DECIMAL POINT ANALYTICS PRIVATE LIMITED

DELIVER • PERFORMANCE • ADVANTAGE

System and Organizational Controls (SOC3)
Report on Decimal Point Analytics's Description of its Services and on the Suitability of the Design and Operating Effectiveness of its Controls Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy

For the period June 20, 2025, to June 19, 2026
Prepared pursuant to Statement on Standards for Attestation Engagements No.18

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations

KEN & Co.

Proprietary and Confidential Nature of this Report

This report provides an overview of controls related to security, availability, processing integrity, confidentiality and privacy operating at Decimal Point Analytics. It is intended for general use. For any questions regarding this report, please contact the Decimal Point Analytics representative.

Table of Contents

SECTION 1:

INDEPENDENT SERVICE AUDITOR'S REPORT

Independent Service Auditor's Report

To: Decimal Point Analytics Private Limited

Scope

We have examined Decimal Point Analytics's ('service organization' or 'Decimal Point Analytics Private Limited') accompanying assertion titled "Assertion of Decimal Point Analytics's Management" that the controls within Decimal Point Analytics's services, were effective throughout the period June 20, 2025 to June 19, 2026, to provide reasonable assurance that Decimal Point Analytics's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy (AICPA, Trust Services Criteria).*

Decimal Point Analytics uses certain subservice organizations for implementing a portion of its services (*Refer to Subservice Organizations referred in Section 3: "Decimal Point Analytics's Description of its services"*). The description indicates that complementary subservice organization controls are necessary, along with controls at Decimal Point Analytics, to achieve Decimal Point Analytics's service commitments and system requirements based on the applicable trust services criteria. The description presents Decimal Point Analytics's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Decimal Point Analytics's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design and operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

The management of Decimal Point Analytics is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Decimal Point Analytics's service commitments and system requirements are achieved. Management of Decimal Point Analytics has provided the accompanying assertion titled "Assertion of Decimal Point Analytics's Management" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period June 20, 2025, to June 19, 2026, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Decimal Point Analytics's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective in achieving Decimal Point Analytics's service commitments and system requirements based on the applicable trust services criteria.

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

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. The projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

As AI technologies are inherently probabilistic and context-sensitive, there is a risk of misinterpretation, inaccuracies, or possible incorrect outputs. Additionally, the system may process personal or sensitive information, which could be subject to privacy, legal, or ethical considerations. As a part of the engagement, we have not evaluated the accuracy or reliability of AI-generated transcriptions or summaries, nor the appropriateness of data handling in all scenarios. Accordingly, the effectiveness of these AI components is restrictive and falls outside the scope of the assurance provided in this report.

Opinion

In our opinion, management's assertion that the controls within Decimal Point Analytics's system were effective throughout the period June 20, 2025 to June 19, 2026, to provide reasonable assurance that Decimal Point Analytics's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if subservice organization controls assumed in the design of Decimal Point Analytics's controls operated effectively throughout the period June 20, 2025 to June 19, 2026.

KEN & Co. CPA LLC

CPA FIRM KEN & CO. CPA LLC MONTANA, USA

KEN & Co. CPA LLC

CPA Firm License Number: PAC-FIRM-LIC-47392

Montana, USA

July 20, 2026

SECTION 2:

ASSERTION OF DECIMAL POINT ANALYTICS'S MANAGEMENT

Assertion of Decimal Point Analytics's Management

July 16, 2026

We are responsible for designing, implementing, operating and maintaining effective controls within Decimal Point Analytics's ('service organization' or 'Decimal Point Analytics Private Limited') system throughout the period June 20, 2025 to June 19, 2026, to provide reasonable assurance that Decimal Point Analytics's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy (applicable trust services criteria). Our description of the boundaries of the system is presented in Section 3 and identifies the aspects of the system covered by our assertion.

Decimal Point Analytics uses certain subservice organizations for implementing a portion of its services (Refer Subservice Organizations in Section -3 "Decimal Point Analytics's Description of its services"). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Decimal Point Analytics, to achieve Decimal Point Analytics's service commitments and system requirements based on the applicable trust services criteria. The description presents Decimal Point Analytics's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Decimal Point Analytics's controls. The description does not disclose the actual controls at the subservice organization.

There are inherent limitations in any system of internal controls, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period June 20, 2025 to June 19, 2026, to provide reasonable assurance that Decimal Point Analytics's service commitments and system requirements were achieved based on the applicable trust services criteria.

Shailesh Dhuri

Chief Executive Officer

Decimal Point Analytics Private Limited

SECTION 3:

DECIMAL POINT ANALYTICS'S DESCRIPTION OF ITS SERVICES

I. OVERVIEW OF OPERATIONS AND DESCRIPTION OF SERVICES PROVIDED

A. Company Background

Decimal Point Analytics was established in 2003 to provide technology-enabled data analytics and financial research solutions. The Company is registered in Mumbai, India. Operational delivery centers are strategically located across Mumbai, Nashik, and GIFT City (Gandhinagar), enabling efficient execution and scalability of services.

B. Description of Services Provided

Decimal Point Analytics delivers an integrated suite of data analytics, automation, and financial research services that generate actionable insights and enhance operational efficiencies. Below services are offered in conjunction and support of business partner solutions.

The following table outlines the in-scope services provided by Decimal Point Analytics:

Service / Feature	What it is / does
Data analytics	Analyzes structured and unstructured data to identify trends, generate insights, and support informed business decision-making.
Automation	Automates repetitive business processes and workflows to improve efficiency, accuracy, and productivity while reducing manual effort.
Data science	Applies statistical analysis, machine learning, and predictive modelling to extract insights, forecast outcomes, and solve complex business problems.
Data solutions, Visualization and BI dashboards	Develops data integration solutions and interactive dashboards that transform data into visual reports for real-time monitoring and business intelligence.
Strategic Financial Advisory & Intelligence	Provides financial analysis, planning, forecasting, and strategic insights to support business growth, investment decisions, and performance optimization.
Investment Strategy & Portfolio Optimization	Assists in designing investment strategies, assessing risk, and optimizing portfolios to maximize returns while aligning with financial objectives.
Reg Tech & Compliance Management	Delivers technology-enabled solutions to help organizations manage regulatory compliance, monitor risks, automate compliance activities, and maintain governance requirements.

II. COMPONENTS OF THE SYSTEM

A. System Boundaries

The boundaries of Decimal Point Analytics's system are the specific aspects of the Company's infrastructure, software, people, data and procedures that are necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of Decimal Point Analytics's system.

B. Infrastructure

Decimal Point Analytics provides services wherein the infrastructure, environments, and software deployments are predominantly managed and maintained by the clients. The clients provide computing resources (cloud, on-premises, or hybrid), install necessary software components, and control configuration and operational management.

The company's personnel access the client's environment through secure, client-managed access channels (such as VPN or virtual desktops). All critical system components including servers, databases, and analytic tools are deployed, patched, and maintained under the client's administrative domain. As a result, the company does not host or control the primary production environment or its underlying infrastructure.

The primary infrastructure used to provide Decimal Point Analytics's services includes the following:

Infrastructure Components	Platform	Business Function Description
Cloud Services	Oracle	Primary compute, storage, and networking resources.
Application Services	Microsoft Azure	Web applications, Intune and Azure OpenAI APIs.
Database Servers	MySQL (Oracle),	Managed, high-availability database service with flexible scaling.
Network Infrastructure	Oracle	Global load balance, content delivery, web application firewall, and domain name resolution.
Identity Infrastructure	Microsoft	Authentication services and directory management.
CI/CD Pipeline	Jenkins	Open-source automation server used for continuous integration (CI) and continuous delivery (CD) in software development
Code Repository	Bitbucket	Source code repository

C. Software

Primary software used to provide Decimal Point Analytics's services includes the following:

Primary Software

Software	Platform	Purpose
Salesforce CRM	Web-Based (SaaS)	Centralized customer relationship management and sales tracking.
Click Up	Web-Based (SaaS)	Project and task management, Incident management and ticket tracking.
BitLocker	Application (On Prem)	HDD/SSD encryption and BitLocker key management.
Power BI and Tableau	Application (On Prem)	Data visualization and dashboarding.
Zabbix	Web-Based (SaaS)	Monitoring and real-time alerts.
Up Guard	Web-Based (SaaS)	Security posture monitoring and Third-party Risk Management (Passive Scanning).
CrowdStrike XDR	Application (On Prem)	Extensive Defence Response.
Wazuh	Web-Based (SaaS)	Security Orchestration/SIEM.
Crowdstrike DLP	Application (On Prem)	Advanced Data Loss Prevention tool.

D. People

The company employs dedicated team members to handle major product functions, including operations, and support. The IT Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the company and its data secure.

Organizational charts are in place to communicate key areas of authority and responsibility. Decimal Point Analytics has staff organized in the following functional areas:

- **Chief Executive Officer -** Provides strategic directions to the organization, approves key business and information security initiatives, ensures adequate resources are available, and oversees organizational governance and compliance. Additionally responsible for privacy matters
- **Managing Partner-** Oversees business operations, client relationships, and strategic initiatives. Ensures organizational objectives, regulatory requirements, and information security expectations are achieved.
- **President-** Manages day-to-day business operations, oversees departmental performance, ensures implementation of management decisions, and monitors operational risks.
- **Executive Vice President-** Leads multiple business functions, supports strategic planning, oversees major projects, and ensures organizational policies and controls are effectively implemented.

- **Senior Vice President-** Oversees departmental operations, manages senior management teams, ensures compliance with organizational policies, and monitors operational and security performance.
- **Vice President-** Manages specific business units or functional departments, oversees project delivery, approves operational activities, and ensures compliance with company policies.
- **Assistant Vice President-** Supports the Vice President in managing daily operations, supervises teams, monitors performance, and assists with implementation of organizational initiatives and controls.
- **Senior Manager-** Leads operational teams, manage resources, reviews work quality, ensures adherence to established procedures, and escalates significant risks or issues.
- **Manager-** Supervises day-to-day team activities, allocates work, reviews deliverables, monitors performance, and ensures compliance with company policies and procedures.
- **Consultant-** Delivers client services, performs assigned project activities, protects confidential information, complies with organizational policies, and reports operational or security concerns promptly.

New Hire Procedures

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

Employees are required to sign confidentiality agreement. Background and reference checks are completed for prospective employees.

Employee Terminations

Termination or change in employment is processed as per Decimal Point Analytics's HR-related procedures. There are clearly identified and assigned responsibilities about termination or change in employment.

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

Code of Conduct and Disciplinary Action

Decimal Point Analytics has put forward the Code of Conduct and Disciplinary Process to encourage and maintain standards of conduct and ensure consistent and fair treatment for all. Decimal Point Analytics's employees, whose conduct does not comply with an element of the code of conduct and have been found to have breached the code, are dealt with as per defined process.

E. Data

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements, if any. Customer data is captured which is utilized by the company in delivering its services. Production data is hosted on OCI in the India- Mumbai region.

Data pertaining to the configuration of systems, logs of the network, and access to the IT resources are tracked and monitored. All personnel and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, Decimal Point Analytics has established policies and procedures to ensure the proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

The organization does not maintain a customer service business unit. Employees do not request or collect personal information directly from clients as part of customer support, troubleshooting, or related service activities.

F. Processes, Policies and Procedures

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by management, the executive team, and control owners. These procedures cover the following key security life cycle areas. Below is the list of policies and procedures

S. No	Policy Name
1.	Information Security Policy
2.	CCTV Monitoring Policy
3.	Admin Policy
4.	Fire Safety Policy
5.	Privacy Policy
6.	Code of Conduct Policy
7.	Attendance and Leave Policy
8.	Whitelisting Policy
9.	Communication Policy
10.	Asset Classification and Handling policy
11.	Electronic Media and Computing Devices Disposal Policy
12.	Network Security Policy
13.	Patch Management Policy

S. No	Policy Name
20.	Recruitment Onboarding Policy
21.	Separation Policy
22.	Performance Management Policy
23.	People Development Initiatives Policy
24.	Workplace Integrity and Safety Policy
25.	Conflict of Interest Policy
26.	Fraud Detection and Prevention Policy
27.	Agreement with Clients Policy
28.	Access Control Logical Policy
29.	Internet Policy
30.	Malicious Code Policy
31.	Mobile Computing Devices and Handling Policy
32.	Password Policy

S. No	Policy Name
14.	Backup Policy
15.	Email Policy
16.	Acceptable Usage Policy
17.	Change Management policy
18.	Incident Management Policy
19.	Business Continuity Plan policy

S. No	Policy Name
33.	Security Monitoring Policy
34.	Server Security Policy
35.	Software Security Policy
36.	Supplier Relationship policy
37.	Internal Audit policy
38.	Log Management policy

Logical Access

Decimal Point Analytics provides employees and contractors access to infrastructure via a role-based access control system, to ensure uniform, least privileged access to identified users and to maintain simple and repeatable user provisioning and deprovisioning processes. Access to these systems is split into admin roles, user roles, and users without assigned roles have no system access. User access and roles are reviewed on an annual basis to ensure least privileged access.

IT team is responsible for granting access to systems based on the employee's role, following completion of an HR-conducted background check. The employee is responsible for acknowledging Decimal Point Analytics's policies and completing security training. When an employee is terminated, IT team is responsible for deprovisioning access to all in-scope systems as the access control policy.

Computer Operations – Backups

Customer data is backed up and monitored by the IT Team for completion and exceptions. If there is an exception, IT Team will perform troubleshooting to identify the root cause and either rerun the backup or as part of the next scheduled backup job.

Backup infrastructure is maintained in OCI with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

Computer Operations – Monitoring

Decimal Point Analytics maintains an incident response plan to guide employees on reporting and responding to any information security or data privacy events or incidents. Procedures are in place for identifying, reporting and acting upon breaches or other incidents.

Decimal Point Analytics internally monitors all applications, including the web UI, databases, and cloud storage to ensure that service delivery matches SLA requirements.

Change Control

Decimal Point Analytics maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation

requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Development and testing are performed in an environment that is logically separated from the production environment. IT Team head approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

III. RELEVANT ASPECTS OF INTERNAL CONTROL

A. Control Environment

The control environment at Decimal Point Analytics is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel.

The components of the control environment factors include integrity and ethical values, management's commitment to competence; its organizational structure; the assignment of authority and responsibility;

and the oversight and direction provided by the board of directors and operations management.

The company's management style fosters open communication among all personnel. The executive management and senior leadership are committed to reinforcing the core values for all personnel. Management has documented information security policies, which are communicated to all company personnel. Roles and responsibilities relevant to Decimal Point Analytics's control environment are documented.

B. Risk Assessment Process

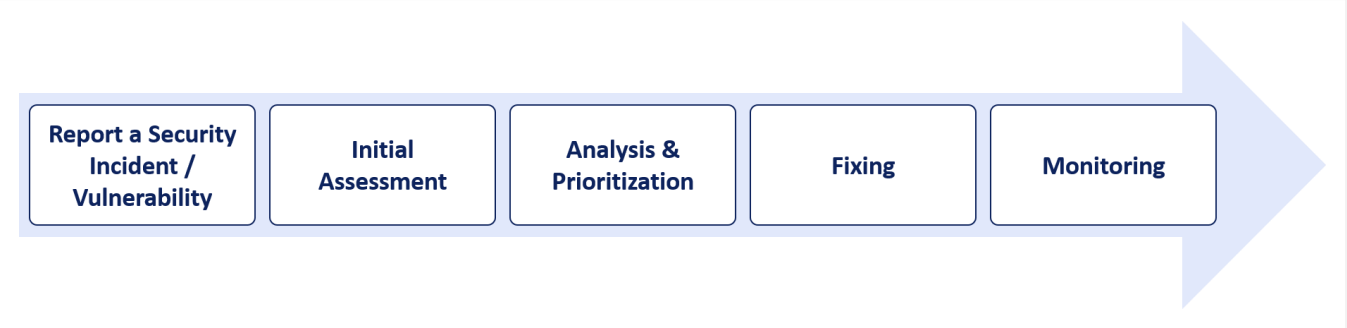
Decimal Point Analytics's risk assessment process identifies and manages risks that could potentially affect Decimal Point Analytics's ability to provide reliable and secure services to the customers. As part of this process, Decimal Point Analytics maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is evaluated annually, and tasks are incorporated into the regular improvement process so they can be dealt with predictably and iteratively.

Integration with Risk Assessment

As part of the design and operation of the system, Decimal Point Analytics identifies the specific risks that service commitments may not be met and designs the necessary control to address those risks. Decimal Point Analytics's management performs an annual risk assessment exercise to identify and evaluate internal and external risks to the company, as well as their potential impacts, likelihood, severity, and mitigating action.

Vulnerability Assessment and Penetration Testing

VAPT is conducted on Decimal Point Analytics's environment for in-house products internally to maintain confidentiality. Decimal Point Analytics remediates those vulnerabilities based on the recommendations. Vulnerabilities are classified as critical, high, or medium risk and tracked to remediation.



Information and Communications Systems

Information and communication are an integral component of Decimal Point Analytics's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

Decimal Point Analytics uses several information and communication channels internally to share information with management, employees, contractors, and customers. Decimal Point Analytics uses chat systems and email as the primary internal and external communications channels.

C. Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Decimal Point Analytics's management performs monitoring activities to continuously assess the quality of internal control over time. Employee activity and adherence to company policies and procedures are also monitored.

On-Going Monitoring

Decimal Point Analytics's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

IT Team evaluates the facts and circumstances related to any suspected control breakdown. Members of the IT Team respond to security issues. A decision to address any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel.

Reporting Deficiencies

Internal risk management tracking tools are utilized to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy

documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked

IV. COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOCs)

Decimal Point Analytics utilizes certain service organizations ("subservice organizations") to implement portions of its system. The controls implemented by Decimal Point Analytics cover only a portion of the overall internal control necessary to achieve the applicable trust services criteria. Accordingly, the achievement of those criteria depends, in part, on the design and operating effectiveness of complementary subservice organization controls (CSOCs) expected to be implemented by these subservice organizations.

Therefore, user entities should consider Decimal Point Analytics's controls described in this report in conjunction with the complementary subservice organization controls described below when evaluating the effectiveness of controls relevant to the system.

S.No	Applicable Trust Services Criteria	CSOCs
1	CC3.2, CC3.3	Procedures are established and implemented to identify, analyse, and remediate potential security, availability, and confidentiality threats and or risks
2	CC4.1, CC4.2	Procedures are established and implemented to evaluate the designs and operating effectiveness of controls as they relate to security, availability and / or confidentiality commitments, as well as to identify and track to resolve the corrective actions for control deficiencies.
3	CC6.1	Physical and Logical security has been implemented to authenticate authorized users, restrict access, prevent, and detect unauthorized access.
4	CC6.2	The systems are configured to identify and authenticate internal and external users with appropriate valid credentials.
5	CC6.1	Security measures are implemented to prevent unauthorized disclosure, usage, and/or access to confidential information.
6	CC6.2	Procedures are implemented to provision and de-provision user access to systems and applications based on appropriate authorization.
7	CC6.3	Logical access to the software and physical access to the software hosting datacentre facilities are provisioned to authorized personnel and revoked upon termination or when access is no longer needed.
8	CC6.4, CC6.5	Physical access to the datacenter facilities is restricted to authorized personnel.
9	CC6.6	Physical and Logical security measures have been implemented to protect and detect external threats.
10	CC6.7	Physical and Logical security measures have been implemented to secure the transmission, movement, and removal of information, as well as restricting with the ability to do so.

S.No	Applicable Trust Services Criteria	CSOCs
11	CC6.8	Antivirus and/or malware software have been implemented to prevent or detect the introduction of unauthorized or malicious software.
12	CC7.2	Vulnerability scans and penetration testing are performed periodically to identify vulnerabilities threatening the systems.
13	CC7.3, 7.4, 7.5	Incident Response Procedures are established and implemented to identify, analyse, and remediate potential security, availability, and confidentiality events and/or incidents.
14	CC8.1	Procedures are implemented to identify deficiencies in the system and to ensure secured change management procedures are tracked and monitored.
15	CC8.1	Software development lifecycle (“SDLC”) has been established and implemented to ensure system changes are authorized, tested, and approved prior to production deployment.
16	CC8.1	Policies and procedures for SDLC or infrastructure changes have been established and reviewed and are updated periodically.
17	CC8.1	Procedures are established and implemented to ensure changes to systems are authorized, designed, developed, configured, documented, tested, and approved prior to production deployment.
18	CC8.1	Procedures are implemented to ensure confidential information is protected during systems change management processes.
19	CC9.2	Confidential information is only obtained in accordance with the defined commitments or agreements.
20	A1.1	Monitoring tools are implemented to monitor and manage the system capacity and availability
21	A1.2	Environmental protections, data backup processes, recovery infrastructure, and monitoring and alarming mechanisms have been implemented to adequately address availability requirements.
22	A1.3	Business continuity/disaster recovery procedures are tested periodically.

Decimal Point Analytics’s management, along with the subservice provider, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements.

In addition, Decimal Point Analytics performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing attestation reports over the services provided by vendors and subservice organization(s).
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization.

V. COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

Decimal Point Analytics's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to Decimal Point Analytics's services to be solely achieved by Decimal Point Analytics control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Decimal Point Analytics's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

S.No	Applicable Trust Services Criteria	CUECs
1	Common Criteria 2.2, 2.3, 6.1. Availability Criteria 1.2	User entities are responsible for understanding and complying with their contractual obligations to organization.
2	Common Criteria 6.1 Availability Criteria 1.2	User entities are responsible for notifying organization of changes made to technical or administrative contact information.
3	Common Criteria 2.2, 2.3	User entities are responsible for maintaining their own systems of record.
4	Common Criteria 6.1, 6.6	User entities are responsible for ensuring the supervision, management, and control of the use of organization services by their personnel.
5	Availability Criteria 1.2, 1.3, Common Criteria 3.1, 5.1 5.2 ,5.3, 7.5	User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize organization services.
6	Common Criteria 8.1	User entities are responsible for providing organization with a list of approvers for security and system configuration changes for data transmission.
7	Common Criteria 7.3, 7.4, 7.5	User entities are responsible for immediately notifying organization of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers
8	Privacy Criteria 2.0, 3.0	User entities are responsible for obtaining the consent from the end user about usage and processing of personal information and such other controls defined in the "Privacy" criterion in the Trust Services Categories.

S.No	Applicable Trust Services Criteria	CUECs
9	Confidentiality Criteria 1.1, 1.2, Common Criteria 6.1	User entities are responsible for configuring the message retention settings appropriately for the organization.
10	Common Criteria 6.1,6.3,6.6	User entities are responsible for ensuring the appropriateness of designated organization workspace owner(s) and administrator(s).
11	Common Criteria 6.1,6.3,6.6	User entities are responsible for ensuring that entity profile information stored by the System is accurate and complete.
12	Privacy Criteria 2.0,3.0	User Entities are responsible for customer service employees to follow when confirming the identity of the customer and obtaining access to customer data for processing the customer request or debugging
13	Privacy Criteria 2.0,3.0	User Entities are responsible to give their explicit consent to the Privacy Policy and the Terms of User prior to subscribing to the services.
14	Privacy Criteria 2.0,3.0	Access restrictions are in place to ensure only respective user entities have access to their data.

SECTION 4:

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

VI. PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Decimal Point Analytics designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Decimal Point Analytics makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Decimal Point Analytics has established for the services. The system services are subject to the Security commitments established internally for its services.

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

- System features and configuration settings are designed to authorize user access while restricting unauthorized users from accessing information not needed for their role.
- Operational procedures for managing security incidents and breaches, including notification procedures.
- Use of encryption technologies to protect customer data both at rest and in transit.

<<End of report>>