



BlockSurvey Inc

SOC 2 TYPE II Report

For The Period,
June 01, 2024 to May 31, 2025

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



Prepared by: **Accorp Partners**

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

SECTION 2

MANAGEMENT ASSERTION

SECTION 3

DESCRIPTION OF SYSTEM

Background and Overview of Services

Principal Service Commitments and System Requirements

SECTION 4

DESCRIPTION OF TEST OF CONTROLS AND THEREOF

SECTION 5

OTHER INFORMATION PROVIDED BY BLOCKSURVEY

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

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

To: Management of BlockSurvey Inc (BlockSurvey)

Scope

We have examined BlockSurvey Inc's accompanying description of its BlockSurvey system found in Description of System, Section 3 titled "Empower Business to collect data through forms and Surveys in secure manner as SaaS for their clients" throughout the period June 01, 2024 to May 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) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period June 01, 2024 to May 31, 2025, to provide reasonable assurance that BlockSurvey's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability and 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.

BlockSurvey uses Render and Google Cloud Platform as a subservice organization for data center services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at BlockSurvey, to achieve BlockSurvey's service commitments and system requirements based on the applicable trust services criteria. The description presents BlockSurvey's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of BlockSurvey's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The Description also indicates that BlockSurvey's controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of BlockSurvey'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.

Service Organization's Responsibilities

BlockSurvey 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 BlockSurvey's service commitments and system requirements were achieved. In Management Assertion, Section 2, BlockSurvey has provided the accompanying assertion titled "Assertion of the Management of BlockSurvey Inc" about the description and the suitability of design and operating effectiveness of controls stated therein. BlockSurvey is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

- obtaining an understanding of the system and the service organization's service commitments and system requirements.
- assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- evaluating the overall presentation of the description.

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

Inherent Limitations

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

Description of Test of Controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in section 4 of our report titled "Independent Service Auditors' Description of Test of Controls and Results".

Opinion

In our opinion, in all material respects -

- a. the description presents BlockSurvey's system that was designed and implemented throughout the period June 01, 2024 to May 31, 2025 in accordance with the description criteria.
- b. the controls stated in the description were suitably designed throughout the period June 01, 2024 to May 31, 2025 to provide reasonable assurance that BlockSurvey's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization applied the complementary controls assumed in the design of BlockSurvey's controls throughout that period.
- c. the controls stated in the description operated effectively throughout the period June 01, 2024 to May 31, 2025 to provide reasonable assurance that BlockSurvey's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of BlockSurvey's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in section 4 of this report, is intended solely for the information and use of BlockSurvey; user entities of BlockSurvey's system during some or all of the period June 01, 2024 to May 31, 2025, business partners of BlockSurvey subject to risks arising from interactions with the BlockSurvey system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

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

Accorp Partners CPA LLC
License No.: PAC-FIRM-LIC-47383
Kalispell, Montana

SECTION 2

MANAGEMENT ASSERTION

Assertion of the Management of BlockSurvey Inc

We have prepared the accompanying description of BlockSurvey Inc's (BlockSurvey) system titled Empower Business to collect data through forms and Surveys in secure manner as SaaS for their clients throughout the period June 01, 2024 to May 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). The description is intended to provide report users with information about the BlockSurvey system that may be useful when assessing the risks arising from interactions with BlockSurvey's system, particularly information about system controls that BlockSurvey 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 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*.

BlockSurvey uses Render and Google Cloud Platform as a subservice organization for data center services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at BlockSurvey, to achieve BlockSurvey's service commitments and system requirements based on the applicable trust services criteria. The description presents BlockSurvey's, controls the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of BlockSurvey's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at BlockSurvey, to achieve BlockSurvey's service commitments and system requirements based on the applicable trust services criteria. The description presents the service organization's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the service organization's controls.

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

1. The description presents BlockSurvey system that was designed and implemented throughout the period June 01, 2024 to May 31, 2025 in accordance with the description criteria.
2. The controls stated in the description were suitably designed throughout the period June 01, 2024 to May 31, 2025 to provide reasonable assurance that BlockSurvey's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of BlockSurvey's controls throughout that period.
3. The controls stated in the description operated effectively throughout the period June 01, 2024 to May 31, 2025 to provide reasonable assurance that BlockSurvey's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of BlockSurvey's controls operated effectively throughout that period.

Sincerely,

Wilson Bright John

Wilson Bright John
CEO

SECTION 3

DESCRIPTION OF SYSTEM

Background and Overview of Services

Background and Overview of Services

BlockSurvey enables businesses and individuals to create no-code online forms and surveys and collect data based on anonymity.

Significant Changes during the Review Period

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

Subservice Organizations

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

Render (Render)

Render has provided an Independent Service Auditors Report (SOC2).

The Criteria that relate to controls at the subservice organizations included all criteria related to the Trust Service Principles of Security, Confidentiality, and Availability. The types of controls that are necessary to meet the applicable trust services criteria, either alone or in combination with controls at BlockSurvey include:

- The system is protected against unauthorized logical access
- The system is available for operation and use and in the capacities as committed or agreed.
- Policies and procedures exist related to security and availability and are implemented and followed.

Google Cloud Platform (GCP)

GCP has provided an Independent Service Auditors Report (SOC2).

The Criteria that relate to controls at the subservice organizations included all criteria related to the Trust Service Principles of Security, Confidentiality, and Availability. The types of controls that are necessary to meet the applicable trust services criteria, either alone or in combination with controls at BlockSurvey include:

- The system is protected against unauthorized logical access
- The system is available for operation and use and in the capacities as committed or agreed.
- Policies and procedures exist related to security and availability and are implemented and followed.

GCP is used for hosting database services i.e Firebase within the BlockSurvey environment.

Principal Service Commitments and System Requirements

BlockSurvey designs its processes and procedures related to the System to meet its objectives. Those objectives are based on the service commitments, related laws and regulations of products and services, and financial, operational, and other compliance requirements that have been established for such services. Security commitments to user entities are documented and communicated in customer agreements, as well as in the description of the service offering provided online. BlockSurvey establishes operational requirements that

support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in BlockSurvey's system policies and procedures, system design documentation, and contracts with customers.

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

Specific security, availability, and confidentiality commitments include the following:

- Maintain technical and organizational measures, internal controls, and data security routines to protect customer data.
- Protection of data at rest and in transit.
- Protection of information systems from unauthorized access, use, modification, disclosure, destruction, threats, or hazards.
- Continuous communication of the BlockSurvey platform service availability.
- Ability to recover and restore customer data in the event of a business disruption or disaster.
- Maintain customer data as confidential and not disclose information to any unauthorized party.
- Customer data is removed from BlockSurvey systems upon customer request or as per the agreed terms in the contract.

BlockSurvey has also established system requirements that support the achievement of the principal service commitments relevant to the security, availability, and confidentiality trust services categories and relevant laws and regulations. These requirements are communicated internally via the information security policies and procedures and regular security awareness training documentation, and externally via the BlockSurvey public-facing website.

These requirements include, but are not limited to, defined processes around the following:

- Employees undergo background checks as per the requirements
- Employees undergo mandatory security awareness training upon hire, and annually thereafter.
- Roles and responsibilities for BlockSurvey employees who have access to confidential data and the responsibility for protecting the information and information systems.
- Access control policies for employees with access to BlockSurvey's production environment and source code such that access levels are approved prior to credentials being issued, reviewed at predefined intervals, and based on legitimate business need based on the principle of least privilege.
- Software development lifecycle (SDLC) policies for any changes to the production environment to ensure that key processes and security checks are consistently performed from change initiation through release.
- Risk assessment practices to assist in identifying and managing potential internal or external risks that could negatively affect BlockSurvey's critical business processes and their ability to provide reliable services to their customers.
- Incident management process to address data breaches and security events related to BlockSurvey's products and services in an efficient and timely manner.
- Disaster recovery and business continuity plans to prepare BlockSurvey in the event of extended service outages caused by factors beyond their control and to restore services to the widest extent possible in a minimal timeframe.

Components of the System

The System is comprised of the following components:

- Infrastructure including the Information Technology (IT), and other hardware.
- Software including application programs and IT system software that support application programs.
- People including executives, sales and marketing, client services, product support, information processing, software development, IT, Finance, and Human resources.
- Procedures (automated and manual).

- Data including transaction streams, files, databases, tables, and output used or processed by the system.

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

Boundaries of the System

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

Products and Services in Scope
Products • BlockSurvey
Geographic Locations in Scope
No physical offices and related physical and availability specific controls are included since BlockSurvey does not have any physical office locations/physical servers and all data is processed on cloud services.

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

Control Environment

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

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

Integrity and Ethical Values

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

Management's Philosophy and Operating Style

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

Risk Management and Risk Assessment

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

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

The following steps are involved in performing risk assessments

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

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

Monitoring

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

Information and Communication

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

Electronic Mail (e-Mail)

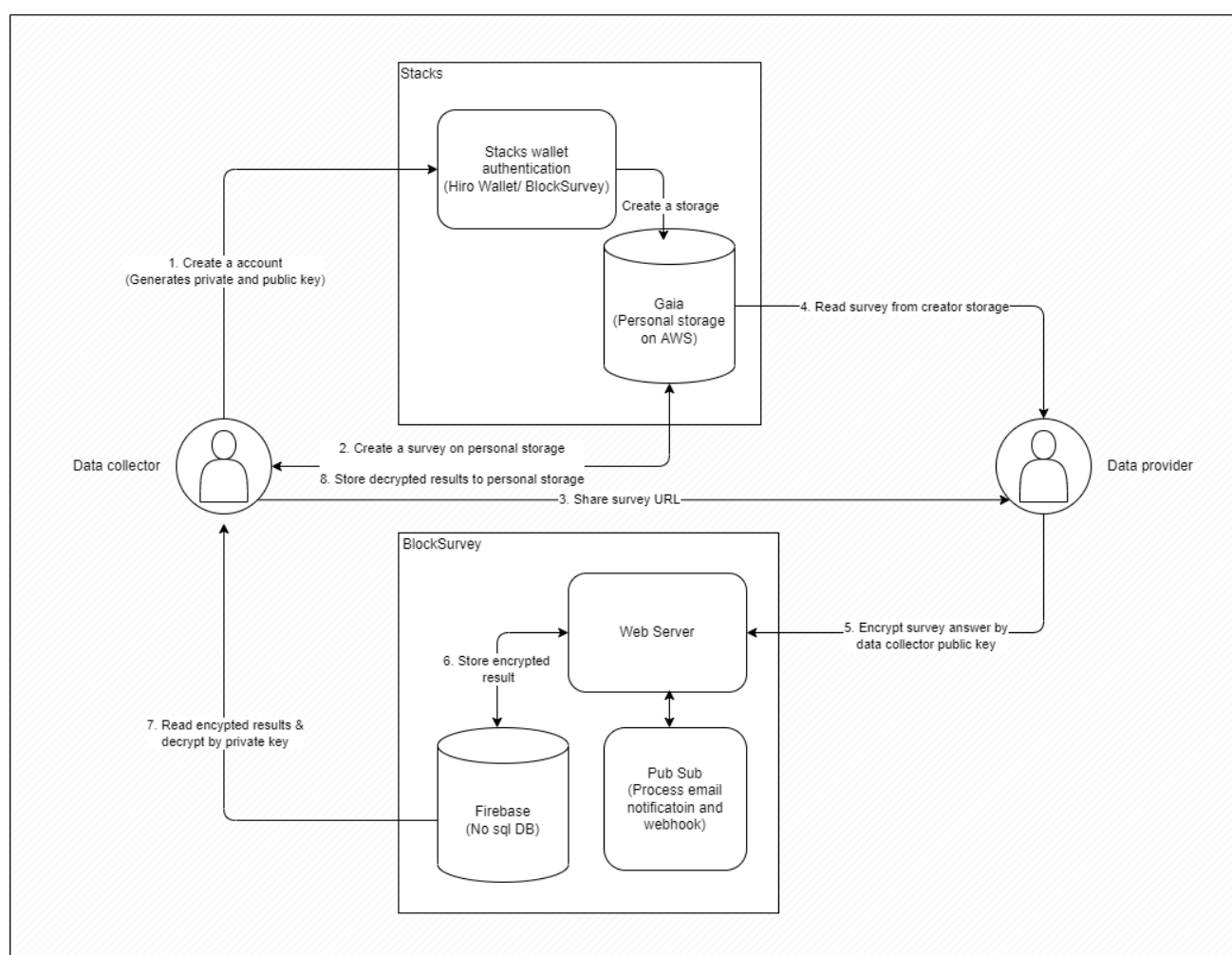
Communication to Customer organizations and project teams is through e-mail. Important corporate events, employee news, and cultural updates are some of the messages communicated using e-mail. E-mail is also a means to draw the attention of employees towards adherence to specific procedural requirements.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

Components of the System

Network Segmentation Overview

BlockSurvey's network is equipped with the latest software, and networking infrastructure.

BlockSurvey Architecture



Software

Firewalls

The production system at Render is protected by security group rules (virtual firewall) set up for the virtual private cloud (VPC) provided by Render. VPC is used to protect all Production systems hosted at Render. Any change to configuration is overseen by the IT Security team. All configurations, backups, and rules have been documented for compliance.

Network & Endpoint Protection

All systems and devices are protected by the comprehensive endpoint protection system. The endpoints include antivirus, anti-malware, and Trojan protection from any source. This also includes the e-mail scanning of the systems which prevents malicious scripts and viruses from the e-mails. Apart from this, all systems are restricted to the internet with the content filtering system routed through the proxy server.

Monitoring

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. BlockSurvey's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures are also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

BlockSurvey'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.

Management's close involvement in BlockSurvey's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of BlockSurvey's personnel.

Capacity Management

Capacity management controls are put in place so as to monitor, tune and project certain BlockSurvey's resources to ensure system performance meets the expected service levels and minimize the risk of systems failure and capacity-related issues. The addition of new information systems and facilities, upgrades, new versions, and changes are subject to formal system analysis, testing, and approval prior to acceptance.

Patch Management

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

Vulnerability Scans & Security Audits

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

Virus Scans and Endpoint Security

BlockSurvey ensures antivirus is installed with the feature of scanning the device automatically in all the systems and log reports are reviewed by the IT Head. Updates to the virus definition files are managed and downloaded by the software itself on a daily basis from the vendor website at specific intervals.

People

Organizational Structure

The organizational structure provides the overall framework for planning, directing, and controlling operations. It has segregated personnel and business functions into functional groups according to their job responsibilities. This approach helps to enable the organization to define responsibilities, lines of reporting, and communication and helps facilitate employees to focus on the specific business issues impacting clients.

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

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

BlockSurvey has employees organized into the following functional areas:

- **Executive management** - Responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
- **Human resources (HR)** - Responsible for HR policies, practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisitions, employee retention, compensation, employee benefits, performance management, employee relations and training, and development).
- **IT and DevOps** - Responsible for installation, configuration, operation, monitoring, and maintenance of IT and DevOps.
- **IT Security** – Responsible for Information Security including implementing, managing, and monitoring the information security program along with IT Risk Management.
- **Development** - Responsible for the development, testing, deployment, and maintenance of code for internally developed applications

Processes and Procedures

Formal IT policies and procedures exist that describe logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the BlockSurvey policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any BlockSurvey team member.

Administrative Level Access

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

Confidentiality

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

BlockSurvey does not store or persist API keys or access tokens on its servers. All key handling is performed client-side, and the platform is designed under a zero-knowledge architecture that prevents access to decrypted credentials or personal data.

Backup and Recovery of Data

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

Applicable Trust Services Criteria and related Controls

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

BlockSurvey has identified that following criteria are not included in the system description since BlockSurvey does not have an office and Render is responsible for implementing controls that ensure the data center facilities equipped with physical and environmental security safeguards.

CC6.4 - *The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.*

A1.2 - *The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.*

Complimentary User-Entity Control Considerations

The following complimentary 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.

1. User entities are responsible for understanding and complying with their contractual obligations to BlockSurvey.
2. User entities are responsible for notifying BlockSurvey of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of BlockSurvey services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize BlockSurvey services.
6. User entities are responsible for providing BlockSurvey with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying BlockSurvey of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

SECTION 4

DESCRIPTION OF TEST OF CONTROLS AND THEREOF

Trust Services Security, Confidentiality and Availability, Criteria & Related Controls and Test of effectiveness and Results of Test

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
Control Environment			
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.		
CC1.1.1	Terms of employment and ethical and behavioral values and expectations are communicated via employment contracts and the code of conduct.	Inspected the code of conduct and an example employment contract to determine that terms of employment and BlockSurvey's ethical and behavioral values and expectations were communicated via employment contracts and the code of conduct.	No Exceptions Noted
CC1.1.2	Mandatory security awareness training includes security requirements and expectations of employees in achieving internal control responsibilities to meet business and regulatory objectives.	Inspected the security and privacy awareness training material to determine that mandatory security awareness training included security requirements and expectations of BlockSurvey employees in achieving internal control responsibilities to meet business and regulatory objectives.	No Exceptions Noted
CC1.1.3	Employees receive code of conduct training on at least an annual basis to ensure that employees acknowledge the policies that comprise the code of conduct and the importance of the code of conduct to BlockSurvey's business practices.	Inspected the code of conduct training material and results for a sample of current employees to determine that training was completed during the period for each employee sampled to ensure that employees acknowledged the policies that comprised the code of conduct and the importance of the code of conduct to BlockSurvey's business practices.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC1.1.4	Employees receive security and privacy awareness education and refresher training at least on an annual basis.	Inspected the security and privacy awareness education and refresher training results for a sample of current employees to determine that security and privacy awareness education and training was completed during the period for each employee sampled.	No Exceptions Noted
CC1.1.5	Employees receive security and privacy awareness education and training upon hire.	Inspected the security and privacy awareness training results for a sample of employees hired during the period to determine that security and privacy awareness education and training was completed upon hire for each employee sampled.	No Exceptions Noted
CC1.1.6	Employees agree to the acceptable use policy before they are granted access to BlockSurvey information assets.	Inspected the signed IT acceptable use policy for a sample of employees hired during the period to determine that each employee sampled agreed to the IT acceptable use before they were granted access to BlockSurvey information assets.	No Exceptions Noted
CC1.1.7	All new employees have to read and sign the Confidentiality Agreement/NDA upon joining.	Selected a sample of new joiners and inspected personnel files to determine that Confidentiality agreements / NDAs are signed.	No Exceptions Noted
CC1.1.8	Agreements are established with third parties or subcontractors that include clearly defined terms, conditions, and responsibilities for third parties and subcontractors.	Selected a sample and inspected the vendor agreements to determine that the agreements define the terms, conditions, and responsibilities of these vendors and their subcontractors.	No Exceptions Noted
CC1.1.9	Customer can provide their issues, complaints, or feedback through email to Business Heads. Employees can raise their complaints and grievances to HR.	Inspected customer resolution clauses in a sample of customer Statement of Work (SOW) and Client Contracts and determined that customers have a mechanism to communicate with BlockSurvey.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
CC1.2.1	Management Review Meetings are held every year to discuss the security level, Internal Audit results, Risks, changes, technology trends, occurrence of incidents, and security initiatives.	Selected a sample of Management Review Meetings held and inspected the minutes to determine that these are held on annually.	No Exceptions Noted
CC1.2.2	The Management team meets monthly and discusses the business as well as operational issues.	Selected a sample of management meetings held and inspected the minutes to determine that management meetings are held on a periodic basis.	No Exceptions Noted
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
CC1.3.1	Organization charts are established that depict authority, reporting lines, and responsibilities for the management of its information systems. These charts are communicated to employees and are updated as needed.	Inspected the organization chart for an understanding of the organization structure. Enquired with the management to determine that organization charts are updated periodically.	No Exceptions Noted
CC1.3.2	Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	Inspected the organization chart to determine that conflicting duties and areas of responsibility were segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	No Exceptions Noted
CC1.3.3	Organization has Information security policies and procedures that describe information security processes, practices.	Inspected Information Security policies and procedures to determine that these are documented, approved and reviewed by the management at least annually.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC1.3.4	A security governance structure for information security is defined, and the defined roles and responsibilities are allocated to accountable leadership.	Inspected the security governance group charter to determine that information security was defined, and the defined roles and responsibilities were allocated to accountable leadership.	No Exceptions Noted
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
CC1.4.1	Organization has established HR policies and procedures including recruitment, training, and exit	Inspected the HR Policies and procedures to determine that Policies and procedures including recruitment, training, and exit are established.	No Exceptions Noted
CC1.4.2	Job descriptions are in place which define roles and responsibilities, skills, knowledge levels and required competencies.	Inspected the job description for a sample of current employees to determine that documented job descriptions were in place for each employee sampled and defined roles and responsibilities, skills, knowledge levels and required competencies.	No Exceptions Noted
CC1.4.3	New employees sign the offer letter as their agreement and acceptance of broad terms of employment including a brief description of the position and other terms.	Selected a sample of new joiners and inspected the appointment letter to determine that new joiners accept the terms of employment.	No Exceptions Noted
CC1.4.4	Management evaluates the need for additional resources in order to achieve business objectives as part of its periodic management meetings	Inspected Manpower Planning meeting invite to determine that resource planning is reviewed periodically.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC1.4.5	Background verification checks on candidates for employment or contract work are carried out in accordance with relevant laws and regulations, and are conducted in proportion to business requirements, the classification of the information to be accessed, and the perceived risks.	Inspected the completed background verification checks for a sample of employees and contractors hired during the period to determine that background verification checks were completed for each sampled employee or contractor in accordance with relevant laws and regulations and were in proportion to business requirements, the classification of the information to be accessed, and the perceived risks.	No Exceptions Noted
CC1.4.6	Employees receive security and privacy awareness education and training upon hire.	Inspected the security and privacy awareness training results for a sample of employees hired during the period to determine that security and privacy awareness education and training was completed upon hire for each employee sampled.	No Exceptions Noted
CC1.4.7	Employees receive security and privacy awareness education and refresher training at least on an annual basis.	Inspected the security and privacy awareness education and refresher training results for a sample of current employees to determine that security and privacy awareness education and training was completed during the period for each employee sampled.	No Exceptions Noted
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC1.5.1	BlockSurvey leadership demonstrates leadership and commitment to the effectiveness of the information security management system by: 1) Ensuring its information security policy and objectives are compatible with organization's strategy, and that security objectives are achieved 2) Making sure the information security management system is integrated into organization's business processes and the required resources are available 3) Communicating the importance of conforming to requirements to ensure effective information security 4) Supporting management to provide leadership and directing and supporting people to contribute to the effectiveness of the information security management system 5) Promoting continual improvement	Inspected the Information security policy to determine that BlockSurvey leadership demonstrated leadership and commitment to the effectiveness of the information security management system by: 1) Ensuring its information security policy and objectives were compatible with organization's strategy, and that security objectives were achieved 2) Making sure the information security management system was integrated into organization's business processes and the required resources were available 3) Communicating the importance of conforming to requirements to ensure effective information security 4) Supporting management to provide leadership and directing and supporting people to contribute to the effectiveness of the information security management system 5) Promoting continual improvement	No Exceptions Noted
CC1.5.2	Job descriptions are reviewed by entity management on an annual basis as part of performance appraisals.	Inspected updated job descriptions to determine that job descriptions and roles and responsibilities are revised as and when required.	No Exceptions Noted
CC1.5.3	Performance appraisals are performed at least annually.	Inspected the evidence for performance appraisal for sampled employees to determine that Performance appraisals are performed at least annually.	No Exceptions Noted
Communication and Information			
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC2.1.1	BlockSurvey has defined and applies an information security risk assessment process. BlockSurvey has a risk management framework established to identify, report, and manage risks across key risk categories, including operational, strategic, legal, and financial.	Inspected a sample of internal audit reports & the corrective action taken to determine that an effective internal audit process is in place.	No Exceptions Noted
CC2.1.2	Risk assessments are performed on in-scope BlockSurvey assets for the information security management system and take into account threats to and vulnerabilities of the asset. The results of the risk assessments are reviewed by management at least annually.	Inspected the BlockSurvey asset register, the most recent risk register, and the Management Review meeting invite and agenda determine that risk assessments were performed on in-scope assets during the period and took into account threats to and vulnerabilities of the asset, and the results of the risk assessments were reviewed by management.	No Exceptions Noted
CC2.1.3	BlockSurvey has developed and implemented an ISMS for ensuring the confidentiality, integrity, and availability of its services and information assets. The ISMS operates within the context of organization's activities, and is documented, maintained, and continually improved.	Inspected the ISMS framework to determine that BlockSurvey developed and implemented an ISMS for the confidentiality, integrity, and availability of its services and information assets that operated within the context of organization's activities, and was documented, maintained, and continually improved.	No Exceptions Noted
CC2.1.4	BlockSurvey evaluates the information security performance and the effectiveness of the ISMS on at least an annual basis.	Inspected the most recent internal audit report and ISMS management review to determine that BlockSurvey evaluated the information security performance and the effectiveness of the ISMS during the period.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC2.1.5	BlockSurvey has an internal business assurance function which provides independent and objective assurance and advice on BlockSurvey's organisational governance, risk management, and internal control processes.	Inspected the security assurance, performance, and compliance framework to determine that an internal business assurance function provided independent and objective assurance and advice on BlockSurvey's organisational governance, risk management and internal control processes.	No Exceptions Noted
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
CC2.2.1	System boundaries in terms of logical boundaries are documented and network architecture diagrams are in place. System Boundaries are shared with the customers when it is required.	Inspected the network architecture diagram to determine that system boundaries in terms of logical boundaries are documented.	No Exceptions Noted
CC2.2.2	Customer responsibilities and appropriate system descriptions are provided in client contracts.	Inspected sampled client contracts to determine that terms related to brief requirements of the system and customer responsibilities are documented.	No Exceptions Noted
CC2.2.3	A ticketing system is in place which allows internal and external system users to report security failures, incidents, and concerns. Incidents and security incidents are responded to and managed to resolution by the incident response manager and the security operations team, respectively.	Inspected the incident ticket for a sample of incidents during the period to determine that a ticketing system was in place which allowed internal and external system users to report security failures, incidents and concerns, and incidents, and security incidents were responded to and managed through to resolution.	No Exceptions Noted
CC2.2.4	BlockSurvey communicates its commitment to security as a top priority for its customers via contracts.	Inspected client contracts of sampled customers to determine BlockSurvey communicates its commitment to security as a top priority for its customers via contracts.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC2.2.5	Changes to BlockSurvey's organisation, business processes, information processing facilities and systems that affect information security are controlled, and change details are communicated to relevant persons.	Inspected the path to production standard and sync up call meeting documentation to determine that changes to BlockSurvey's organisation, business processes, information processing facilities and systems that affected information security were controlled, and change details were communicated to relevant persons.	No Exceptions Noted
CC2.2.6	New employees hired at senior levels are communicated to stakeholders by HR through Email.	Enquired that senior management hires are communicated internally and if necessary, externally.	No Exceptions Noted
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.		
CC2.3.1	The organization's security, availability, and confidentiality commitments regarding the system are included in the client contracts and service agreements.	Inspected sample of client SOW, MSA, and NDA and determined that terms related to delivery of services are covered.	No Exceptions Noted
CC2.3.2	BlockSurvey requires employees as part of signing their employment contract, and contractors, to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire.	Inspected the signed NDA for a sample of employees and contractors hired during the period to determine that BlockSurvey required employees to sign agreements that included non-disclosure provisions and asset protection responsibilities, upon hire, for each employee sampled.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC2.3.3	NDA's are established with third parties during the procurement process where sensitive information is included within the scope of the services to be provided to BlockSurvey.	Inspected the NDA established with a sample of vendors onboarded during the period to determine that NDA's were established during the procurement process for each vendor sampled where sensitive information was included within the scope of the services to be provided to BlockSurvey.	No Exceptions Noted
CC2.3.4	Customer responsibilities are described in client contracts.	Inspected a sample of client contracts to determine explicit responsibilities of customer are documented .	No Exceptions Noted
CC2.3.5	Employees are informed of the process for reporting complaints and security breaches during induction Security Training.	Selected a sample of new employees and inspected evidence to determine that details related to reporting complaints and security breaches is covered as part of induction process.	No Exceptions Noted
CC2.3.6	Customer can provide their issues, complaints, or feedback through email to Business Heads.	Inspected customer resolution clauses in a sample of customer Statement of Work (SOW) and escalation matrix and determined that customers have a mechanism to communicate with BlockSurvey.	No Exceptions Noted
CC2.3.7	Changes to system boundaries, network systems are communicated to clients, if it impacts their operations.	Enquired with the management that system boundaries, network systems are communicated to clients, if it impacts their operations.	No Exceptions Noted
CC2.3.8	Incidents impacting external users are communicated to them through emails along with root cause analysis, if required.	Enquired with the management that Incidents impacting external users are communicated to them through emails along with root cause analysis, if required.	No Exceptions Noted

Risk Assessment

CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
--------------	---

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC3.1.1	Risk Assessment Scales (Risk Rating scales) are defined to evaluate and assess the significance of Risk. This is part of the Risk Management Framework.	Inspected Risk Assessment and Risk Treatment procedure to determine that Risk Assessment Scales (Risk Rating scales) are defined to evaluate and assess the significance of Risk.	No Exceptions Noted
CC3.1.2	Risk Assessment and Risk Treatment Procedure related to risk management are developed, implemented, and communicated to personnel.	Inspected Risk Assessment and Risk Treatment Procedures to determine that the BlockSurvey has a defined and documented risk assessment process.	No Exceptions Noted
CC3.1.3	Management evaluates the need for additional resources in order to achieve business objectives as part of its periodic management meetings	Inspected a sample of Manpower Planning sheet to determine that resource planning is reviewed periodically.	No Exceptions Noted
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.		
CC3.2.1	Risk Assessment and Risk Treatment Procedure related to risk management are developed, implemented, and communicated to personnel.	Inspected Risk Assessment and Risk Treatment Procedure to determine that the BlockSurvey has a defined and documented risk assessment process.	No Exceptions Noted
CC3.2.2	A risk assessment is performed annually or whenever there are changes in security posture. As part of this process, threats to security are identified and the risk from these threats is formally assessed.	Inspected Risk Assessment and Risk Treatment were performed during the audit period to determine updating of asset inventory, threats and risks and to determine that risk assessment is carried out at least on an annual basis.	No Exceptions Noted
CC3.2.3	Identified risks are rated and get prioritized based on their likelihood, impact, priority, and the existing control measures.	Inspected Risk Assessment performed during the year to determine identified risks are rated.	No Exceptions Noted
CC3.2.4	All information assets are identified in an asset inventory.	Inspected the Asset Inventory to determine that all information assets are identified in an asset inventory.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
CC3.3.1	The IT department maintains an up-to-date listing of all software and the security patches related to OS and application and patches are monitored.	Inspected sampled laptops to determine that latest patches are updated.	No Exceptions Noted
CC3.3.2	A List of all hardware is maintained as part of the asset register.	Inspected the asset register list to determine that all assets are recorded.	No Exceptions Noted
CC3.3.3	BlockSurvey has defined a formal Risk Assessment and Risk Treatment procedure for evaluating risks based on identified Probability, Impact, Risk Rating, Risk Priority, and mitigating controls.	Inspected Risk Assessment and Risk Treatment procedure to determine that the BlockSurvey has a defined and documented risk assessment process.	No Exceptions Noted
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.		
CC3.4.1	Changes to BlockSurvey's organisation, business processes, information processing facilities and systems that affect information security are controlled, and change details are communicated to relevant persons.	Inspected the path to production standard and sync up call meeting documentation to determine that changes to BlockSurvey's organisation, business processes, information processing facilities and systems that affected information security were controlled, and change details were communicated to relevant persons.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC3.4.2	Change management processes are in place to ensure that changes are recorded, evaluated authorised, planned, communicated, tested, and implemented successfully, before being deployed to production, in order to reduce the business impact of failed changes on BlockSurvey operation and its customers.	Inspected the change ticket for a sample of changes implemented during the period to determine that change management processes were in place to ensure that changes were recorded, evaluated authorised, planned, communicated, tested, and implemented successfully, before being deployed to production, in order to reduce the business impact of failed changes on BlockSurvey operation and its customers.	No Exceptions Noted
CC3.4.3	A risk assessment is performed annually or whenever there are changes in security posture. As part of this process, threats to security are identified and the risk from these threats is formally assessed.	Inspected Risk Assessment and Risk Treatment were performed during the audit period to determine updating of asset inventory, threats and risks and to determine that risk assessment is carried out at least on an annual basis.	No Exceptions Noted
CC3.4.4	A business continuity policy is defined to safeguard good service to BlockSurvey's customers, enhance the safety of staff, and protect the interests of other stakeholders.	Inspected the business continuity policy to determine that a business continuity policy was defined to safeguard good service to our customers, enhance the safety of staff, and protect the interests of other stakeholders.	No Exceptions Noted
CC3.4.5	The high availability and disaster recovery strategy align with the company strategy and are reviewed at least annually.	Inspected the high availability and disaster recovery strategy to determine that the high availability and disaster recovery strategy aligned with the company strategy and were reviewed during the period.	No Exceptions Noted

Monitoring Activities

CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
--------------	---

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC4.1.1	Information systems are reviewed on at least an annual basis for compliance with BlockSurvey's information security policies and standards.	Inspected the most recent internal audit report to determine that information systems were reviewed during the period for compliance with BlockSurvey's information security policies and standards.	No Exceptions Noted
CC4.1.2	IT system access is reviewed on a quarterly basis.	Inspected the information security policies containing access controls to determine that these are documented. Inspected evidence for access control reviews to determine that access rights are reviewed regularly, and user access lists are reconciled against active HR records.	No Exceptions Noted
CC4.1.3	Vulnerability assessment & penetration tests of the Network are performed at least annually by a third party.	Inspected the latest vulnerability assessment and penetration test report performed by a third party and determined that these are carried out at least annually and that vulnerabilities were closed.	No Exceptions Noted
CC4.1.4	BlockSurvey has an internal business assurance function which provides independent and objective assurance and advice on BlockSurvey's organisational governance, risk management, and internal control processes.	Inspected the security assurance, performance, and compliance framework to determine that an internal business assurance function provided independent and objective assurance and advice on BlockSurvey's organisational governance, risk management and internal control processes.	No Exceptions Noted
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.		

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC4.2.1	BlockSurvey evaluates the information security performance and the effectiveness of the ISMS on at least an annual basis.	Inspected the most recent internal audit report and management review meeting minuted to determine that BlockSurvey evaluated the information security performance and the effectiveness of the ISMS during the period.	No Exceptions Noted
CC4.2.2	Vulnerability assessment & penetration tests of the Network are performed at least annually by a third party.	Inspected the latest vulnerability assessment /penetration test report performed by a third party and determined that VA/PT have carried out at least annually and that vulnerabilities were closed.	No Exceptions Noted
CC4.2.3	All internal audit issues are tracked until closure to ensure that these are closed.	Inspected the Internal Audit results that issues are tracked until closure to ensure that these are closed.	No Exceptions Noted
CC4.2.4	A ticketing system is in place which allows internal and external system users to report security failures, incidents, and concerns. Incidents and security incidents are responded to and managed to resolution by the incident response manager and the security operations team, respectively.	Inspected the incident ticket for a sample of incidents during the period to determine that a ticketing system was in place which allowed internal and external system users to report security failures, incidents and concerns, and incidents, and security incidents were responded to and managed through to resolution.	No Exceptions Noted

Control Activities

CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.		
CC5.1.1	Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	Inspected the organization chart to determine that conflicting duties and areas of responsibility were segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC5.1.2	Information systems are reviewed on at least an annual basis for compliance with BlockSurvey's information security policies and standards.	Inspected the most recent internal audit report to determine that information systems were reviewed during the period for compliance with BlockSurvey's information security policies and standards.	No Exceptions Noted
CC5.1.3	A risk assessment is performed annually or whenever there are changes in security posture. As part of this process, threats to security are identified and the risk from these threats is formally assessed.	Inspected Risk Assessment and Risk Treatment were performed during the audit period to determine updating of asset inventory, threats and risks and to determine that risk assessment is carried out at least on an annual basis.	No Exceptions Noted
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.		
CC5.2.1	BlockSurvey has defined and documented access control policy that outline processes for identifying and authenticating authorized users, restricting user access to authorized system components, and preventing and detecting unauthorized system access.	Inspected the access control policy to determine that BlockSurvey defined and documented standards for access control that outlined processes for identifying and authenticating authorized users, restricting user access to authorized system components, and preventing and detecting unauthorized system access.	No Exceptions Noted
CC5.2.2	Policies and procedures related to risk management are developed, implemented, and communicated to personnel.	Inspected Risk Assessment & Treatment Procedure to determine that the organization has a defined and documented risk assessment process.	No Exceptions Noted
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC5.3.1	Information security policies are reviewed at planned intervals, or if significant changes in the BlockSurvey environment occur, to ensure their continuing suitability, adequacy, and effectiveness.	Inspected the Information security policies to determine that information security policies were reviewed during the period, or if significant changes in the BlockSurvey environment occurred, to ensure their continued suitability, adequacy, and effectiveness.	No Exceptions Noted
CC5.3.2	All policies and procedures clearly define the roles, responsibilities, and accountability for executing policies and procedures.	Inspected the policies roles to determine that roles, responsibilities are present for execution.	No Exceptions Noted
CC5.3.3	BlockSurvey has an internal business assurance function which provides independent and objective assurance and advice on BlockSurvey's organisational governance, risk management, and internal control processes.	Inspected the security assurance, performance, and compliance framework to determine that an internal business assurance function provided independent and objective assurance and advice on BlockSurvey's organisational governance, risk management and internal control processes.	No Exceptions Noted

Logical Access Controls

CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		
CC6.1.1	BlockSurvey has documented procedures for logical access controls.	Inspected the access control policy and procedure and determined that these are documented.	No Exceptions Noted
CC6.1.2	Access is granted on least privileges basis as default and any additional access needs to be approved.	Inspected access control procedure document and determined that access is granted on a least privileges basis as default and any additional access needs to be approved.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC6.1.3	The Engineering team has formally documented standard build procedures for installation and maintenance of the Firebase database and code repository that includes the requirement for access control systems to enforce logical access.	Inspected the evidence to determine that the Engineering team has formally documented standard build procedures for installation and maintenance of Firebase database and GitLab code repository that includes the requirement for access control systems to enforce logical access	No Exceptions Noted
CC6.1.4	BlockSurvey has established hardening standards in production infrastructure that include requirements for the implementation of security groups, access control, configuration settings, and standardized policies.	Inspected the hardening standards to determine that hardening standards have been established.	No Exceptions Noted
CC6.1.5	Production hosts and Security Groups (which are the equivalent of Firewalls) are hardened according to Industry best practices. Only the required ports are opened for inbound access at the load balancer level.	Inspected Render settings to determine that VPC has been set up and all production servers are within the private subnet. Inspected the IAM settings and security groups to determine that only the production group has access to production resources.	No Exceptions Noted
CC6.1.6	The in-scope systems and applications are configured to authenticate users with a unique user account and enforce minimum password requirements or SSH public key authentication.	Inspected the evidence to determine that the in-scope systems and applications are configured to authenticate users with a unique user account and enforce minimum password requirements or SSH public key authentication.	No Exceptions Noted
CC6.1.7	Cloud infrastructure is configured to use the Render's identity and access management system (IAM). Relevant groups have been added to IAM.	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

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC6.1.8	For Render console access, Multi-Factor Authentication is implemented.	Inspected the user settings in the Render console for the production group members to determine that multifactor authentication has been enabled.	No Exceptions Noted
CC6.1.9	All Assets are assigned owners who are responsible for evaluating access based on job roles. The owners define access rights when assets are acquired or changed.	Inspected the asset register and determined that assets and their owners are clearly documented.	No Exceptions Noted
CC6.1.10	Privileged access is allocated to users on a need-to-use basis in line with their job responsibilities and is controlled as per the access control policy.	Inspected the access control policy, listing of Render administrators to determine that privileged access was allocated to users on a need-to-use basis in line with their job responsibilities and was controlled as per the access control policy.	No Exceptions Noted
CC6.1.11	Predefined security groups are in place for in-scope systems using role-based access privileges.	Inspected the listing of Render user groups to determine that predefined security groups were in place for in-scope systems using role-based access privileges.	No Exceptions Noted
CC6.1.12	Data storage mechanisms are configured to encrypt data at rest in accordance with the cryptography standard.	Inspected the data at rest encryption configurations to determine that data storage mechanisms were configured to encrypt data at rest in accordance with the cryptography standard.	No Exceptions Noted
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC6.2.1	Permissions to individual accounts are restricted based on roles and job requirements.	Inspected the user access request for a sample of requests to the in-scope data systems and services during the period to determine that permissions to individual accounts was restricted based on roles and job requirements.	No Exceptions Noted
CC6.2.2	Access to in-scope systems requires users to authenticate via an individual user account using multi-factor or two-step authentication.	Inspected the Render management and authentication configurations to determine that access to in scope systems required users to authenticate via an individual user account using multi-factor or two-step authentication.	No Exceptions Noted
CC6.2.3	On the day of joining, HR will send a mail to the IT Help desk providing the details of the new joiners. The IT then provides necessary access as per the request. Employee user accounts are removed from various applications and network systems as of the last date of employment manually based on access revocation requests sent by the HR department.	Inspected the Access Control policy to determine that granting, modifying, or deactivating access is only done against written authorization. Inspected access request forms/emails for a sample of employees to determine that written authorization is in place. Inspected access revocation request /exit checklist for a sample of employees to determine that written authorization for deactivation is in place.	No Exceptions Noted
CC6.2.4	When an employee leaves the organization, the employee's manager initiates the 'Exit Process'. HR informs respective teams / IT teams within 24 hours to deactivate/delete the user ID from the email system and all applications. An exit checklist is used to ensure compliance with termination procedures.	Selected a sample of exited users and inspected Email from HR to IT and Exit Checklist to determine that the exit process and related account deactivation is as per defined procedures. Inspected Render IAM to determine that the exited user has disabled status.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC6.2.5	Access to data, systems and services in-scope systems is reviewed on a quarterly basis to confirm access is still appropriate.	Inspected the user access review for a sample of quarters to determine that access to data, systems and services in-scope systems was reviewed for each quarter sampled to confirm access was still appropriate.	No Exceptions Noted
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.		
CC6.3.1	A role based security process has been defined with in Render infrastructure based on job requirements.	Inspected the Render console screens to determine that security groups based on departments and roles have been defined.	No Exceptions Noted
CC6.3.2	Access to data, systems and services in-scope systems is reviewed on a quarterly basis to confirm access is still appropriate.	Inspected the user access review for a sample of quarters to determine that access to data, systems and services in-scope systems was reviewed for each quarter sampled to confirm access was still appropriate.	No Exceptions Noted
CC6.3.3	Permissions to individual accounts are restricted based on roles and job requirements.	Inspected the user access request for a sample of requests to the in-scope data systems and services during the period to determine that permissions to individual accounts was restricted based on roles and job requirements.	No Exceptions Noted
CC6.3.4	Company does not allow reactivation of ID belonging to an exited employee.	Enquired with IT Head that reactivation of IDs it is prohibited.	No Exceptions Noted
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.		
	<i>Not Applicable - No physical offices and related physical and availability specific controls are included since BlockSurvey does not have any physical office locations/physical servers and all data is processed on cloud services.</i>		

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.		
CC6.5.1	Media Handling Policy is implemented for procedures relating to disposal of information assets.	Inspected Media Handling Policy to determine that procedures relating to disposal of information assets are implemented.	No Exceptions Noted
CC6.5.2	All data is erased from laptops and other media prior to destruction disposal	Enquired with IT Head that all data is erased from laptops and other media prior to destruction disposal	No Exceptions Noted
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
CC6.6.1	The production system at Render is protected by security group rules (virtual firewall) set up for the virtual private cloud (VPC) provided by Render. VPC is used to protect all Production systems hosted at Render.	Inspected Render settings to determine that VPC has been set up and direct access to production instances is only through 2048-bit SSH keys.	No Exceptions Noted
CC6.6.2	Access to modify security group rules is restricted by IT Head to administrators.	Inspected the user list on IAM to determine that access to modify security group rules is restricted to only administrators.	No Exceptions Noted
CC6.6.3	Connections to the Render-hosted servers are through authenticated SSH sessions or authenticated secure browser sessions using HTTPS.	Inspected Render settings to determine that direct access to production instances is only through SSH keys.	No Exceptions Noted
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.		

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC6.7.1	The cryptography standard defines the security controls and operational practices applicable to customer data at rest, end user devices, backups, and web communication sessions. The standard also defines requirements for the annual generation, use, protection, audit, and rotation of cryptographic keys.	Inspected the cryptography and encryption policy to determine that it defined the security controls and operational practices applicable to customer data at rest, end user devices, backups, and web communication sessions and the requirements for the annual generation, use, protection, audit, and rotation of cryptographic keys.	No Exceptions Noted
CC6.7.2	Information involved in application services which passes over public networks is encrypted as per the established standards for data controls and for cryptography.	Inspected the cryptography and encryption policy, the TLS encryption certificate, and SSL labs report to determine that information involved in application services which passes over public networks was encrypted as per the established standards for data controls and for cryptography.	No Exceptions Noted
CC6.7.3	Transport encryption requirements are defined within the cryptography standard and comply with legal and regulatory requirements.	Inspected the cryptography and encryption policy to determine that transport encryption requirements were defined within the cryptography standard and complied with legal and regulatory requirements.	No Exceptions Noted
CC6.7.4	Data storage mechanisms are configured to encrypt data at rest in accordance with the cryptography standard.	Inspected the data at rest encryption configurations to determine that data storage mechanisms were configured to encrypt data at rest in accordance with the cryptography standard.	No Exceptions Noted
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.		

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC6.8.1	Antivirus protection is enabled on end-user devices and virus definitions are updated automatically. Network traffic is inspected for malware, application, and server vulnerabilities, insider threats and unwanted application traffic.	Inspected the antivirus configurations to determine that antivirus protection was enabled on end-user devices and virus definitions were updated automatically and that network traffic was inspected for malware, application and server vulnerabilities, insider threats and unwanted application traffic.	No Exceptions Noted
CC6.8.2	Security monitoring systems are in place to monitor and analyse the in-scope systems for possible or actual security breaches.	Inspected the logging and monitoring application configurations and example alerts generated during the period to determine that security monitoring systems were in place to monitor and analyse the in-scope systems for possible or actual security breaches.	No Exceptions Noted
CC6.8.3	Systems in the production environment are hardened, based on CIS benchmarks.	Inspected the CIS benchmark and hardening guidelines to determine that systems in the production environment were hardened, based on CIS benchmarks.	No Exceptions Noted
System Operations			
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.		
CC7.1.1	Management has defined configuration standards and hardening standards.	Inspected the system hardening checklist to determine that Management has defined configuration standards and hardening standards.	No Exceptions Noted
CC7.1.2	BlockSurvey monitors infrastructure and software for non-compliance with the standards, which could threaten the achievement of the organization's objectives.	Inspected the Render Metrics dashboard to determine entity monitors infrastructure and software for noncompliance with the standards.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC7.1.3	Vulnerability assessment & penetration tests are performed at least annually by a third party.	Inspected the latest vulnerability assessment /penetration test report performed by a third party and determined that these are carried out at least annually and that vulnerabilities were closed.	No Exceptions Noted
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.		
CC7.2.1	Documented incident response procedures are in place to guide personnel that handle incidents and include the process for informing the entity about actual and potential events that impact system security and for submitting complaints as well as roles and responsibilities for teams involved. Procedures are communicated to employees and customers as required.	Inspected the security incident response plan and procedures to determine that documented procedures were in place to guide personnel in the handling of incidents and included the process for informing the entity about actual and potential events that impacted system security and for submitting complaints as well as roles and responsibilities for teams involved, and procedures were communicated to employees and customers.	No Exceptions Noted
CC7.2.2	The IT team receives requests for support through phones, emails, which may include requests to reset user passwords, etc.	Inspected a sample of IT support ticket emails reported by users to determine that support tickets are logged as emails.	No Exceptions Noted
CC7.2.3	Vulnerability assessment & penetration tests are performed at least annually by a third party.	Inspected the latest vulnerability assessment /penetration test report performed by a third party and determined that these are carried out at least annually and that vulnerabilities were closed.	No Exceptions Noted
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.		

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC7.3.1	A formal, defined incident management Policy is documented as part of Information Security Policies for evaluating reported events.	Inspected Incident Management Policy to determine that the incident management process is documented.	No Exceptions Noted
CC7.3.2	Incidents are reported to the IT team by email. These are tracked through the Incident logs.	Inspected the screenshot of the incident log to determine that incidents are tracked.	No Exceptions Noted
CC7.3.3	Reported incidents are logged in Excel/Incident form and include the following details: - Incident Type - Data and Time of incident - Details - Action Taken - Root Cause (For select high-risk incidents)	Inspected a sample of the incident report to determine that incidents covered the following: - Incident Type - Data and Time of incident - Details - Action Taken - Root Cause (For select high-risk incidents)	No Exceptions Noted
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.		
CC7.4.1	All security incidents are also reviewed and monitored by the Information Security Group. Corrective and preventive actions are completed for incidents.	Inspected minutes MRM meeting minutes to determine that discussion on incidents takes place.	No Exceptions Noted
CC7.4.2	All incidents are evaluated and necessary action taken to close the threat/vulnerability.	Inspected Incident Management Procedure and determined that necessary action is taken to close the threat/vulnerability.	No Exceptions Noted
CC7.4.3	Protocols for communicating security incidents and actions taken to affected parties are developed and implemented to meet the entity's objectives.	Inspected Incident Management Procedure and determined that necessary action is taken for communicating security incidents and actions taken to affected parties are developed and implemented	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC7.4.4	Management reviews all incidents that occurred during the year as part of Management Review Meeting.	Inspected MRM meeting minutes to determine that annually management reviews all incidents that occurred during the year is conducted.	No Exceptions Noted
CC7.4.5	HR policies include a code of conduct and disciplinary policy for employee misconduct.	Inspected the Code of Conduct and Disciplinary Policy to determine that these are established.	No Exceptions Noted
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.		
CC7.5.1	All incidents are evaluated and necessary action is taken to close the identified vulnerability/threat.	Inspected Incident Management Policy and determined that necessary action is taken to close the identified threat/vulnerability.	No Exceptions Noted
CC7.5.2	Root cause analysis is performed for major incidents.	Inspected the screenshot of the incident log and related root cause description for some incidents to determine that incidents are tracked.	No Exceptions Noted
Change Management			
CC8.1	The entity authorizes, designs, develops acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.		
CC8.1.1	Application development and testing on BlockSurvey platform are done in separate environments from production.	Inspected the evidence to determine that the platform application development and testing are done in separate environments from production.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC8.1.2	BlockSurvey uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system admin.	Inspected the screenshot from the version control/GitLab code repository to determine that BlockSurvey uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system admin.	No Exceptions Noted
CC8.1.3	BlockSurvey's application code changes, code reviews, and tests are performed by someone other than the person who made the code change.	Inspected the company records to determine that BlockSurvey's application code changes, code reviews, and tests are performed by someone other than the person who made the code change.	No Exceptions Noted
CC8.1.4	Authorized BlockSurvey personnel can push or make changes to production code.	Inspected the company records to determine that authorized BlockSurvey personnel can push or make changes to production code.	No Exceptions Noted
CC8.1.5	All change requests are submitted with Risk Assessment, implementation, and rollback plans. The code repository & deploy tool has a turnover process that includes back out steps commit is to be reverted.	Inspected a sample of change requests to determine that they had Risk Assessment, implementation, and rollback plans included.	No Exceptions Noted
CC8.1.6	Changes are communicated to the appropriate client and user community if the change has any potential impact on the user base.	Enquired with IT Head that changes are communicated to clients and end users if it has an impact on those users.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC8.1.7	Change management policies and procedures are in place to guide personnel in the request, documentation, testing, and approval of changes. The policies and procedures also outline the requirement for segregation of duties such that authorization, development, testing and implementation are segmented functions within the process.	Inspected the change management policies and procedures to determine that these were in place to guide personnel in the request, documentation, testing, and approval of changes. The policies and procedures also outline the requirement for segregation of duties such that authorization, development, testing and implementation are segmented functions within the process.	No Exceptions Noted
Risk Mitigation			
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
CC9.1.1	BlockSurvey has a documented Business Continuity Procedure & Plan including Disaster Recovery guidelines to be used in the event of an event necessitating systems infrastructure recovery.	Inspected the Business Continuity Procedure & Plan to determine that a plan and procedure have been documented with clear responsibilities on those required to respond.	No Exceptions Noted
CC9.1.2	Business continuity and disaster recovery plans, including restoration of backups, are tested annually.	Inspected the Business Continuity Planning Policy and determined that BCP plans are tested at least annually.	No Exceptions Noted
CC9.2	The entity assesses and manages risks associated with vendors and business partners.		
CC9.2.1	BlockSurvey management reviews the annual SOC report for its sub-processors to confirm that outsourced controls are appropriately designed and operating effectively.	Inspected the company records to determine that BlockSurvey management reviews the annual SOC report for its sub-processors to confirm that outsourced controls are appropriately designed and operating effectively.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC9.2.2	A vendor management process is in place and requires signed contracts for vendors and includes (1) scope of services and product specifications, (2) roles and responsibilities, (3) compliance requirements, and (4) service levels where applicable.	Inspected the company records to determine that a vendor management process is in place and requires signed contracts for vendors and includes (1) scope of services and product specifications, (2) roles and responsibilities, (3) compliance requirements, and (4) service levels where applicable.	No Exceptions Noted
CC9.2.3	A formal contract is executed between the Company and Third-Party Service Providers before the work is initiated. The agreement includes terms of confidentiality and responsibilities of both parties.	Inspected a sample of vendor contracts to determine that vendor's contracts are in place which includes terms of confidentiality and responsibilities of both parties.	No Exceptions Noted
CC9.2.4	All customer & vendor contracts have signed NDA.	Inspected signed NDA and vendor contracts for sample vendors to determine that they NDA is signed.	No Exceptions Noted

ADDITIONAL CRITERIA FOR AVAILABILITY

A1.1	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.		
A1.1.1	A monitoring system is utilized to monitor system performance and operations, including unusual activities, system uptime, system processing, CPU usage, and memory storage.	Inspected the monitoring tool dashboard to determine that a monitoring system is utilized to monitor system performance and operations, including unusual activities, system uptime, system processing, CPU usage, and memory storage.	No Exceptions Noted
A1.1.2	Load balancing is enforced to distribute network traffic across multiple infrastructure resources within the cloud IT environment.	Inspected the evidence to determine that load balancing is enforced to distribute network traffic across multiple infrastructure resources within the cloud IT environment.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
A1.1.3	Auto-scaling is enforced within the cloud IT environment to automatically scale infrastructure resources to support network workload and facilitate continued operations.	Inspected the company records to determine that auto-scaling is enforced within the cloud IT environment to automatically scale infrastructure resources to support network workload and facilitate continued operations.	No Exceptions Noted
A1.1.4	Processing capacity for cloud infrastructure is monitored on an ongoing basis.	Inspected dashboard of Render Metrics settings to determine that alerts & thresholds have been setup for abnormal conditions such as low CPU utilization, network outage, free storage, etc.	No Exceptions Noted
A1.2	The entity authorizes, designs, develops, or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup, and recovery infrastructure to meet its objectives.		
A1.2.1	Incremental and full backup procedures are performed on production databases, on a daily basis to store duplicate copies of data for system availability and data restoration in the event of a business disruption or security incident.	Inspected the evidence to to determine that incremental and full backup procedures are performed on production databases, on a daily basis to store duplicate copies of data for system availability and data restoration in the event of a business disruption or security incident.	No Exceptions Noted
A1.2.2	The BlockSurvey platform is implemented in a high-availability configuration which uses multiple, redundant availability zones and is based on the good practice guidelines set by the cloud provider.	Inspected the Render server and Firebase database configurations to determine that the GCP platform was implemented in a high-availability configuration which used multiple, redundant availability zones based on the good practice guidelines set by Render.	No Exceptions Noted
	<i>Render is responsible for implementing controls that ensure the data center facilities are equipped with physical and environmental security safeguards.</i>		
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.		

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
A1.3.1	Management performs annual testing of the Business Continuity and Disaster Recovery (BCDR) plan to evaluate the effectiveness of its defined procedures. Issues identified during testing procedures are investigated and remediated to remediate identified issues.	Inspected the evidence to determine that management performs annual testing of the Business Continuity and Disaster Recovery (BCDR) plan to evaluate the effectiveness of its defined procedures. Issues identified during testing procedures are investigated and remediated to remediate identified issues.	No Exceptions Noted
A1.3.2	Business continuity plans, including restoration of backups, are tested at least annually.	Inspected backup restoration test report to determine that restoration tests are conducted at least annually.	No Exceptions Noted
ADDITIONAL CRITERIA FOR CONFIDENTIALITY			
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.		
C1.1.1	Management has established a Data Retention and Disposal Policy to define procedures for the appropriate retention, disclosure, and disposal of sensitive, confidential, and personal information	Inspected the evidence to determine that management has established a Data Retention and Disposal Policy to define procedures for the appropriate retention, disclosure, and disposal of sensitive, confidential, and personal information.	No Exceptions Noted
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.		
C1.2.1	Management has established a Data Retention and Disposal Policy to define procedures for the appropriate retention, disclosure, and disposal of sensitive, confidential, and personal information.	Inspected the evidence to determine that management has established a Data Retention and Disposal Policy to define procedures for the appropriate retention, disclosure, and disposal of sensitive, confidential, and personal information.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
C1.2.2	BlockSurvey securely deletes Customer Data upon termination of services.	Inspected the evidence to determine that BlockSurvey securely deletes Customer Data upon termination of services as per the contractual requirements.	No Exceptions Noted

SECTION 5

OTHER INFORMATION PROVIDED BY BLOCKSURVEY

Other Information Provided by BlockSurvey

The information provided in this section is provided for informational purposes only by BlockSurvey. 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.

BlockSurvey has implemented logical controls to safeguard against interruption of service. BlockSurvey has developed a number of procedures that provide for the continuity of operations in the event of an availability zone failure by spinning up multiple servers across all availability zones.

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

CERTIFICATE *of* SIGNATURE

REF. NUMBER
QA53V-BFCWJ-NQI37-4D4JO

DOCUMENT COMPLETED BY ALL PARTIES ON
05 AUG 2025 17:59:36 UTC

SIGNER

WILSON BRIGHT JOHN

EMAIL
WILSON@BLOCKSURVEY.ORG

TIMESTAMP

SENT
05 AUG 2025 07:11:55 UTC

VIEWED
05 AUG 2025 17:59:06 UTC

SIGNED
05 AUG 2025 17:59:36 UTC

SIGNATURE

Wilson Bright John

IP ADDRESS
223.185.130.93

LOCATION
BENGALURU, INDIA

RECIPIENT VERIFICATION

EMAIL VERIFIED
05 AUG 2025 17:59:06 UTC

