Rezolve.ai

Independent Service Auditor's Report on Management's Description of Service Organization's System Relevant to Security, Confidentiality, Availability and the Suitability of the Design and Operating Effectiveness of the Controls

For the period, January 01, 2025 to December 31, 2025

(SSAE 21 - SOC 2 Type 2 Report)

Prepared by: Subhajit Guha, CPA

Table of Contents

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

Independent Service Auditor's Report

To: Management of Rezolve.Ai (Rezolve.ai)

Scope

We have examined the attached Rezolve.ai's description of the system titled "**Software As A Service" (**description) throughout the period January 01, 2025 to December 31, 2025, 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 January 01, 2025 to December 31, 2025, to provide reasonable assurance that Rezolve.ai's service commitments and system requirements would be achieved based on the trust service criteria for security, availability and confidentiality (applicable trust services criteria) set forth in TSP Section 100, 2017 Trust Services Principles and Criteria for Security *Availability, Processing Integrity, Confidentiality and Privacy* (AICPA trust service criteria). Rezolve.ai has determined that Processing Integrity and Privacy Trust Services Principles are not applicable to the services provided to its client and are not included in the description.

The information included in Section 5, "Other Information Provided by Rezolve.ai" is presented by the management of Rezolve.ai to provide additional information and is not a part of Rezolve.ai's description of its system made available to user entities during the period January 01, 2025 to December 31, 2025. Information in Section 5 has not been subjected to the procedures applied in the examination of the description of the system and of the suitability of the design and operating effectiveness of controls to achieve the Service Organization's service commitments and system requirements based on the applicable trust services criteria, and accordingly, we express no opinion on the same.

The description indicates that Rezolve.ai's controls can provide reasonable assurance that certain service commitments and system requirements relating to applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of Rezolve.ai's 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, Rezolve.ai uses subservice organizations for providing customer services. The description in Section 3 includes only the controls of Rezolve.ai 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 Rezolve.ai'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

Rezolve.ai is responsible for its service commitments and system requirements and designing, implementing, and operating effective controls within the system to provide reasonable assurance that the service commitments and system requirements were achieved.

Rezolve.ai has provided the accompanying assertion titled, Management of Rezolve.ai's Assertion (Assertion) about the presentation of the Description based on the Description Criteria and suitability of the design and operating effectiveness of the controls described therein to provide reasonable assurance that the service commitments and system requirement would be achieved based on the applicable trust services criteria if operating effectively. Rezolve.ai is responsible for (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the

Description and Assertion; (3) providing the services 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 that are suitably designed and operating effectively 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 set forth in Rezolve.ai's assertion and on the suitability of the design and 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 and (2) the controls are suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements relating to applicable trust services criteria stated in the description would be achieved throughout the period January 01, 2025 to December 31, 2025.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design and 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 and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the applicable trust services criteria were met. Our examination also included 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.

Service Auditor's Independence and Ethical Requirements

We have complied with the independence requirements and other ethical responsibilities in accordance with relevant ethical requirements related to this engagement.

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 individual 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 and operating effectiveness 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 Rezolve.ai's assertion and the applicable trust services criteria:

a. the description fairly presents the system that was designed and implemented throughout the period January 01, 2025 to December 31, 2025.
b. the controls stated in the description were suitably designed to provide reasonable assurance that Rezolve.ai's service commitments and system requirements and the applicable trust services criteria would be achieved if the controls operated effectively throughout the period January 01, 2025 to December 31, 2025, and the subservice organization and user entities applied the controls contemplated in the design of Rezolve.ai's controls throughout the period January 01, 2025 to December 31, 2025.

c. The controls operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period January 01, 2025 to December 31, 2025, and user entities and subservice organizations applied the controls contemplated in the design of Rezolve.ai's controls, and those controls operated effectively throughout the period January 01, 2025 to December 31, 2025.

Description of Test 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 "Independent Service Auditors' Description of Test of Controls and Results"

Restricted Use

This report, including the description of controls and test results thereof in Section 4 of this report, is intended solely for the information and use of Rezolve.ai; user entities of Rezolve.ai's systems during some or all the period January 01, 2025 to December 31, 2025; 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.

Subhajit Guha, CPA
(Illinois License Number - 065.056711)
May 12, 2026

SECTION 2

MANAGEMENT OF REZOLVE.AI'S ASSERTION

Management of Rezolve.ai's Assertion

REZOLVE.ai

May 12, 2026

Assertion of the Management of Rezolve.ai

We have prepared the accompanying description of Rezolve.AI system titled "**Software As A Service**" throughout the period January 01, 2025 to December 31, 2025 (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* in AICPA, *Description Criteria* (description criteria).

Rezolve.AI uses a subservice organization to provide customer services. The description includes only the control objectives and related controls of Rezolve.AI and excludes the control objectives and related controls of the subservice organization(s). The description also indicates that certain control objectives specified in the description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The description does not extend to controls of the subservice organization.

The description is intended to provide report users with information about the system that may be useful when assessing the risks arising from interactions with Rezolve.AI 's system, particularly information about system controls that Rezolve.AI has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and/or confidentiality. (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA, *Trust Services Criteria*.

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

a) the description fairly presents the system that was designed and implemented throughout the period January 01, 2025 to December 31, 2025 in accordance with the description criteria:

b) the controls stated in the description were suitably designed throughout the period January 01, 2025 to December 31, 2025 to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period

c) the controls stated in the description operated effectively throughout the period January 01, 2025 to December 31, 2025 to provide reasonable assurance that Rezolve.AI's service commitments and system requirements were achieved based on the applicable trust services criteria.

Sincerely

Aanchal Saini

Rezolve.ai
Regd. Office: F-14,Nehru Colony,
D-1 Block, Dehradun-248001

Associate Manager- HR/Admin
Date- May 12, 2026

Registered Office - F-14, Nehru Colony, D-1 Block, Dehradun 248001, Uttarakhand

Doon Express Business Park,
1000 Building, suit#1304,
Dehradun, Uttarkhand - 248001

NSIC Tech Park,
Suit No - 213, 214, 1st Floor,
Ekkatuthangal, Chennai,
Tamil Nadu – 600032

IndiQube Orion,
24th Main Rd, Agara Village, 1st
Sector, HSR Layout, Bengaluru,
Karnataka - 560102

SECTION 3

DESCRIPTION OF REZOLVE.AI SOFTWARE AS A SERVICE

THROUGHOUT THE PERIOD

JANUARY 01, 2025 TO DECEMBER 31, 2025

Description of Rezolve.ai - Software as a Service throughout the period January 01, 2025 to December 31, 2025

Background and Overview of Services

Actionable Science Labs Pvt. Ltd. (trading as Rezolve.ai) is a leading provider of Agentic AI solutions purpose-built for IT Support, HR Support, Employee Help Desk, and Shared Services Support. The company's platform moves beyond traditional chatbot functionality to deliver autonomous, end-to-end resolution of employee and support requests across the enterprise.

Product or Service Overview

Rezolve.ai offers an integrated suite of Agentic AI products:

1. **SideKick 3.0**
   Purpose-built SAAS platform for autonomous IT and HR support. Rezolve.ai's flagship offering enables fully autonomous resolution of IT Help Desk Level 1 requests - reducing costs and freeing human agents from routine, repetitive tasks. The platform handles complete processes end-to-end: from triage via natural language understanding, through execution via robotic process automation (RPA), to integration with leading IT Service Management (ITSM) platforms.
2. **Rezolve.ai Creator Studio**
   An intuitive workspace for designing, customizing, and managing workflows. Enables enterprise teams to build production-ready automations from plain English descriptions, without requiring code.
3. **ITSM**
   A help desk for end-to-end IT support management, including AI Ops capabilities for autonomous enterprise IT operations.

Significant Changes During the Audit Period

No other significant changes to the control environment occurred during the audit period.

Impact of Covid and Changes to our Controls

There is no material ongoing impact of COVID-19 on company operations. All office locations are fully operational, with employees working on-site across all development centers. Remote working policies established during the pandemic period remain documented and available as contingency controls.

Subservice Organizations

Rezolve.ai utilizes the following subservice providers for cloud-hosted infrastructure. These providers are not within the direct scope of this examination; however, Rezolve.ai's responsibilities for all applications and services operating on this infrastructure remain fully in scope. The responsibility matrix is defined in SLAs and agreements with each subservice organization.

1. **Microsoft Azure**
   Microsoft Azure serves as the primary cloud infrastructure provider for the Rezolve.ai platform. Azure is SOC 2 attested and has provided an Independent Service Auditor's Report (SOC 2) covering the period 30 September 2025 – 30 September 2026.

The Trust Services Criteria relevant to controls at the subservice organization level include Security, Confidentiality, and Availability. Specific control requirements include:

- Protection of the system against unauthorized access (physical and logical).
- System availability consistent with committed or agreed service levels.
- Documented and implemented policies and procedures related to security and availability.

Principal Service Commitments and System Requirements

Rezolve.ai designs its processes and procedures to meet service commitments made to user entities, applicable laws and regulations, and the company's own financial, operational, and compliance requirements. Security commitments are documented in customer agreements and in the description of service offerings provided online at www.rezolve.ai.

Operational requirements that support the achievement of these commitments are communicated through Rezolve.ai's system policies and procedures, system design documentation, and contracts with customers.

Information security policies define an organization-wide approach to the protection of systems and data. These policies govern service design and development, system operations, internal business systems and network management, and employee hiring and training. Standard operating procedures complement these policies by documenting how specific manual and automated processes are executed.

Components of the System

The System is comprised of the following components:

- Infrastructure including the physical 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,
- Procedures (automated and manual), and
- Data including transaction streams, files, databases, tables, and output used or processed by the system.

Boundaries of the System

The System boundaries include the applications, databases and infrastructure required to directly support the services provided to Rezolve.ai’s clients. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to Rezolve.ai’s customers are not included within the boundaries of its system. Only development centers mentioned are in scope of this SOC2 Type 2 assessment. The registered office is use for communication purposes. The specific products and services and locations included in the scope of the report are given below. All other products, services and locations are not included.

Products and Services in Scope
The scope of this report is limited to Technology and Development activities. **Products** • Rezolve.ai Platform **Services** • Application Development • Maintenance • Managed Services • SaaS services

Geographic Locations in Scope	
Registered Office Locations	**Address**
USA	11501, Dublin Blvd, STE 200, CA 94568
Dehradun	F-14, Nehru Colony, D-1 Block, Dehradun, Uttarakhand, India – 248001
Development Office Locations	**Address**
Dehradun	Doon Express Business Park - Suite # 1304, Building number 1000, 2nd floor, Dehradun, Uttarakhand - 248001
Chennai	NSIC STP - Suite# 214 B-24 Guindy Industrial Estate Ekkadathangal, Guindy Chennai, India- 600032
Bangalore	Indiqube Orion, 24th Main Road, 1st Sector, HSR Layout, Bengaluru, Karnataka India – 560102.
USA	Actionable Science Inc. Cincinnati, 209, E 4th St, Covington, KY 41011

The report excludes all processes and activities executed outside the above locations. No customer or personal data for client operations is stored on the Rezolve.ai office network by design. For service delivery, Rezolve.ai teams connect remotely to client networks, work within client applications, and are governed by client security policies. All Rezolve.ai products are hosted by third-party cloud service providers; no production systems are hosted on-premises.

Subsequent Events

Management is not aware of any relevant events that occurred after the period covered by management's description included in Section 3 of this report through the date of the service auditor's report that would have a significant effect on management's assertion.

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

Control Environment

Rezolve.ai's internal control environment reflects management's overall attitude, awareness, and commitment to effective controls across all policies, procedures, methods, and the 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 (ISMS) in accordance with the company's strategic objectives.

Management ensures that IT policies are communicated, understood, implemented, and maintained at all levels of the organization, and that these policies are reviewed regularly for continued suitability.

Integrity and Ethical Values

Rezolve.ai requires all directors, officers, and employees to observe high standards of business and personal ethics in the conduct of their duties. Honesty and integrity are core principles of the company. All employees are expected to fulfil their responsibilities in accordance with these principles and to comply with all applicable laws and regulations.

Rezolve.ai promotes open communication and has established an environment in which employees are protected from retaliation for good-faith reports of ethics violations. Executive management holds exclusive responsibility to investigate reported violations and take corrective action where warranted.

Board of Directors

Business activities are conducted under the direction of the Board of Directors, headed by its founder, Saurabh Kumar, as Chairman and CEO. Saurabh Kumar is responsible for global operations, with a primary focus on strategy and client engagement. Udaya Bhaskar Reddy is the CTO and Manish Sharma is the CRO of the Company.

Management's Philosophy and Operating Style

The Executive Management team assesses risk before entering into new business relationships or ventures. Given the size of the organization, the executive team maintains daily interaction with operating management, enabling timely identification and response to emerging issues.

Risk Management and Risk Assessment

The application of protection measures is based on the risk associated with information assets and the importance of those assets to the organization. As part of this process, security threats are identified and the risk from these threats is formally assessed.

Rezolve.ai has placed into operation 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 management identifying significant risks in their areas of responsibility and implementing appropriate measures to address those risks.

Pandemic /COVID 2019 Risks

Rezolve.ai has reassessed its risk with respect to Pandemic risk / COVID risks. Appropriate short term and long-term changes have been made to impacted controls. Some of the control changes that have taken place as a result of this include:

- Zoom and teams Channels are created to track the work of employees
- Remote working Policy is shared with employees
- Security Meetings are held to make sure team is up to date

Information Security Policies

Rezolve.ai maintains a comprehensive organization-wide Information Security Policy framework. Relevant policies are made available to all employees via shared OneDrive. Changes to these policies are reviewed by the CISO (currently the CTO) and approved by the CTO prior to implementation.

Monitoring

Monitoring is a critical aspect of internal control in evaluating whether controls operate as intended and remain appropriate as business conditions change.

Production systems and infrastructure are monitored through service level monitoring tools that track compliance with service level commitments and agreements. Reports are shared with applicable internal personnel and customers. Where commitments are not met, corrective actions are taken and communicated to relevant parties, including customers.

Information and Communication

Rezolve.ai maintains documented procedures covering significant functions and operations across all major workgroups. Policies and procedures are reviewed and updated based on operational changes, and formal approval by management is required prior to implementation. Departmental managers monitor adherence to policies and procedures as part of their daily activities.

Management holds regular departmental status meetings, including strategic planning meetings, to identify and address service issues, customer concerns, and project management matters. A designated service manager serves as the focal point for communication on each service line. Additionally, designated personnel interface directly with client organizations when processing or development issues arise.

Electronic communications — primarily via email and Microsoft Teams — are incorporated into operational processes to provide timely information to employees and to enable efficient management communication across all locations.

Components of the System

Infrastructure

The infrastructure comprises physical and hardware components of the System including facilities, equipment, and networks.

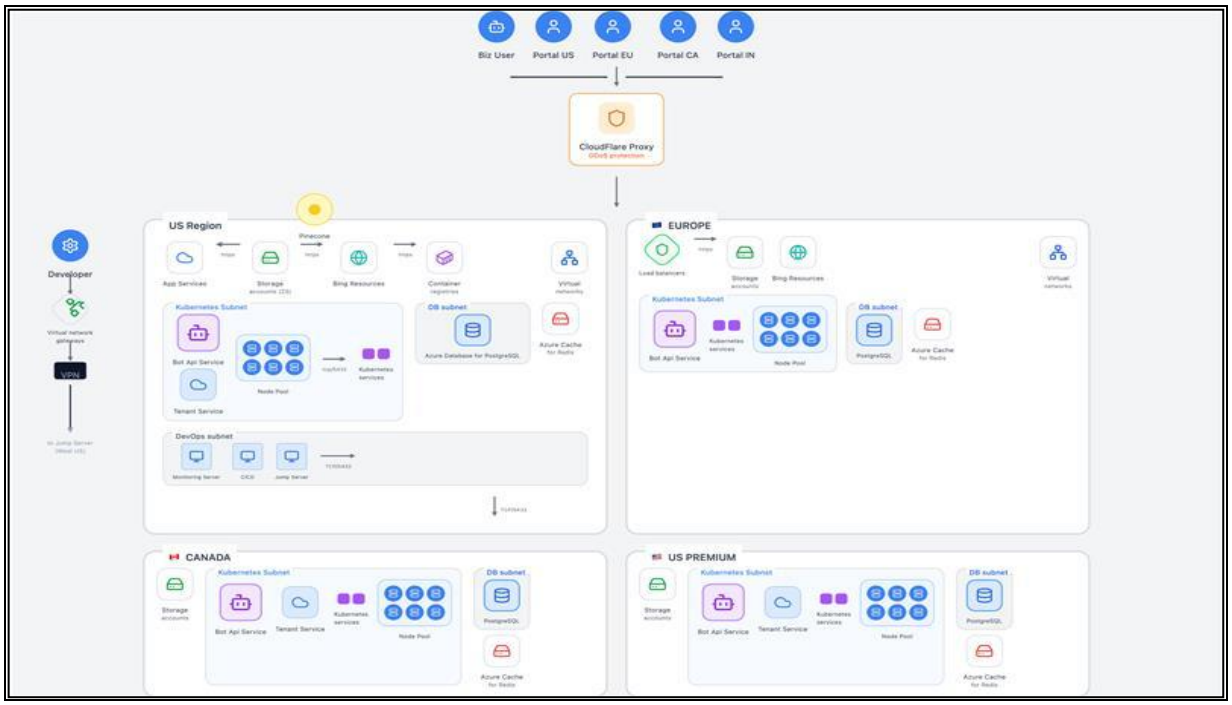
Network Segmentation Overview

Rezolve.ai does not maintain a traditional office network or on-premises internet access. All significant operations are conducted via cloud infrastructure. Employees access cloud systems from Rezolve.ai-provided, hardened endpoint device.

Network Connection to Client Sites

Rezolve.ai teams access client networks only when required for support, using secured connections — including site-to-site VPN, dual-factor authentication, and IP whitelisting — in accordance with each client's security policies. Client application credentials are provided to authorized employees on a need-to-know basis. Clients are notified promptly of any terminations or role changes affecting personnel with access to client systems.

Network Diagrams



Additional Network Security Controls

- Data in transit is encrypted using industry-standard encryption. Communication between Rezolve.ai Infrastructure and hardened workstations is over encrypted VPNs.
- No production data is residing in non-production environments.
- Hardware-based full disk encryption is enabled for all virtual machines within Azure as part of the initial setup. The Pseudonymization and Encryption Policy specifies the expected levels of cryptographic control.

Physical Structures and Physical Access

Physical Structure Overview

Rezolve.ai occupies office space within shared coworking facilities. Physical access to these facilities is controlled via multi-factor authentication (biometrics and passcode) provided by the coworking operator and monitored by CCTV. Development centers are located in Dehradun, Chennai, Bengaluru (India), and Covington, KY (USA). Entrances are secured by security personnel and biometric access control systems. Biometric thumbprint and door passcode are required to access office areas.

Attendance is recorded through the biometric system. Employees are required to always display and wear their ID cards within the facility. ID cards are issued to new employees following an access requisition initiated by the Human Resources (HR) group, with IT provisioning access rights accordingly. On employee separation, the HR group initiates the Exit Process, resulting in prompt revocation of physical and logical access privileges. Visitor, contractor, and third-party access to sensitive areas is managed on a need-to-have basis and monitored by security personnel.

Environmental Controls

Environmental controls (power backup, fire suppression, smoke detection) are the responsibility of the coworking facility provider at each location. Rezolve.ai is not responsible for the maintenance of environmental equipment or facilities.

Software

Firewalls

There are no on-premises firewalls, as all users connect directly to cloud infrastructure. Employees access cloud services securely from company-provided laptops. Internet access for certain employees is restricted through content filtering tools and VPN port restrictions, limiting access to approved sites required for production operations.

Network & Endpoint Protection / Monitoring

Access to Internet services from any company computing device (laptop, workstation, server etc.) or from any company address designation should be made through the company's approved perimeter security mechanisms.

Monitoring

Rezolve.ai has implemented monitoring controls to detect unauthorized information processing activities. Critical systems are configured to log user activities, exceptions, and information security events. System administrator and operator activities are logged and reviewed periodically.

Capacity management controls are in place to monitor and project resource requirements, minimizing the risk of performance degradation or systems failure. All new information systems, upgrades, and configuration changes are subject to formal analysis, testing, and approval before acceptance into production.

Patch Management

Operating system and infrastructure patches are managed by the Microsoft Azure team. Patches are assessed for stability and availability impact, tested, and deployed on a regular cycle or immediately in response to critical security events. Operating system patches for employee laptops are managed and applied as they become available.

Vulnerability Scans & Intrusion Detection/Intrusion Prevention

Rezolve.ai has implemented external Vulnerability Assessment and Penetration Testing (VAPT) scanning, initiated in 2023 conducted annually. Anti-virus software is installed and active on all in-scope desktops and laptops, with virus definition files updated daily by the vendor.

People

Organizational Structure

The organizational structure provides the overall framework for planning, directing, and controlling operations. Rezolve.ai's operations are overseen by Saurabh Kumar (CEO). The organization is structured across the following functional areas:

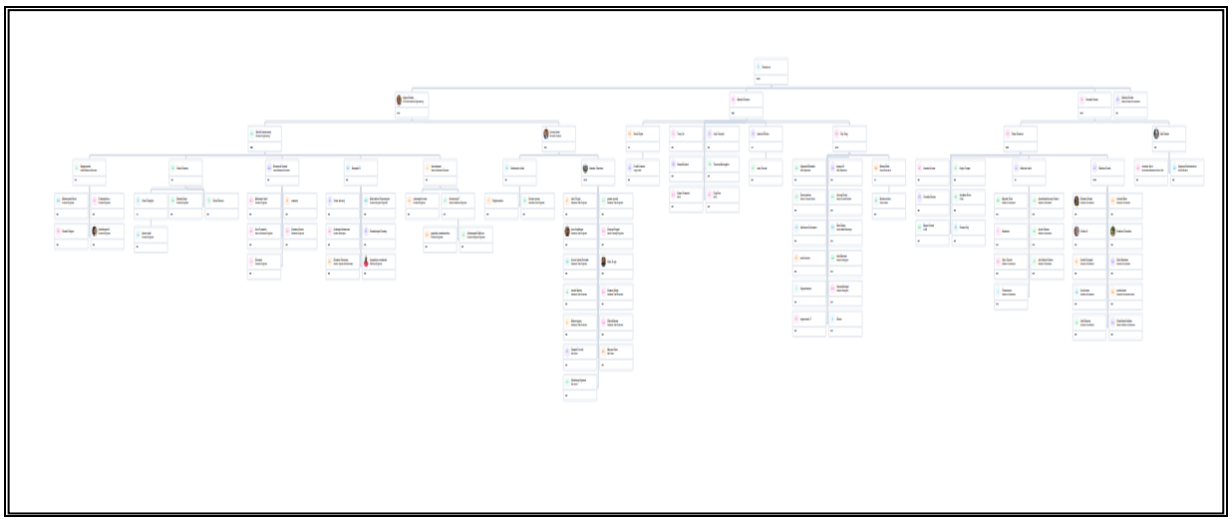
- Operations / Compliance
- Engineering
- Finance
- Marketing
- Sales
- Quality Assurance
- Product Delivery
- Information Technology

- Compliance and Audit
- Administration
- Human Resources
- Business Development

The management team meets periodically to review business unit plans and performances. Weekly, monthly meetings and calls with senior management, and department heads are held to review operational, security and business issues, and plans for the future.

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

Rezolve.ai Organization Chart



Roles and Responsibilities

The following are the responsibilities of key roles.

CEO (Chief Executive Officer)

The CEO is in charge company's fiscal activity, including budgeting, reporting, and auditing. Work with the executive board to determine values and mission, and plan for short and long-term goals. Seek opportunities to work alongside marketing to identify new customer. Make high-quality investing decisions to advance the business and increase profits. Build alliances and partnerships with other organizations. Assure all legal and regulatory documents are filed and monitor compliance with laws and regulations. CEO is also functioning as the Chief Privacy Officer in the organization.

CTO (Chief Technology Officer)

The CTO is in charge of the technical assets of the organization and developing safeguards to reduce the risk of breaches. Responsible for developing and implementing internal communication systems, generating IT budgets, evaluating new technologies, managing digital media assets, and executing policies. Helps maintain production applications and tackle high profile customer escalations. Determine all technology requirements of company and prepare appropriate growth and development plans. CTO is also functioning as the Chief Information Security Officer (CISO) in the organization.

The CISO is charge of security for the organization. Develop, maintain and oversee agency-wide IT security programs. Oversee the establishment and maintenance of information security on an automated and continuous basis. Detect, report, contain and mitigate incidents that impair adequate data and infrastructure security. Report within 24 hours of IT security incidents to the appropriate security

operations center.

HBD (Head of Business Development)

The HBD is in charge of business growth and development for company. Develop a growth strategy focused both on financial gain and customer satisfaction. Promote the company's products/services addressing or predicting clients' objectives. Prepare sales Contracts ensuring adherence to law established rules and guidelines. Researching business opportunities and viable income streams. Research and develop a thorough understanding of the company's people and capabilities.

Customer Success Director

The Customer Success Director is charge of delivery of product and client implementation. Lead the collaborative, dynamic planning process – prioritizing the work that needs to be done against the capacity and capability of the team. Ensure all products are built to an appropriate level of quality. Identifying and implementing technology trends that will be able to support the future success of the business.

Commitment To Competence

Rezolve.ai's formal job descriptions outline the responsibilities and qualifications required for each position in the company. Training needs are identified on an ongoing basis and are determined by the current and anticipated needs of the Business. Employees are evaluated on an annual basis to document performance levels and to identify specific skill training needs.

Assignment of Authority and Responsibility

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

Human Resources Policies and Procedures

Rezolve.ai maintains written Human Resources Policies and Procedures. The policies and procedures describe Rezolve.Ai's practices relating to hiring, training and development, performance appraisal and advancement, and termination. Human Resource ('HR') policies and practices are intended to inform employees on topics such as expected levels of integrity, ethical behavior, and competence.

The Human Resources department reviews these policies and procedures periodically 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 and sign an acknowledgment form confirming their receipt. Personnel policies and procedures are documented in the Human Resources Policy.

New Hire Procedures

New employees are required to read Rezolve.ai's corporate policies and procedures and sign an acknowledgment form stating that they have read and understood them. 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.

Background and reference checks are completed for prospective employees before employment over the phone. Employees are required to sign Employee Confidentiality Agreement and are on file for employees. Discrepancies noted in background investigations are documented and investigated by the Human Resources Department in conjunction with a third-party verification agency. Any discrepancies found in background investigations result in disciplinary actions, up to and including employee termination.

Training and Development

Training needs are assessed on an ongoing basis and aligned to current and anticipated business requirements. Targeted training is provided to employees as needed. Regular security awareness training is provided to all technical employees. As part of the onboarding process, HR coordinates information

security awareness training for all new employees.

Performance Evaluation

Rezolve.ai operates a formal performance review program. Employee performance reviews, promotions, and compensation adjustments are conducted annually. Reviews are completed jointly by the employee and their manager and are signed by both parties.

New Employee Training

HR coordinates to provide information security awareness program to all employees as part of induction. HR maintains the records of information security awareness training namely attendance sheets and feedback forms from employees. Employees undergo security awareness training regularly.

Employee Terminations

Terminations are processed in accordance with Rezolve.ai's HR procedures. All employees, contractors, and third-party personnel are required to return physical and digital identification and access tokens upon termination. Access privileges — physical and logical — are revoked promptly on separation. Where an employee changes role, prior access rights are removed and new access is provisioned appropriately for the new role.

Ethical Practices

Rezolve.ai reinforces the importance of the integrity message and the tone starts at the top. Every employee, manager, and director consistently maintain an ethical stance and supports ethical behavior. Employees encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.

Code of Conduct and Disciplinary Action

Rezolve.ai maintains a Code of Conduct setting out expected standards of behavior and providing a consistent and fair disciplinary process. Breaches of the Code of Conduct are subject to disciplinary action, up to and including termination of employment.

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, etc. Additionally, production and training standard operating procedures are available.

Help Desk

Rezolve.ai has support document which is shared with client. In case of incident and support required by user, user can reach for support by sending the mail. If urgency is there then contact person name and contact number are available to escalate the incident. All requests received are considered criticality and resolved within the minimum resolution time as detailed in the Change Management and Incident Response procedure.

Change Management

Rezolve.ai 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 to any work product. All the changes need to be subjected to a formal Change Management process.

Change Management covers any change to the Information assets and infrastructure of Rezolve.ai and includes but is not limited to addition/ modification in the application, application components, database

structure, DBMS, system and network components, policies, and procedures.

Every change to such baselined components is governed by the change control and management procedures as outlined in the Helpdesk, Change management, and Incidence Response procedure. Rezolve.ai'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 every significant change is analyzed and approved by the IT Head before such implementation. A sign-off was obtained from the person 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. The help desk personnel study and escalate all security incidents to the designated team for further escalation/resolution. Any event related to security of Information assets including facilities and people are termed as an Incident.

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. Root-cause analyses of all the incidents are performed and the root cause identified shall remedy and reported. The actions proposed from the root-cause analyses are approved by CTO.

Logical Access

Security Authorization and Administration

Email is sent from HR to 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. Any additional access is recommended by the line manager and/or CTO. The company has a standard configuration that is implemented across Desktops & laptops individually.

Only the IT team has access to change user profiles or give higher access. Other employees do not have local admin privileges on their desktops, only the IT team has access to install software on employees' machines. The ability to create or modify users and user access privileges is limited to the IT team.

User Access and review

Access is granted based on authenticated user identity (unique login ID and password). Asset owners are responsible for periodically evaluating the appropriateness of access rights based on job roles. Access rights are documented in an Access Rights Tracker and reviewed by the IT team on a regular basis. Privileged access to sensitive resources is restricted to the IT team.

Security Configuration

Employees establish their identity to the network and remote systems through the use of a valid unique user ID that is authenticated by an associated password.

Passwords are controlled through Password policy and include periodic forced changes, password expiry, and complexity requirements. User accounts are disabled after a limited number of unsuccessful login 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.

Additional IT Infra security controls

- The use of encrypted VPN channels helps to ensure that only valid users gain access to IT components.

- Remote access is permitted to all employees via VPN.
- Unattended desktops are locked within a time of inactivity. Users are required to provide their password to unlock the desktop.
- Administrative rights and access to administrative accounts are granted to individuals that require that level of access to perform their jobs. All administrative level access, other than to the IT team, must be justified and approved.
- USB Ports are disabled for employees and hard drives are encrypted for all laptops.

Confidentiality

Rezolve.ai has implemented a data retention policy to ensure the confidentiality of client data. All agreements with related parties and vendors include confidentiality commitments consistent with the company's confidentiality policy.

Secure disposal procedures are established for media no longer required, with the level of destruction determined by the information classification of the data held on the media. Additional controls include:

- Access to data is restricted through the access control system and password-controlled storage.
- Data is classified as public, internal, or confidential, with access controls applied accordingly.
- No confidential customer data is stored on the Rezolve.ai office network.

Availability

Backup and Recovery of Data

Rezolve.ai maintains a formal Backup Policy. Backup processes define the type of information to be backed up, backup cycles, and backup methods. These processes are approved by business owners and comply with business continuity, legal, and regulatory requirements. All backup and restoration logs are maintained for defined retention periods. Backup copies are tested periodically to verify secure recoverability.

Additional Controls Relating to Availability

- Periodic backup copies are stored in a secure cloud location.
- Periodic replication of production data is performed automatically to another availability zone within Azure

Applicable Trust Services Criteria and related Controls

The control objectives and Rezolve.ai's related controls are included in section 4 of this report, "Independent Service Auditor's Description of Tests of Controls

Complementary User- Entity Controls

Services provided by Rezolve.ai to user entities and the controls of Rezolve.ai cover only a portion of the overall controls of each user entity. Rezolve.ai 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 Rezolve.ai. This section highlights those internal control responsibilities that Rezolve.ai 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.

- **Contractual Arrangements**
    - User organizations are responsible for understanding and complying with their contractual obligations to Rezolve.ai such as providing input information, reviewing and approval of processed output, and releasing any instructions.

- **Other Controls**

#	Complementary User Entity Controls	Related Criteria
1	User Organizations are responsible for their network security policy and access management for their networks, application & data.	CC 6.1: 4
2	User Organizations are responsible for working with Rezolve.ai to jointly establish service levels and revise the same based on changes in business conditions. User Organizations are responsible for reviewing specific SLA reports and hold meetings jointly with Rezolve.ai	CC 2.2: 5
3	User Organizations are responsible for implementing sound and consistent internal controls regarding general IT system access and system usage. User Organizations are responsible for implementing controls necessary to ensure that transactions relating to Rezolve.ai services are appropriately authorized, timely, and complete.	CC 6.1: 4
4	User Organizations are responsible for implementing controls to remove user access for terminated users and who were involved in services associated with Rezolve.ai services.	CC 6.1: 4, CC 6.1: 14, CC 6.1: 16, CC 6.3: 3
5	User Organizations are responsible for ensuring that any data sent to Rezolve.ai should be protected by methods to ensure confidentiality, privacy, integrity, availability. User Organizations are responsible for ensuring that input data is provided by them as per the process agreed with Rezolve.ai and using the secure HTTPS/SFTP or other secure connections and mechanisms.	CC 6.1: 4, CC 6.1: 14
6	User Organizations are responsible for logging any complaint, service disruption, or security incident with Rezolve.ai.	CC 1.1: 5, CC 2.3:3, CC 7.2: 2
7	User Organizations are responsible for approving any change requests, releases or UAT sign off on UE initiated changes User Organizations are responsible for ensuring that complete, accurate, and timely information is provided to Rezolve.ai for processing. User Organizations are responsible for ensuring that clear instructions are provided to Rezolve.ai as part of the onboarding process and project setup.	CC 8.1

8	User Organizations are responsible for ensuring restricted access control to Rezolve.ai applications and systems. UE is responsible to provide complete and accurate access requests during the onboarding process.	CC 6.6: 2, CC 9.2: 1

SECTION 4

INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

Audit Methodology

Introduction

Our examination was limited to the controls specified by Rezolve.ai in sections 3, “Management of Rezolve.ai’s Description of its System,” and 4 of the report, and did not extend to controls in effect at user entities.

It is the responsibility of each user entity and its independent auditor to evaluate this information in conjunction with the evaluation of internal control over financial reporting at the user entity in order to assess total internal control. If internal control is not effective at user entities, Actionable Science Labs Pvt. Ltd (Rezolve.ai)'s controls may not compensate for such weaknesses.

Rezolve.ai's internal control represents the collective effect of various factors on establishing or enhancing effectiveness of the controls specified by Rezolve.ai. In planning the nature, timing, and extent of our testing of the controls to achieve the control objectives specified by Rezolve.ai, we considered aspects of Rezolve.ai’s control environment, risk assessment process, monitoring activities, and information and communications.

Tests of Operating Effectiveness of Specific Controls

The control environment represents the collective effort of various elements in establishing, enhancing, or mitigating the effectiveness of specific controls. In addition to tests of specific controls described below, our procedures included tests of, or consideration of, the relevant elements of the control environment including:

- Organizational structure and approach to segregation of duties;
- The function of management and its established procedures relating to developing and disseminating new policies and procedures;
- Management control methods; and
- Personnel policies and practices of the Company.

Our tests of the control environment included the following procedures, to the extent considered necessary:

- review of organizational structure, including management controls, segregation of functional responsibilities, policy statements, accounting and processing manuals, and personnel policies;
- discussions with management, operations, administrative, and other personnel who are responsible for developing, ensuring adherence to, and applying controls;
- observations of personnel in the performance of their assigned duties; and
- review of actions taken by the Company in response to recommendations to improve controls made by management, personnel responsible for compliance adherence, and any outside advisors and experts engaged by the Company.

Our tests of the operating effectiveness of the specific controls included such tests as were considered necessary, given the circumstances, to evaluate whether the controls, and the extent of compliance with them, were sufficient to provide reasonable, but not absolute, assurance.

Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity (IPE)

In addition, as required by paragraph 35 of AT-C section 205 and paragraph .30 of AT-C section 320, when using information produced (or provided) by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

When IPE was used for sampling purposes, (such as HR population, lists of change requests, incidents, etc) we performed the following procedures to ensure completeness, the accuracy of the data/reports, and lists provided.

- Inquiry with management that the list is complete and covers all in-scope products, services, and people.
- Review of the sequences, Employee ID, and other transaction numbers for completeness.
- Reasonable checks against other data provided including last year's data.
- Requesting clients to generate the population and reports from the source systems in our presence, where feasible.

Testing Methodology

Section 4 outlines the controls in place by Rezolve.ai and describes the tests of their effectiveness performed by the independent service auditor. The following methodologies were used in testing the suitability of the design and operating effectiveness of Rezolve.ai's controls:

Test Methodology	Description
Inquiry	The auditor inquired of relevant personnel to corroborate control placement or activity.
Inspection	The auditor obtained and read relevant documentation or read the screenshots provided.
Observation	The auditor directly witnessed control placement or activity or evidence thereof.
Reperformance	The auditor reperformed the control steps

Materiality

We report all deviations which have been identified during the test of controls. User entities should determine the materiality of these deviations in respect to their contract with the service organization.

Independent Service Auditor's Description of Tests of Controls and Results

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
CC 1	**Control Environment:**			
CC 1.1	Integrity and Ethics: COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected a sample of performance appraisals for existing employees to determine that performance appraisals are performed at least annually.	No exception noted
		The company performs background checks on new employees.	Inspected the Human Resource Security Policy to determine the has been created and approved. Selected a sample of new joiners and inspected the BGV reports to determine that background verifications are carried out by the company.	No exception noted
		The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.	Inspected the code of conduct policies to determine that the company has established standards and guidelines for personnel / contractors' ethical behavior including code of conduct. Inspected a sample of contractor agreements to determine that the agreement includes Security, Confidentiality, and Breach Notification clauses.	No exception noted
		The company requires contractors to sign a confidentiality agreement at the time of engagement.	Inspected a sample of contractor agreements to determine that contractors sign a confidentiality agreement at the time of engagement.	No exception noted
		The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the	Inspected the code of conduct policies to determine that the company has established standards	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
		code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	and guidelines for personnel ethical behavior including code of conduct. Inspected the sample new joiners' policy acceptance to determine that the code of conduct has been acknowledged by all the new joiners.	
		The company requires employees to sign a confidentiality agreement during onboarding.	Selected a sample of new joiners and inspected the sample new joiners' policy acceptance to determine that the code of conduct has been acknowledged by all the new joiners.	No exception noted
CC 1.2	Board Oversight: COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. The board engages third-party information security experts and consultants as needed.	Inspected the Board of directors' profile to determine that board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls.	No exception noted
		The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected company's board of directors charter to determine that it outlines Board of Directors' oversight responsibilities for internal control.	No exception noted
		The company's board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the company.	Inspected a copy of the annual board meeting presentation (containing annual, medium term plans) done by Senior management to determine that strategic plans / business objectives are in place. Selected a sample of MRM meetings held and inspected the minutes to determine that MRM are held on a periodic basis.	No exception noted
		The company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The	Inspected a copy of the annual board meeting presentation and minutes of meetings to determine that state of the company's cybersecurity and privacy	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
		board provides feedback and direction to management as needed.	risk, feedbacks and direction to management are discussed in the same.	
CC 1.3	Management Structures: COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected Information security Roles and Responsibility Document to determine that Information Security Roles and Responsibilities has been created and approved.	No exception noted
		The company maintains an organizational chart that describes the organizational structure and reporting lines.	Inspected the organization chart for an understanding of the hierarchy. Enquired with Management to determine that organization charts are updated periodically.	No exception noted
		The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected Information security Roles and Responsibility Document to determine that Information Security Roles and Responsibilities has been created and approved.	No exception noted
		The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected company's board of directors charter to determine that it outlines Board of Directors' oversight responsibilities for internal control.	No exception noted
CC 1.4	Attract and Retain Talent: COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected Information security Roles and Responsibility Document to determine that Information Security Roles and Responsibilities has been created and approved.	No exception noted
		The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected a sample of performance appraisals for existing employees to determine that performance appraisals are performed at least annually.	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
		The company performs background checks on new employees.	Inspected the Human Resource Security Policy to determine the has been created and approved. Selected a sample of new joiners and inspected the BGV reports to determine that background verifications are carried out by the company.	No exception noted
		The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.	Selected a sample of new joiners and inspected the training records to determine that new joiners undergo information security trainings.	No exception noted
CC 1.5	Accountability: COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected Information security Roles and Responsibility Document to determine that Information Security Roles and Responsibilities has been created and approved.	No exception noted
		The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected a sample of performance appraisals for existing employees to determine that performance appraisals are performed at least annually.	No exception noted
		The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Inspected the code of conduct policies to determine that the company has established standards and guidelines for personnel ethical behavior including code of conduct. Inspected the sample new joiners' policy acceptance to determine that the code of conduct has been acknowledged by all the new joiners.	No exception noted
CC 2	**Communication and Information:**			
CC 2.1	Internal Communication and Information: COSO Principle	Host-based vulnerability scans are performed at least quarterly on all	Inspected the external VAPT report/tools to determine that all the	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
	13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	external-facing systems. Critical and high vulnerabilities are tracked to remediation.	issues identified for Cloud infrastructure as Critical/High/Medium/Low are addressed and closed. Inspected the external VAPT report to determine that all the issues identified for Code Repository as Critical/High/Medium/Low are addressed and closed. Inspected the security incident tracker to determine that all security issues are tracked/have owners assigned and closed.	
		The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.	Inspected the Azure controls self-assessments on continuous basis, and has configured SLAs in the application. Inspected a sample of SLA breach cases to determine that findings are reviewed and closed as per the remediation date.	No exception noted
		The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected the integrations section on Azure to determine that cloud infrastructure are successfully linked. Inspected the cloud configuration settings to determine that logs are enabled for all the cloud accounts and only authorized users can access the logs Inspected the cloud storage settings to determine that logs are enabled and logs are retained at least for 365 days Inspected the cloud configuration to	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
			determine that VNets flow logs are enabled.	
CC 2.2	Internal Communication: COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected Information security Roles and Responsibility Document to determine that Information Security Roles and Responsibilities has been created and approved.	No exception noted
		The company communicates system changes to authorized internal users.	Enquired with the management and inspected screenshots of internal communication channels (email, Slack, Teams, etc.) for tracking deployment of code changes to determine that changes are communicated internally.	No exception noted
		The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns.	Inspected the whistle blower policy to determine that the same is documented and approved. Inspected Information security Roles and Responsibility Document to determine that Information Security Roles and Responsibilities has been created and approved.	No exception noted
		The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Security and Privacy Incident response policies and procedure to determine that the same is documented and approved.	No exception noted
		The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected Information security Roles and Responsibility Document to determine that Information Security Roles and Responsibilities has been created and approved.	No exception noted
		The company provides a description of its products and services to internal and external users.	Enquired with the management whether the company provides a description of its products and services to internal and external users.	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
			Inspected available public link, documentation of how-to guides and reference materials for company's product or service.	
		The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.	Selected a sample of new joiners and inspected the training records to determine that new joiners undergo information security trainings.	No exception noted
		The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the Information Security policy and other IT policy to determine that the same is documented and approved.	No exception noted
CC 2.3	External Communication: COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected publicly available customer support site and a sample of customer support request emails/tickets to determine that customers have a mechanism to communicate with the Entity.	No exception noted
		The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected sample vendor agreements including cloud provider service agreement to determine that these agreement includes confidentiality and privacy commitments applicable to the entity. Inspected the link to publicly available Privacy policy and Terms of Service to determine that the same is documented.	No exception noted
		The company notifies customers of critical system changes that may affect their processing.	Enquired with the management that the company notifies customers of critical system changes that may affect their processing. Inspected the available link to public release notes/updates or a screenshot of the sample product update communication to customers.	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
		The company provides a description of its products and services to internal and external users.	Enquired with the management whether the company provides a description of its products and services to internal and external users. Inspected available public link, documentation of how-to guides and reference materials for company's product or service.	No exception noted
		The company provides guidelines and technical support resources relating to system operations to customers.	Enquired with the management whether the company provides guidelines and technical support resources relating to system operations to customers. Inspected publicly available customer support site and a sample of customer support request emails/tickets to determine that customers have a mechanism to communicate with the Entity.	No exception noted
		The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).	Inspected the Signed Mater service agreement (MSA) with sample clients to determine that the same is documented and communicated to the clients. Inspected available links to publicly accessible Terms of Service page outlining company's security practices to determine that the security commitments are communicated to the customers.	No exception noted
CC 3	**Risk Assessment:**			
CC 3.1	Business Objectives: COSO Principle 6: The entity specifies objectives with sufficient clarity to enable	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the	Inspected the risk management policy to determine the same is documented and approved.	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
	the identification and assessment of risks relating to objectives.	significance of the risks associated with the identified threats, and mitigation strategies for those risks.		
		The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the sample new joiners' policy acceptance to determine that the policy has been agreed by all the employees. Inspected the Risk Register maintained.	No exception noted
CC 3.2	Risk Assessments: COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the BCP and DR plan to determine the same is documented and approved. Inspected the BCP and DR activity report to determine whether business continuity and disaster recovery plans are tested.	No exception noted
		The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy to determine the same is documented and approved.	No exception noted
		The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the Third-Party Management Policy to determine the same is documented and approved. Inspected the vendor monitoring console on Azure to determine that all the vendor have been assigned with level of risks	No exception noted
		The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally	Inspected the risk management policy to determine the same is documented and approved. Inspected the Risk register to	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
		assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	determine that risk assessment is performed annually.	
CC 3.3	Fraud Risk: COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy to determine the same is documented and approved.	No exception noted
		The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk management policy to determine the same is documented and approved. Inspected the Risk register to determine that risk assessment is performed annually.	No exception noted
CC 3.4	Changes to Systems and Risks: COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the Operations Security Policy to determine configuration management is defined within it and approved. Inspected sample configurations for cloud resources.	No exception noted
		The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy to determine the same is documented and approved.	No exception noted
		The company's penetration testing is performed at least annually. A remediation plan is developed and	Inspected the latest vulnerability assessment /penetration test report performed by a third party and determined that VA/PT are carried out	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
		changes are implemented to remediate vulnerabilities in accordance with SLAs.	periodically. Inspected sample tickets raised / minutes of management meetings to address vulnerabilities discovered in VA/PT to determine that vulnerabilities were closed.	
		The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk management policy to determine the same is documented and approved. Inspected the Risk register to determine that risk assessment is performed annually.	No exception noted
CC 4	**Monitoring Activities:**			
CC 4.1	Evaluation of Internal Controls: 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.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the external VAPT report/tools to determine that all the issues identified for Cloud infrastructure as Critical/High/Medium/Low are addressed and closed. Inspected the external VAPT report to determine that all the issues identified for Code Repository as Critical/High/Medium/Low are addressed and closed. Inspected the security incident tracker to determine that all security issues are tracked/have owners assigned and closed.	No exception noted
		The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory;	Inspected the Third-Party Management Policy to determine the same is documented and approved.	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
		- vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the vendor monitoring console on Azure to determine that all the vendor have been assigned with level of risks	
		The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.	Inspected the Azure controls self-assessments on continuous basis, and has configured SLAs in the application. Inspected a sample of SLA breach cases to determine that findings are reviewed and closed as per the remediation date.	No exception noted
		The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the latest vulnerability assessment /penetration test report performed by a third party and determined that VA/PT are carried out periodically. Inspected sample tickets raised / minutes of management meetings to address vulnerabilities discovered in VA/PT to determine that vulnerabilities were closed.	No exception noted
CC 4.2	Internal Control Deficiencies: COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the Third-Party Management Policy to determine the same is documented and approved. Inspected the vendor monitoring console on Azure to determine that all the vendor have been assigned with level of risks	No exception noted
		The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed	Inspected the Azure dashboard to perform controls self-assessments on continuous basis, and has configured SLAs in the application. Inspected a sample of SLA breach cases to determine that findings are	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
		to an SLA for a finding, the corrective action is completed within that SLA.	reviewed and closed as per the remediation date.	
CC 5	**Control Activities:**			
CC 5.1	Risk Mitigation: 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.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy to determine the same is documented and approved.	No exception noted
		The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the Information Security policy and other IT policy to determine that the same is documented and approved.	No exception noted
CC 5.2	General Controls over Technology: COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the Secure Development Policy to determine that the same has been created, it governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements and is approved.	No exception noted
		The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the Access Control policy and other IT policy to determine that the same is documented and approved. Selected a sample of new joiner employees with privileged access and inspected the authorization email to determine that such access is approved prior to setup.	No exception noted
		The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the Information Security policy and other IT policy to determine that the same is documented and approved.	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
CC 5.3	Policies and Procedures: COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected Information security Roles and Responsibility Document to determine that Information Security Roles and Responsibilities has been created and approved.	No exception noted
		The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy to determine the same is documented and approved.	No exception noted
		The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the Secure Development Policy to determine that the same has been created, it governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements and is approved.	No exception noted
		The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the Third-Party Management Policy to determine the same is documented and approved. Inspected the vendor monitoring console on Azure to determine that all the vendor have been assigned with level of risks	No exception noted
		The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the Data Management Policy to determine the same has been created and approved.	No exception noted
		The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Security and Privacy Incident response policies and procedure to determine that the same is documented and approved.	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
		The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the Change Management Policy / SDLC policy and Procedures to determine that they define how changes to software and infrastructure components of the service should be authorized, documented, tested, reviewed, and approved prior to being implemented in the production environment. Inspected evidence that the policy is reviewed and approved during the audit period. Inspected sample change tickets to determine that approval is required to merge to the default branch for all linked version control repositories.	No exception noted
		The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the sample new joiners' policy acceptance to determine that the policy has been agreed by all the employees. Inspected the Risk Register.	No exception noted
		The company's data backup policy documents requirements for backup and recovery of customer data.	Inspected the Data Management Policy to determine the same has been created and approved.	No exception noted
		The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the Information Security policy and other IT policy to determine that the same is documented and approved.	No exception noted
CC 6	**Logical and Physical Access Controls:**			
CC 6.1	Logical Access: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect	System access restricted to authorized access only	Inspected the IAM settings to determine that security groups are created and each groups have at least one IAM policy linked to the group. Inspected a sample of access	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
	them from security events to meet the entity's objectives.		requests to determine that access is granted to authorized users.	
		The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Selected a sample of new joiner employees and inspected the authorization email to determine that such access / privileged is approved prior to setup.	No exception noted
		The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the Data Management Policy to determine the has been created that defines confidential data storage and security and access restrictions to authorized personnel and it is approved.	No exception noted
		The company maintains a formal inventory of production system assets.	Inspected the Inventory section in Azure and determined that a formal inventory of production system assets is maintained and their owners are clearly documented.	No exception noted
		The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as unique SSH key.	Inspected the settings of cloud infra/Code Repository/Identity provider to determine that MFA is enabled on all the accounts. Inspected cloud settings to determine that direct access to production instances is only through 2048 bit SSH keys.	No exception noted
		The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.	Inspected the IAM settings and security groups to determine that several groups have been formed for different teams and only the production group has access to production resources. Inspected the IAM settings and security groups to determine that several groups have been formed for different teams and only the	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
			production group has access to production resources.	
		The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected settings on the cloud console to determine that direct access to production instances is only through 2048 bit SSH keys. Inspected evidence for implementation of https encryption to determine that secure https connections are used.	No exception noted
		The company requires passwords for in-scope system components to be configured according to the company's policy.	Inspected the default password security setting in the IAM tool / G-Suite / Cloud console to determine that password settings are: 1. length of 8-character length 2. complexity is enabled 3. password expires in 60 days 4. Password history is set at 6 5. Minimum password age is set at 2 days. Inspected the cloud settings to determine that password policies are enabled	No exception noted
		The company restricts access to migrate changes to production to authorized personnel.	Inspected sample change tickets to determine showing recent successful production code deployments. Inspected code repository console to determine that access to merge codes and migrate changes to production are restricted to authorized personnel.	No exception noted
		The company restricts privileged access to databases to authorized users with a business need.	Inspected the infrastructure to determine that only privileged users have access to the Database.	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
			Inspected the access review reports to determine that access to Database is reviewed periodically.	
		The company restricts privileged access to encryption keys to authorized users with a business need.	Inspected the cloud console to determine that only privileged users have access to the encryption keys. Inspected the access requests to determine that access to encryption keys is granted only to only authorized users.	No exception noted
		The company restricts privileged access to the firewall to authorized users with a business need.	Inspected the Access Management Policy to determine has been created and approved. Inspected network security settings to determine that 1. VNet has been setup and all production server are within the private subnet 2. Direct access to production instances is only through 2048 bit SSH keys. Inspected the IAM settings and security groups to determine that only the production group has access to production resources. Inspected database configurations to determine that database can be accessed only from certain security groups and cannot be accessed directly. Inspected SSH settings in SSH client to determine that encrypted SSH key is required for connecting to Azure / Cloud infrastructure.	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
		The company restricts privileged access to the operating system to authorized users with a business need.	Inspected the access review reports to determine that access to Operating System is reviewed periodically Inspected the cloud console to determine that only privileged users have access to the production system / operating system in end user machines.	No exception noted
		The company restricts privileged access to the production network to authorized users with a business need.	inspected cloud / network management console to determine that admin / root access to cloud infrastructure is restricted	No exception noted
		The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the Access Control policy and other IT policy to determine that the same is documented and approved. Selected a sample of new joiner employees with privileged access and inspected the authorization email to determine that such access is approved prior to setup.	No exception noted
		The company's datastores housing sensitive customer data are encrypted at rest.	Inspected encryption settings on cloud infra to determine that databases including user data in cloud instances and other data are encrypted at rest .	No exception noted
		The company's network is segmented to prevent unauthorized access to customer data.	Inspected the Information Security policies and scope document to determine that the company has defined system boundaries. Inspected the networking diagrams to determined that these are documented.	No exception noted
		The company's production systems can only be remotely accessed by authorized employees possessing a	Inspected the settings of cloud infra / code repository / Identity provider to determine that MFA is enabled on all	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
		valid multi-factor authentication (MFA) method.	the accounts including Admin users and root accounts.	
		The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the properties of VNet security group and determined that the inbound connection to instances in the VNet is set to be accessed by a SSH connection. Inspected SSH settings in SSH client to determine that encrypted SSH key is required for connecting to Cloud infrastructure.	No exception noted
CC 6.2	Granting Logical Access: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the employee handbook or Human Resource Security / Access Control policy to determine that the company establishes information security commitments for former employees following termination. Selected a sample of exited users and inspected Exit Checklist/ticket and Access page on Azure Directory showing disabled status in the primary authentication system along with other critical applications to determine that the exit process and related account deactivation is as per defined procedures and offboarding had marked as completed.	No exception noted
		The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the Access Control policy to determine that the same is documented and approved. Inspected integrations and access page in Azure to determine that all critical systems including Azure/ Bitbucket/O365 etc. are linked to Azure and all related accounts have been linked to users within Azure.	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
			Inspected the access review report for all in-scope components, including data stores, cloud infrastructure, version control system to determine that	
		The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Selected a sample of new joiner employees and inspected the authorization email to determine that such access / privileged is approved prior to setup.	No exception noted
		The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected settings on the cloud console to determine that direct access to production instances is only through 2048 bit SSH keys. Inspected evidence for implementation of https encryption to determine that secure https connections are used.	No exception noted
		The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the Access Control policy and other IT policy to determine that the same is documented and approved. Selected a sample of new joiner employees with privileged access and inspected the authorization email to determine that such access is approved prior to setup.	No exception noted
CC 6.3	Revoking or modifying Logical Access: 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,	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the employee handbook or Human Resource Security / Access Control policy to determine that the company establishes information security commitments for former employees following termination. Selected a sample of exited users	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
	giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.		and inspected Exit Checklist/ticket and Access page on Azure showing disabled status in the primary authentication system along with other critical applications to determine that the exit process and related account deactivation is as per defined procedures and offboarding had marked as completed in Azure.	
		The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the Access Control policy to determine that the same is documented and approved. Inspected integrations and access page in Azure to determine that all critical systems including Azure/ GW/ Bitbucket/O365 etc. are linked to Azure and all related accounts have been linked to users within Azure. Inspected the access review report for all in-scope components, including data stores, cloud infrastructure, version control system to determine that	No exception noted
		The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Selected a sample of new joiner employees and inspected the authorization email to determine that such access / privileged is approved prior to setup.	No exception noted
		The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected settings on the cloud console to determine that direct access to production instances is only through 2048 bit SSH keys. Inspected evidence for implementation of https encryption to	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
			determine that secure https connections are used.	
		The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the Access Control policy and other IT policy to determine that the same is documented and approved. Selected a sample of new joiner employees with privileged access and inspected the authorization email to determine that such access is approved prior to setup.	No exception noted
CC 6.4	Physical Access: 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.	The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the Access Control policy to determine that the same is documented and approved. Inspected integrations and access page in Azure to determine that all critical systems including Azure/ Bitbucket/O365 etc. are linked to Azure and all related accounts have been linked to users within Azure. Inspected the access review report for all in-scope components, including data stores, cloud infrastructure, version control system.	No exception noted
		The company has processes in place for granting, changing, and terminating physical access to company data centers based on an authorization from control owners.	Inspected the Physical Security Policy to determine the same has been created and approved.	No exception noted
		The company requires visitors to sign-in, wear a visitor badge, and be escorted by an authorized employee when accessing the data center or secure areas.	Inspected the visitor register for a sample of dates to determine that visitor register is maintained. Virtually Observed that visitor badges are for identification purposes only and do not permit access to any secured areas of the facility.	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
			Virtually Observed that all visitors are escorted by an Entity employee when visiting the Entity office.	
		The company reviews access to the data centers at least annually.	Inspected evidence of access reviews for the data centers to determine that these are conducted annually.	No exception noted
CC 6.5	Media Handling: 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.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the employee handbook or Human Resource Security / Access Control policy to determine that the company establishes information security commitments for former employees following termination. Selected a sample of exited users and inspected Exit Checklist/ticket and Access page on Azure showing disabled status in the primary authentication system along with other critical applications to determine that the exit process and related account deactivation is as per defined procedures and offboarding had marked as completed in Azure.	No exception noted
		The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	Inspected the Asset Management Policy to determine has been created and approved. Inspected the media handling policy to determine that for all media that is disposed of, data is erased from these prior to disposal or reuse. Selected a sample of media destruction certifications / shredding evidences to determine that media containing information are destroyed prior to disposal.	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
		The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the Data Management Policy to determine the same has been created and approved.	No exception noted
		The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	Inspected the Data Management Policy manually to determine that it has been created and approved. Inspected a manually sample data deletion request to determine that the data is deleted as per SLA defined.	No exception noted
CC 6.6	Network Security: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the external VAPT report to determine that all the issues identified for Cloud infrastructure as Critical/High/Medium/Low are addressed and closed. Inspected the external VAPT report to determine that all the issues identified for code repository as Critical/High/Medium/Low are addressed and closed. Inspected the security incident tracker to determine that all security issues are tracked/have owners assigned and closed.	No exception noted
		The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected settings on the cloud console to determine that direct access to production instances is only through 2048 bit SSH keys. Inspected evidence for implementation of https encryption to determine that secure https connections are used.	No exception noted
		The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.	Inspected evidence of firewall ruleset reviews to determine that these are conducted annually.	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
		The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the external VAPT reports performed during the assessment period. 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.	No exception noted
		The company uses firewalls and configures them to prevent unauthorized access.	Observed that firewall device has been installed in the office network. Inspected firewall console screens containing rules about ports, incoming connection types, whitelisted IPs and type of traffic and determined that configuration is in compliance with the policy and incoming connection are allowed only from whitelisted IPs.	No exception noted
		The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the information security policies / encryption policy to determine that transmission of sensitive information over the internet happens only when the information is encrypted. Access to Internet services from any company computing device (laptop, workstation, server etc.) or from any company address designation is made through the company's approved perimeter security mechanisms	No exception noted
		The company's network and system hardening standards are documented,	Inspected the Operations Security Policy to determine the same contains network and system hardening	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
		based on industry best practices, and reviewed at least annually.	standards and approved. Inspected on Azure console to determine that Azure ECS services do not allow unrestricted access to TCP port 22.	
		The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Inspected the settings of cloud infra / code repository / Identity provider to determine that MFA is enabled on all the accounts including Admin users and root accounts.	No exception noted
		The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the properties of VNet security group and determined that the inbound connection to instances in the VNet is set to be accessed by a SSH connection. Inspected SSH settings in SSH client to determine that encrypted SSH key is required for connecting to Cloud infrastructure.	No exception noted
CC 6.7	Encryption Controls: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	The company encrypts portable and removable media devices when used.	Inspected the Cryptography policy to determine that the same is documented and approved. Inspected the Azure dashboard to determine that all laptops have the Azure Agent installed and removable media devices are encrypted.	No exception noted
		The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the information security policies / encryption policy to determine that transmission of sensitive information over the internet happens only when the information is encrypted. Access to Internet services from any company computing device (laptop, workstation, server etc.) or from any	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
			company address designation is made through the company's approved perimeter security mechanisms	
CC 6.8	Malicious software and Vulnerabilities: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.	Inspected the Azure dashboard that all employees required to install the Azure Agent have installed the agent on their workstations. Inspected Azure Dashboard to determined that antivirus is installed in all workstations.	No exception noted
		The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the Secure Development Policy to determine that the same has been created, it governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements and is approved.	No exception noted
		The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the external VAPT report to determine that all the issues identified for Cloud infrastructure as Critical/High/Medium/Low are addressed and closed. Inspected the external VAPT report to determine that all the issues identified for code repository as Critical/High/Medium/Low are addressed and closed. Inspected the security incident tracker to determine that all security issues are tracked/have owners assigned and closed.	No exception noted
CC 7	**System Operations:**			

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
CC 7.1	System Operations: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the external VAPT report/tools to determine that all the issues identified for Cloud infrastructure as Critical/High/Medium/Low are addressed and closed. Inspected the external VAPT report to determine that all the issues identified for Code Repository as Critical/High/Medium/Low are addressed and closed. Inspected the security incident tracker to determine that all security issues are tracked/have owners assigned and closed.	No exception noted
		The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the Operations Security Policy to determine configuration management is defined within it and approved. Inspected sample configurations for cloud resources.	No exception noted
		The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the Change Management Policy / SDLC policy and Procedures to determine that they define how changes to software and infrastructure components of the service should be authorized, documented, tested, reviewed, and approved prior to being implemented in the production environment. Inspected evidence that the policy is reviewed and approved during the audit period. Inspected sample change tickets to determine that approval is required to	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
			merge to the default branch for all linked version control repositories.	
		The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the Operations Security policy to determine that the Vulnerability Management and System Monitoring is documented and approved.	No exception noted
		The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk management policy to determine the same is documented and approved. Inspected the Risk register to determine that risk assessment is performed annually.	No exception noted
CC 7.2	Monitor events and attacks: 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.	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected the Azure dashboard settings for processing capacity to determine that they are used for monitoring the performance of the systems and configured to log alerts. Inspected the Azure infrastructure and configuration settings to determine that load balancers	No exception noted
		Host-based vulnerability scans are performed annually on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the external VAPT report/tools to determine that all the issues identified for Cloud infrastructure as Critical/High/Medium/Low are addressed and closed. Inspected the console of the Vulnerability scan reports to determine that all the issues identified for Code Repository as Critical/High/Medium/Low are addressed and closed.	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
			Inspected the security incident tracker to determine that all security issues are tracked/have owners assigned and closed.	
		The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the console of the Vulnerability scan report to determine that all the issues identified for Cloud infrastructure as Critical/High/Medium/Low are addressed and closed. Inspected the console of the Vulnerability scan report to determine that all the issues identified for code repository as Critical/High/Medium/Low are addressed and closed. Inspected the security incident tracker to determine that all security issues are tracked/have owners assigned and closed.	No exception noted
		The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the external VAPT reports performed during the assessment period. 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.	No exception noted
		The company utilizes a log management tool to identify events that may have a potential impact on the	Inspected the integrations section on Azure tool to determine that cloud infrastructure are successfully linked.	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
		company's ability to achieve its security objectives.	Inspected the cloud configuration settings to determine that logs are enabled for all the cloud accounts and only authorized users can access the logs Inspected the cloud storage settings to determine that logs are enabled and logs are retained at least for 365 days Inspected the cloud configuration to determine that VNets flow logs are enabled.	
		The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the Operations Security policy to determine that the Vulnerability Management and System Monitoring is documented and approved.	No exception noted
		The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the latest vulnerability assessment /penetration test report performed by a third party and determined that VA/PT are carried out periodically. Inspected sample tickets raised / minutes of management meetings to address vulnerabilities discovered in VA/PT to determine that vulnerabilities were closed.	No exception noted
CC 7.3	Security Incidents: 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.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Security and Privacy Incident response policies and procedure to determine that the same is documented and approved.	No exception noted
		The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security	Inspected the Security and Privacy Incident response policies and procedure to determine that the same is documented and approved.	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
		incident response policy and procedures.	Inspected incident tracker to determine that all incidents are tracked. Selected a sample of incident reporting emails to clients / external users to determine that major incidents are reported to clients along with root cause.	
CC 7.4	Response to security incidents: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the external VAPT report/tools to determine that all the issues identified for Cloud infrastructure as Critical/High/Medium/Low are addressed and closed. Inspected the external VAPT report to determine that all the issues identified for Code Repository as Critical/High/Medium/Low are addressed and closed. Inspected the security incident tracker to determine that all security issues are tracked/have owners assigned and closed.	No exception noted
		The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the external VAPT report to determine that all the issues identified for Cloud infrastructure as Critical/High/Medium/Low are addressed and closed. Inspected the external VAPT report to determine that all the issues identified for code repository as Critical/High/Medium/Low are addressed and closed. Inspected the security incident tracker to determine that all security issues	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
			are tracked/have owners assigned and closed.	
		The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Security and Privacy Incident response policies and procedure to determine that the same is documented and approved.	No exception noted
		The company tests their incident response plan at least annually.	Inspected the Incident Response Plan to determine has been created and approved.	No exception noted
		The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the Security and Privacy Incident response policies and procedure to determine that the same is documented and approved. Inspected incident tracker to determine that all incidents are tracked. Selected a sample of incident reporting emails to clients / external users to determine that major incidents are reported to clients along with root cause.	No exception noted
CC 7.5	Recover from Security incidents: The entity identifies, develops, and implements activities to recover from identified security incidents.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the BCP and DR plan to determine the same is documented and approved. Inspected the BCP and DR activity report to determine whether business continuity and disaster recovery plans are tested.	No exception noted
		The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Security and Privacy Incident response policies and procedure to determine that the same is documented and approved.	No exception noted
		The company tests their incident response plan at least annually.	Inspected the Incident Response Plan to determine has been created and approved.	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
		The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the Security and Privacy Incident response policies and procedure to determine that the same is documented and approved. Inspected incident tracker to determine that all incidents are tracked. Selected a sample of incident reporting emails to clients / external users to determine that major incidents are reported to clients along with root cause.	No exception noted
CC 8	**Change Management:**			
CC 8.1	Change Management: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the external VAPT report/tools to determine that all the issues identified for Cloud infrastructure as Critical/High/Medium/Low are addressed and closed. Inspected the external VAPT report to determine that all the issues identified for Code Repository as Critical/High/Medium/Low are addressed and closed. Inspected the security incident tracker to determine that all security issues are tracked/have owners assigned and closed.	No exception noted
		The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and	Inspected the Secure Development Policy to determine that the same has been created, it governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
		maintenance of information systems and related technology requirements.	and related technology requirements and is approved.	
		The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the external VAPT report to determine that all the issues identified for Cloud infrastructure as Critical/High/Medium/Low are addressed and closed. Inspected the external VAPT report to determine that all the issues identified for code repository as Critical/High/Medium/Low are addressed and closed. Inspected the security incident tracker to determine that all security issues are tracked/have owners assigned and closed.	No exception noted
		The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the Change Management Policy / SDLC policy and Procedures to determine that they define how changes to software and infrastructure components of the service should be authorized, documented, tested, reviewed, and approved prior to being implemented in the production environment. Inspected evidence that the policy is reviewed and approved during the audit period. Inspected sample change tickets to determine that approval is required to merge to the default branch for all linked version control repositories.	No exception noted
		The company restricts access to migrate changes to production to authorized personnel.	Inspected sample change tickets to determine showing recent successful production code deployments.	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
			Inspected code repository console to determine that access to merge codes and migrate changes to production are restricted to authorized personnel.	
		The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Inspected the Operations Security Policy to determine the same contains network and system hardening standards and approved. Inspected on Azure console to determine that Azure ECS services do not allow unrestricted access to TCP port 22.	No exception noted
		The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the latest vulnerability assessment /penetration test report performed by a third party and determined that VA/PT are carried out periodically. Inspected sample tickets raised / minutes of management meetings to address vulnerabilities discovered in VA/PT to determine that vulnerabilities were closed.	No exception noted
CC 9	**Risk Mitigation:**			
CC 9.1	Risk mitigation: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy to determine the same is documented and approved.	No exception noted
		The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	Inspected the policies and procedures relating to disaster recovery & Business Continuity plans to determine that a plan and procedure has been documented with clear	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
			responsibilities on those required to respond.	
		The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	Inspected cybersecurity insurance policy document to determine that cyber security insurance is obtained that covers impact of business disruptions.	No exception noted
		The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk management policy to determine the same is documented and approved. Inspected the Risk register to determine that risk assessment is performed annually.	No exception noted
CC 9.2	Risk mitigation: The entity assesses and manages risks associated with vendors and business partners.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the Third-Party Management Policy to determine the same is documented and approved. Inspected the vendor monitoring console on Azure to determine that all the vendor have been assigned with level of risks	No exception noted
		The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected sample vendor agreements including cloud provider service agreement to determine that these agreement includes confidentiality and privacy commitments applicable to the entity. Inspected the link to publicly available Privacy policy and Terms of Service to determine that the same is documented.	No exception noted
A 1	**ADDITIONAL CRITERIA FOR AVAILABILITY:**			

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
A 1.1	Processing Capacity Monitoring: The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected the Azure dashboard for processing capacity to determine that they are used for monitoring the performance of the systems and configured to log alerts. Inspected the Azure infrastructure and configuration settings to determine that load balancers	No exception noted
		The company evaluates system capacity on an ongoing basis, and system changes are implemented to help ensure that processing capacity can meet demand.	Inspected a sample of capacity monitoring reports to verify that the capacity demand is documented and reviewed by management. Inspected capacity monitoring tool console to determine that tool monitors and reports on uptime, outage and response time. Inspected the cloud console to determine whether load balancers are used.	No exception noted
A 1.2	Environmental Controls and Backup: The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the BCP and DR plan to determine the same is documented and approved. Inspected the BCP and DR activity report to determine whether business continuity and disaster recovery plans are tested.	No exception noted
		The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy to determine the same is documented and approved.	No exception noted
		The company has a multi-location strategy for production environments	Inspected the Information Security policies to determine that the Entity	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
		employed to permit the resumption of operations at other company data centers in the event of loss of a facility.	has defined system boundaries. Inspected the system diagrams and networking diagrams to determined that these are documented. Inspected multiple availability zones with cloud infrastructure.	
		The company has environmental monitoring devices in place and configured to automatically generate an alert to management for environmental incidents.	Virtually Observed the fire extinguisher/ Fire alarms/ smoke detectors/Temperature monitoring tools are installed across all office premises and are in working condition to determine that the company has environmental monitoring devices in place to detect and alert for environmental incidents.	No exception noted
		The company has maintenance inspections of environmental security measures at the company data centers performed at least annually.	Inspected environmental control check report and determined that maintenance reviews are carried out. Inspected the UPS and DG preventive maintenance reports, vendor maintenance contracts to determine that preventive maintenance is performed periodically.	No exception noted
		The company performs periodic backups for production data. Data is backed up to a different location than the production system.	Inspected the backup configuration settings in the cloud to determine that backups are enabled for production instances and recovery time is configured according to customer commitments. Inspected backup vaults to determine that backups are available as per defined frequency.	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
			Inspected configurations for backup availability zones.	
		The company's data backup policy documents requirements for backup and recovery of customer data.	Inspected the Data Management Policy to determine the same has been created and approved.	No exception noted
		The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk management policy to determine the same is documented and approved. Inspected the Risk register to determine that risk assessment is performed annually.	No exception noted
A 1.3	Business Continuity: The entity tests recovery plan procedures supporting system recovery to meet its objectives.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the BCP and DR plan to determine the same is documented and approved. Inspected the BCP and DR activity report to determine whether business continuity and disaster recovery plans are tested.	No exception noted
		The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	Inspected the policies and procedures relating to disaster recovery & Business Continuity plans to determine that a plan and procedure has been documented with clear responsibilities on those required to respond.	No exception noted
		The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the external VAPT reports performed during the assessment period. Anti-virus software has been installed on all desktops & laptops within the scope. Updates to the virus definition files	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
			are managed and downloaded by the software itself on a daily basis from the vendor website at specific intervals.	
		The company's data backup policy documents requirements for backup and recovery of customer data.	Inspected the Data Management Policy to determine the same has been created and approved.	No exception noted
C 1	**ADDITIONAL CRITERIA FOR CONFIDENTIALITY:**			
C 1.1	Data Retention: The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the Data Management Policy to determine the has been created that defines confidential data storage and security and access restrictions to authorized personnel and it is approved.	No exception noted
		The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the Data Management Policy to determine the same has been created and approved.	No exception noted
		The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected sample vendor agreements including cloud provider service agreement to determine that these agreement includes confidentiality and privacy commitments applicable to the entity. Inspected the link to publicly available Privacy policy and Terms of Service to determine that the same is documented.	No exception noted
		The company prohibits confidential or sensitive customer data, by policy, from being used or stored in non-production systems/environments.	Inspected the Data Management Policy and enquired with CISO to determine that company prohibits confidential or sensitive customer data, by policy, from being used or stored in non-production systems/environments.	No exception noted

Framework requirement	CC Description	Control Description	Test Procedure	Test Result
		The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.	Inspected the IAM settings and security groups to determine that several groups have been formed for different teams and only the production group has access to production resources. Inspected the IAM settings and security groups to determine that several groups have been formed for different teams and only the production group has access to production resources.	No exception noted
C 1.2	Data Deletion: The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	Inspected the Asset Management Policy to determine has been created and approved. Inspected the media handling policy to determine that for all media that is disposed of, data is erased from these prior to disposal or reuse. Selected a sample of media destruction certifications / shredding evidences to determine that media containing information are destroyed prior to disposal.	No exception noted

SECTION 5

OTHER INFORMATION PROVIDED BY REZOLVE.AI

Other Information Provided by Rezolve.ai

The information provided in this section is provided for informational purposes only by Rezolve.ai. 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 as opposed 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, Rezolve.ai's disaster recovery plan descriptions of control procedures are presented in this section.

In addition to the physical controls, Rezolve.ai has implemented controls to safeguard against an interruption of service, Rezolve.ai has developed several procedures that provide for the continuity of operations in the event of an extended interruption of service at its data center. In the event of an extended interruption of service, Rezolve.ai will utilize a backup maintained on the cloud.