted.
CC1.1.5	Performance evaluations are conducted, documented, and reviewed regularly to ensure that personnel meet the established criteria and contribute effectively to the entity's objectives. These evaluations include discussions on training needs and the development of a performance development plan to support continuous improvement and professional growth.	Inquired of the control owner to ascertain the appropriateness of the control performed. Selected sample of active employees. For the selected samples, inspected evidence to observe that performance evaluations are conducted, documented, and reviewed regularly to ensure that personnel meet the established criteria and contribute effectively to the entity's objectives. Further observed that these evaluations included discussions on training needs and the development of a performance development plan to support continuous improvement and professional growth.	No exceptions noted.

CC1.4.3	Background checks are conducted on employees and contractors prior to employment to ensure the integrity and reliability of individuals accessing sensitive information and systems.	Inquired of the control owner to ascertain the appropriateness of the control performed. Selected a sample of new employees. For the selected samples, inspected the evidence to observe that background checks are conducted on employees and contractors prior to employment to ensure the integrity and reliability of individuals accessing sensitive information and systems.	No exceptions noted.
CC1.4.4	Management utilizes a pre-hire checklist to ensure that the hiring manager has assessed the qualifications of candidates during the hiring process to confirm that they can perform the necessary job requirements.	Inquired of the control owner to ascertain the appropriateness of the control performed. Selected a sample of new employees. For the selected samples, inspected the evidence to observe that management utilizes a pre-hire checklist to ensure that hiring manager has assessed the qualification of candidates during the hiring process to confirm that they can perform the necessary job requirements.	No exceptions noted.
CC2.1.1	An intrusion detection system is utilized to monitor and detect unauthorized access or anomalies within the network, ensuring timely identification and response to potential security incidents.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that an intrusion detection system is utilized to monitor and detect unauthorized access or anomalies within the network, ensuring timely identification and response to potential security incidents.	No exceptions noted.

CC2.1.2	The Board of Directors has empowered the Risk and Governance Executive Committee ("RGEC") to provide oversight of management's system and supplement its expertise related to security and governance. The RGEC Charter has been established to define the responsibilities of the RGEC members. The Charter is reviewed and updated and is approved on an annual basis and made available to relevant personnel. The RGEC Committee meets semiannually review and evaluate the key internal control measures such and approval of the organization's policies, performance of internal controls assessment, review the organization wide risk assessment based on the identified needs and corrective action, identification of any opportunities for improvements, review resources and budget needs related to information security and compliance frameworks, review assessments conducted by internal and external parties, approve new controls ensuring appropriate mix of both manual and automated controls and preventive and detective controls and consider various ways that fraud and misconduct can occur within the organization, measures to mitigate the risk of fraud.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that the board has empowered the Risk and Governance Executive Committee ("RGEC") to provide oversight of management's system and supplement its expertise related to security and governance. Inspected evidence to observe that the charter includes responsibilities of the RGEC members. Further observed that the charter is reviewed and updated and is approved on an annual basis and made available to relevant personnel. Selected meeting minutes of sample RGEC meeting to observe that the Risk and Governance Committee met quarterly to review and evaluate key internal control measures.	No exceptions noted.

CC2.1.3	A data classification policy is established, documented, and implemented to categorize data based on sensitivity and criticality, ensuring appropriate handling and protection measures are applied.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that the data classification policy is established, documented, and implemented to categorize data based on sensitivity and criticality, ensuring appropriate handling and protection measures are applied.	No exceptions noted.
CC2.1.4	The organization maintains an inventory of production information assets including details on asset ownership and location. The asset inventory listing is reviewed and updated by management on an as-needed basis.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that the organization maintains an inventory of production information assets including details on asset ownership and location. Inspected evidence to observe that the asset inventory listing was reviewed and updated by management on an as-needed basis.	No exceptions noted.
CC2.2.1	Security policies are established, documented, and periodically reviewed to ensure they remain effective and aligned with organizational objectives and regulatory requirements. These policies are made available to and acknowledged by employees and contractors.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that security policies are established, documented, and periodically reviewed to ensure they remain effective and aligned with organizational objectives and regulatory requirements. Selected sample of employees. For the selected samples, inspected evidence to observe that these policies are made available to and acknowledged by employees and contractors.	No exceptions noted.

CC2.2.2	The company has established communication channels that allow employees to securely and anonymously report issues related to fraud, harassment and other issues impacting the organization's ethical and integrity requirements.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that the company has established communication channels that allow employees to securely and anonymously report issues related to fraud, harassment and other issues impacting the organization's ethical and integrity requirements.	No exceptions noted.
CC2.2.3	Significant changes to people, roles and responsibilities for key personnel are internally communicated to all personnel via an internal communication tool.	Inquired of the control owner to ascertain the appropriateness of the control performed. Selected a sample of changes to key personnel, roles, and responsibilities. For the selected samples, inspected evidence to observe that significant changes to people, roles and responsibilities for key personnel are internally communicated to all personnel via an internal communication tool.	No exceptions noted. The operating effectiveness of the control related to significant changes to people, roles and responsibilities could not be tested because there were no significant changes made during the engagement period.
CC2.2.4	Security awareness training is implemented, documented, and conducted regularly to ensure that all personnel are aware of security policies, procedures, and their responsibilities in protecting the entity's information and systems.	Inquired of the control owner to ascertain the appropriateness of the control performed. Selected a sample of active employees. For the selected samples, inspected evidence to observe that security awareness training is implemented, documented, and conducted regularly to ensure that all personnel are aware of security policies, procedures, and their responsibilities in protecting the entity's information and systems.	No exceptions noted.

CC2.3.1	Company commitments to security are clearly communicated to external stakeholders through established channels, ensuring transparency and alignment with trust services criteria.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that company commitments to security are clearly communicated to external stakeholders through established channels, ensuring transparency and alignment with trust services criteria.	No exceptions noted.
CC2.3.2	External support resources are identified, documented, and made available to ensure timely and effective resolution of issues and continuity of operations.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that external support resources are identified, documented, and made available to ensure timely and effective resolution of issues and continuity of operations.	No exceptions noted.
CC2.3.3	A support system is available to assist users with issues related to the entity's information, infrastructure, and software, ensuring timely resolution and maintaining system integrity.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that a support system is available to assist users with issues related to the entity's information, infrastructure, and software. Further selected sample of incidents. For the selected samples, inspected evidence to observe timely resolution for maintenance of system integrity.	No exceptions noted.

CC2.3.4	Risk assessment objectives are established, documented, and communicated to identify, analyze, and manage risks associated with the achievement of the entity's objectives. Risks are ranked according to priority levels and cover areas like security, fraud, legal, regulatory, economic, physical and business environment, competition, customer, vendor relationship, technology changes, and information security.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that risk assessment objectives are established, documented, and communicated to identify, analyze, and manage risks associated with the achievement of the entity's objectives. Further, observed that risks are ranked according to priority levels and cover areas like security, fraud, legal, regulatory, economic, physical and business environment, competition, customer, vendor relationship, technology changes, and information security.	No exceptions noted.
CC2.3.5	A risk management program is established, documented, and maintained to identify, assess, and respond to risks that could impact the achievement of the entity's objectives. Risks are ranked according to priority levels and cover areas like security, fraud, legal, regulatory, economic, physical and business environment, competition, customer, vendor relationship, technology changes, and information security.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that a risk management program is established, documented, and maintained to identify, assess, and respond to risks that could impact the achievement of the entity's objectives. Further, observed that risks are ranked according to priority levels and cover areas like security, fraud, legal, regulatory, economic, physical and business environment, competition, customer, vendor relationship, technology changes, and information security.	No exceptions noted.

CC2.3.6	Risk assessments are conducted periodically to identify potential threats and vulnerabilities to the entity's information systems and data, ensuring appropriate risk mitigation strategies are implemented. Risks are ranked according to priority levels and cover areas like security, fraud, legal, regulatory, economic, physical and business environment, competition, customer, vendor relationship, technology changes, and information security.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that risk assessments are conducted periodically to identify potential threats and vulnerabilities to the entity's information systems and data, ensuring appropriate risk mitigation strategies are implemented. Further, observed that risks are ranked according to priority levels and cover areas like security, fraud, legal, regulatory, economic, physical and business environment, competition, customer, vendor relationship, technology changes, and information security.	No exceptions noted.
CC2.3.7	A formal network diagram outlining boundary protection mechanisms (e.g. firewalls, IDS, etc.) is maintained for all network connections and reviewed annually by IT management.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that a formal network diagram outlining boundary protection mechanisms (e.g. firewalls, IDS, etc.) is maintained for all network connections and reviewed annually by IT management.	No exceptions noted.

CC3.1.1	The Organization has implemented an IT Leadership Committee which is governed by the IT Leadership Committee Charter that provides support to the Risk and Governance Executive Committee (RGEC). The IT Leadership Committee Charter includes roles and responsibilities relevant to security and is reviewed annually. The IT leadership team meets weekly to review and evaluate activities and processes that are key in meeting an organization's security commitment. The organization's executive team meets on a weekly basis to discuss operations, issues relating to internal controls and delivery on key performance metrics.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that the company has implemented an IT Leadership Committee which is governed by IT Leadership Committee Charter that provides support to the Risk and Governance Executive Committee (RGEC). Inspected evidence to observe that the charter includes roles and responsibilities of the ITLC members relates to security. Further observed that the charter is reviewed on an annual basis. Selected meeting minutes of sample ITLC meetings to observe that the Risk and Governance Committee met weekly to review and evaluate activities and processes that are key in meeting an organization's security commitment. Further, observed that the company's executive team meets on a weekly basis to discuss operations, issues relating to internal controls and delivery on key performance metrics.	No exceptions noted.
CC3.2.1	Cybersecurity insurance is maintained to provide financial protection and support in the event of a cyber incident or data breach.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that Cybersecurity insurance is maintained to provide financial protection and support in the event of a cyber incident or data breach.	No exceptions noted. The operating effectiveness of the control related to cybersecurity incidents could not be tested because there no cyber incidents reported during the engagement period.

CC5.2.1	Infrastructure performance is continuously monitored to ensure the availability, efficiency, and reliability of systems and services. Additionally, the monitoring tool generates alerts when specific predefined thresholds are met. An incident management process is invoked for confirmed events and anomalies, with logs and alerts tracked until resolved within the change-management/ticketing application.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that Infrastructure performance is continuously monitored to ensure the availability, efficiency, and reliability of systems and services. Further observed that the monitoring tool generates alerts when specific predefined thresholds are met. Selected sample alerts. For selected sample inspected evidence to observe that an incident management process was invoked for confirmed events and anomalies, with logs and alerts tracked until resolved within the change-management/ticketing application.	No exceptions noted.
CC5.2.2	Access to the production operating system is restricted to authorized personnel to ensure system integrity and security. Generic accounts with administrative privileges are carefully managed and monitored to ensure access to these accounts is limited.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that access to the production operating system is restricted to authorized personnel to ensure system integrity and security. Further observed that generic accounts with administrative privileges are carefully managed and monitored to ensure access to these accounts is limited.	No exceptions noted.

CC5.2.4	Access to the production network is restricted to authorized personnel, ensuring that only individuals with a legitimate business need can access sensitive systems and data.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that access to the production network is restricted to authorized personnel, ensuring that only individuals with a legitimate business need can access sensitive systems and data.	No exceptions noted.
CC5.2.5	Access to production deployment is restricted to authorized personnel to ensure the security and integrity of the production environment. Additionally, source code changes are logged, time-stamped, and attributed to their author in a source code management tool.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that access to production deployment was restricted to authorized personnel to ensure the security and integrity of the production environment. Selected sample changes. For the selected samples, inspected evidence to observe that source code changes were logged, time-stamped, and attributed to their author in a source code management tool.	No exceptions noted.
CC5.2.6	Access to production applications is restricted to authorized personnel based on their roles and responsibilities, ensuring that only individuals with a legitimate need can access sensitive systems and data.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that access to production applications is restricted to authorized personnel based on their roles and responsibilities, ensuring that only individuals with a legitimate need can access sensitive systems and data.	No exceptions noted.

CC6.1.2	Access control procedures are established, documented, and enforced to ensure that only authorized individuals have access to systems and data.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that access control procedures are established, documented, and enforced properly. Further, selected sample of employees. For the selected samples, inspected evidence to observe that only authorized individuals have access to systems and data.	No exceptions noted.
CC6.1.3	Unique network system authentication mechanisms are enforced, documented, and managed to ensure that only authorized individuals and systems can access the network infrastructure.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that unique network system authentication mechanisms are enforced, documented, and managed to ensure that only authorized individuals and systems can access the network infrastructure.	No exceptions noted.
CC6.1.4	Unique account authentication is enforced to ensure that each user accessing the system is individually identified and authenticated, preventing unauthorized access and ensuring accountability.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that unique account authentication is enforced to ensure that each user accessing the system is individually identified and authenticated, preventing unauthorized access and ensuring accountability.	No exceptions noted.
CC6.1.5	Policy and procedures are established, documented, and enforced to ensure the strength and confidentiality of passwords used to access systems and data.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that policy and procedures are established, documented, and enforced to ensure the strength and confidentiality of passwords used to access systems and data.	No exceptions noted.

CC6.1.6	Unique authentication mechanisms are enforced for accessing the production database to ensure that only authorized individuals can gain access.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that unique authentication mechanisms are enforced for accessing the production database to ensure that only authorized individuals can gain access.	No exceptions noted.
CC6.1.7	Network segmentation is implemented to separate systems and data based on sensitivity and criticality, thereby reducing the risk of unauthorized access and potential breaches.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that Network segmentation is implemented to separate systems and data based on sensitivity and criticality, thereby reducing the risk of unauthorized access and potential breaches.	No exceptions noted.
CC6.1.8	Access to the entity's information systems and data is promptly revoked upon termination of an individual's employment or contractual relationship.	Inquired of the control owner to ascertain the appropriateness of the control performed. Selected sample of terminated employees. For the selected samples, inspected evidence to observe that access to the entity's information systems and data is promptly revoked upon termination of an individual's employment or contractual relationship.	No exceptions noted.
CC6.1.9	Access to encryption keys is restricted to authorized personnel only, ensuring that keys are protected from unauthorized access and misuse.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that access to encryption keys is restricted to authorized personnel only, ensuring that keys are protected from unauthorized access and misuse.	No exceptions noted.
CC6.1.10	Data encryption is implemented to protect sensitive information both at rest and in transit, ensuring confidentiality and integrity are maintained.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that Data encryption is implemented to protect sensitive information both at rest and in transit, ensuring confidentiality and integrity were maintained.	No exceptions noted.

CC6.2.1	Access requests are required, documented, and approved prior to granting access to systems and data to ensure that only authorized individuals can access sensitive information.	Inquired of the control owner to ascertain the appropriateness of the control performed. Selected sample of access request received during the period. For the selected sample, inspected the evidence to observe access requests are required, documented, and approved prior to granting access to systems and data to ensure that only authorized individuals can access sensitive information.	No exceptions noted.
CC6.2.2	Access reviews are conducted periodically to ensure that only authorized individuals have access to systems and data, and any discrepancies are promptly addressed.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that access reviews are conducted periodically to ensure that only authorized individuals have access to systems and data, and any discrepancies are promptly addressed.	No exceptions noted.

CC6.5.1	Data retention procedures are established, documented, and implemented to ensure that data is retained in accordance with regulatory, legal, and business requirements.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that Data retention procedures were established, documented, and implemented to ensure that data is retained in accordance with regulatory, legal, and business requirements.	No exceptions noted.
CC6.5.2	Customer data is securely deleted from all systems and storage locations upon termination of the customer relationship.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that customer data is securely deleted from all systems and storage locations upon termination of the customer relationship.	No exceptions noted. The operating effectiveness of the control related to customer data deletion upon termination could not be tested because there were no customer terminations during the engagement period.
CC6.6.1	Firewall access is restricted to authorized personnel to ensure that only approved individuals can modify firewall settings and rules.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that firewall access is restricted to authorized personnel to ensure that only approved individuals can modify firewall settings and rules.	No exceptions noted.
CC6.6.2	Network firewalls are implemented, configured, and managed to control and monitor incoming and outgoing network traffic based on predetermined security rules.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that network firewalls are implemented, configured, and managed to control and monitor incoming and outgoing network traffic based on predetermined security rules.	No exceptions noted.

CC6.6.3	Network firewall configurations and rules are regularly reviewed and updated to ensure they effectively protect the entity's information and systems from unauthorized access and other security threats.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that network firewall configurations and rules are regularly reviewed and updated to ensure they effectively protect the entity's information and systems from unauthorized access and other security threats.	No exceptions noted.
CC6.8.1	Anti-malware technology is implemented, maintained, and regularly updated to protect the entity's information systems, including production servers and workstations, from malicious software.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that anti-malware technology has been implemented, maintained, and regularly updated to protect the entity's information systems, including production servers, from malicious software. Selected sample workstations. For the selected sample inspected evidence to observe that anti-virus technology has been implemented, maintained, and regularly updated to protect the entity's information systems from malicious software.	No exceptions noted.
CC7.1.1	Network and system hardening standards are established, documented, and maintained to protect against unauthorized access and vulnerabilities.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that network and system hardening standards have been established, documented, and maintained to protect against unauthorized access and vulnerabilities.	No exceptions noted.

CC7.1.2	The service infrastructure is maintained to ensure it remains secure, reliable, and available to support the entity's operations and meet its commitments. This includes regular vulnerability scanning, penetration testing, and patch management to identify and address security weaknesses. Monitoring systems with defined thresholds are in place to ensure the availability and reliability of the infrastructure.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that a patch management process exists to confirm that operating system level vulnerabilities are remediated in a timely manner. Inspected evidence to observe that Chief Technology Officer (CTO) / Management, has set up automatic patch management. Selected ITLC meeting minutes for sample months. For the selected samples inspected evidence to observe that CTO / Management during ITLC meeting performs patch management reviews Selected sample of workstations. For the selected samples inspected evidence to observe that the workstations were configured to receive automatic updates. Further observed that the workstations were scanned to test patch compliance on a daily basis	No exceptions noted.
CC7.1.3	Vulnerability and system monitoring procedures are established, documented, and implemented to detect, assess, and remediate potential threats to the entity's information systems.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that vulnerability and system monitoring procedures have been established, documented, and implemented to detect, assess, and remediate potential threats to the entity's information systems.	No exceptions noted.
CC7.1.4	Vulnerability scans are conducted regularly to identify security weaknesses, and remediation efforts are promptly implemented to address identified vulnerabilities.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that vulnerability scans are conducted regularly to identify security weaknesses, and remediation efforts are promptly implemented to address identified vulnerabilities.	No exceptions noted.

CC7.2.1	Log management processes are established, documented, and maintained to ensure the proper collection, retention, and analysis of logs for monitoring and auditing purposes. Logging is enabled to monitor activities such activities, log-on attempts, data deletions at the application and infrastructure level, changes to functions, security configurations, permissions, and roles. Automated alerts are configured to notify IT management of high and critical risk events. Access to change the log configuration and access to modify logs is restricted.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that log management processes have been established, documented, and maintained to ensure the proper collection, retention, and analysis of logs for monitoring and auditing purposes. Inspected onscreen configuration to observe that logging is enabled to monitor activities such activities, logon attempts, changes to functions, security configurations, permissions, and roles. Inspected onscreen configuration to observe that automated alerts are configured to notify IT management of high and critical risk events. Inspected evidence to observe that access to change the log configuration and access to modify logs are restricted.	No exceptions noted.

CC7.3.1	Incident response policies are established, documented, and communicated to ensure timely and effective response to security incidents. Security incidents are documented and include root causes and lessons learned from the incident.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that Incident response policies are established, documented, and communicated to ensure timely and effective response to security incidents. Further, observed that security incidents are documented and include root causes and lessons learned from the incident.	No exceptions noted. The operating effectiveness of the control related to security incidents could not be tested because there no security incidents reported during the engagement period.
CC7.3.2	Incident management procedures are established, documented, and followed to identify, respond to, and remediate security incidents in a timely manner. These procedures include the evaluation of root causes, and the incorporation of lessons learned.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that Incident management procedures are established, documented, and followed to identify, respond to, and remediate security incidents security incidents in a timely manner. Inspected evidence to observe that the company's Incident Management Procedures include the evaluation of root causes, and the incorporation of lessons learned.	No exceptions noted.

CC7.4.1	Continuity and Disaster Recovery plans are established, documented, and tested to ensure the entity can recover and resume operations in the event of a disruption. These plans include alternative working plans, the roles and responsibilities of key personnel in executing the continuity strategy, and communication plans to notify relevant stakeholders of any disaster.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that Continuity and Disaster Recovery plans are established, documented, and tested to ensure the entity can recover and resume operations in the event of a disruption. Further observed that these plans include alternative working plans, the roles and responsibilities of key personnel in executing the continuity strategy, and communication plans to notify relevant stakeholders of any disaster.	No exceptions noted.
CC7.4.2	Backup processes are established, documented, and managed to ensure the availability and integrity of data in the event of a system failure or data loss. Backups are taken daily, multi-availability zones are configured, and alerts are in place to notify operating personnel in case of a backup failure and its remediation.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that backup processes are established, documented, and managed to ensure the availability and integrity of data in the event of a system failure or data loss. Inspected onscreen evidence to observe that Backups are taken daily, multi-availability zones are configured, and alerts are in place to notify operating personnel in case of a backup failure and its remediation.	No exceptions noted.

CC7.5.1	A patch management process exists to confirm that operating system level vulnerabilities are remediated in a timely manner. Chief Technology Officer (CTO) / Management has set up automatic patch management and performs monthly patch management reviews. Workstations are configured to receive automatic updates. In addition, workstations are scanned to test patch compliance on a daily basis.	Inquired of the control owner to ascertain the appropriateness of the control performed. Selected sample of operating system level vulnerabilities. For the selected samples, inspected evidence to observe that a patch management process exists to confirm that operating system level vulnerabilities are remediated in a timely manner. Further, inspected evidence to observe that Chief Technology Officer (CTO) / Management has set up automatic patch management and performs monthly patch management reviews. Selected sample of workstations. For the selected samples inspected evidence to observe that workstations are configured to receive automatic updates. Further observed that workstations are scanned to test patch compliance on a daily basis.	No exceptions noted.
CC8.1.1	A development lifecycle is established, documented, and managed to ensure that system changes are properly controlled, tested, and approved before implementation.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that a development lifecycle is established, documented, and managed to ensure that system changes are properly controlled, tested, and approved before implementation.	No exceptions noted.

CC8.1.2	Change management procedures are established, documented, and enforced to ensure that all changes to systems and applications are properly reviewed, tested, and approved before implementation. The company ensures that environments are segregated, system changes are communicated with external and internal stakeholders, an approval process is followed prior to merging to the master branch, and procedures are in place to implement emergency changes.	Inquired of the control owner to ascertain the appropriateness of the control performed. Inspected evidence to observe that change management procedures are established, documented, and enforced properly. Selected sample of changes to system. For the selected sample, inspected evidence to observe that all changes to systems and applications are properly reviewed, tested, and approved before implementation. Further, observed that the company ensures that environments are segregated, system changes are communicated with external and internal stakeholders, and an approval process is followed prior to merging to the master branch. Further, inspected evidence to observe that procedures are in place to implement emergency changes.	No exceptions noted.
CC8.1.3	Developers are not permitted to make changes to application code in the production environment without obtaining additional approval, in the organization's change management policy.	Inquired of the control owner to ascertain the appropriateness of the control performed. Selected sample changes. For the selected samples inspected evidence to observe that developers do not make changes to application code in the production environment without additional approval.	No exceptions noted.

CC8.1.5	System changes are documented, reviewed, and communicated to relevant stakeholders to ensure awareness and understanding of modifications to the system.	Inquired of the control owner to ascertain the appropriateness of the control performed. Selected sample of system changes during the period. For the selected samples, inspected evidence to observe that system changes are documented, reviewed, and communicated to relevant stakeholders to ensure awareness and understanding of modifications to the system.	No exceptions noted.

SECTION 5

Other Information Provided by Upwage

Other Information Provided by Upwage

The information provided in this section is provided for informational purposes only by Upwage. The Independent Auditor has performed no audit procedures in this section.

Disaster and Recovery Services

The AICPA has published guidance indicating that business continuity planning, which includes disaster recovery, is a concept that addresses how an organization mitigates future risks to actual controls that provide user auditors with a level of comfort surrounding the processing of transactions. As a result, a service organization should not include in its description of controls any specific control procedures that address disaster recovery planning. Therefore, Upwage disaster recovery plan descriptions of control procedures are presented in this section.

In addition to the physical controls, Upwage has implemented logical controls to safeguard against interruption of service. Upwage has developed a number of procedures that provide for the continuity of operations in the event of an availability zone failure by spinning up multiple servers across all availability zones in CLOUDFLARE, VERCEL, and AWS.

The disaster recovery plan defines the roles and responsibilities and identifies the critical IT application programs, operating systems, personnel, data files, and time frames needed to ensure high availability and system reliability based on a business impact analysis.