AEC Solutions, Inc. dba Builterra

Type II System and Organization Controls Report (SOC 2)

Report on a Service Organization's Description of Its System and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security, Availability, and Confidentiality Throughout the Period December 1, 2022, to November 30, 2023.

KirkpatrickPrice
4235 Hillsboro Pike
Suite 300
Nashville, TN 37215

TABLE OF CONTENTS

SECTION I:
ASSERTION OF AEC SOLUTIONS, INC. DBA BUILTERRA MANAGEMENT

ASSERTION OF AEC SOLUTIONS, INC. DBA BUILTERRA MANAGEMENT

We have prepared the accompanying description in section III titled "AEC Solutions, Inc. dba Builterra's Description of Its Construction Contract Administration Platform System" throughout the period December 1, 2022, to November 30, 2023, (description), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (AICPA, *Description Criteria*), (description criteria). The description is intended to provide report users with information about the construction contract administration platform system that may be useful when assessing the risks arising from interactions with AEC Solutions, Inc. dba Builterra's system, particularly information about system controls that AEC Solutions, Inc. dba Builterra 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 section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

AEC Solutions, Inc. dba Builterra uses Azure for cloud hosting. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at AEC Solutions, Inc. dba Builterra, to achieve AEC Solutions, Inc. dba Builterra's service commitments and system requirements based on the applicable trust services criteria. The description presents AEC Solutions, Inc. dba Builterra's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of AEC Solutions, Inc. dba Builterra'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 AEC Solutions, Inc. dba Builterra, to achieve AEC Solutions, Inc. dba Builterra's service commitments and system requirements based on the applicable trust services criteria. The description presents AEC Solutions, Inc. dba Builterra's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of AEC Solutions, Inc. dba Builterra's controls.

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

a. the description presents AEC Solutions, Inc. dba Builterra's construction contract administration platform system that was designed and implemented throughout the period December 1, 2022, to November 30, 2023, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period December 1, 2022, to November 30, 2023, to provide reasonable assurance that AEC Solutions, Inc. dba Builterra'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 AEC Solutions, Inc. dba Builterra's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period December 1, 2022, to November 30, 2023, to provide reasonable assurance that AEC Solutions, Inc. dba Builterra'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 AEC Solutions, Inc. dba Builterra's controls operated effectively throughout that period.

SECTION II:
INDEPENDENT SERVICE AUDITOR'S REPORT

Chris Stebbing, P. Eng.
Founding Partner & Director of Platform Development
AEC Solutions, Inc. dba Builterra
17 Keble Court
Richmond Hill, ON L4E 5E5

Scope

We have examined AEC Solutions, Inc. dba Builterra's accompanying description in section III titled "AEC Solutions, Inc. dba Builterra's Description of Its Construction Contract Administration Platform System" throughout the period December 1, 2022, to November 30, 2023, (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period December 1, 2022, to November 30, 2023, to provide reasonable assurance that AEC Solutions, Inc. dba Builterra'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 section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

AEC Solutions, Inc. dba Builterra uses Azure for cloud hosting. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at AEC Solutions, Inc. dba Builterra, to achieve AEC Solutions, Inc. dba Builterra's service commitments and system requirements based on the applicable trust services criteria. The description presents AEC Solutions, Inc. dba Builterra's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of AEC Solutions, Inc. dba Builterra'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 indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at AEC Solutions, Inc. dba Builterra, to achieve AEC Solutions, Inc. dba Builterra's service commitments and system requirements based on the applicable trust services criteria. The description presents AEC Solutions, Inc. dba Builterra's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of AEC Solutions, Inc. dba Builterra's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

AEC Solutions, Inc. dba Builterra 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 AEC Solutions, Inc. dba Builterra's service commitments and system requirements were achieved. In section I, AEC Solutions, Inc. dba Builterra has provided its assertion titled "Assertion of AEC Solutions, Inc. dba Builterra Management" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. AEC Solutions, Inc. dba Builterra 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 American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, 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.

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

- 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.

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

Inherent Limitations

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

There are inherent limitations in the effectiveness of 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 policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are presented in section IV, "Trust Services Categories, Criteria, Related Controls, and Tests of Controls," of this report in columns 2, 3, and 4, respectively.

Opinion

In our opinion, in all material respects,

a. the description presents AEC Solutions, Inc. dba Builterra's construction contract administration platform system that was designed and implemented throughout the period December 1, 2022, to November 30, 2023, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period December 1, 2022, to November 30, 2023, to provide reasonable assurance that AEC Solutions, Inc. dba Builterra'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 AEC Solutions, Inc. dba Builterra's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period December 1, 2022, to November 30, 2023, to provide reasonable assurance that AEC Solutions, Inc. dba Builterra'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 AEC Solutions, Inc. dba Builterra's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in section IV, is intended solely for the information and use of AEC Solutions, Inc. dba Builterra, user entities of AEC Solutions, Inc. dba Builterra's construction contract administration platform system during some or all of the period December 1, 2022, to November 30, 2023, business partners of AEC Solutions, Inc. dba Builterra subject to risks arising from interactions with the construction contract administration platform 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 user entity controls and 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 these specified parties.

Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

January 11, 2024

SECTION III:
AEC SOLUTIONS, INC. DBA BUILTERRA'S DESCRIPTION OF ITS CONSTRUCTION CONTRACT ADMINISTRATION PLATFORM SYSTEM

SERVICES PROVIDED

Builterra is a software-as-a-service (SaaS) application developed by AEC Solutions, Inc. (AEC). The application provides clients with an end-to-end integrated construction contract administration workflow process that is presented to AEC's clients via Microsoft Azure Cloud Platform-as-a-Service (PaaS) infrastructure. The description this audit covers relates to AEC's development and implementation of its Builterra product. AEC released the Builterra construction contract administration application in 2016 for the workflow of the entire construction contract administration process by providing the following features:

- Design Quantity Take-offs
- Cost Estimating
- Bid Preparation
- Bid Analysis
- Bid Processing
- Field Inspection Reports
- Payment Certification

The Builterra platform allows clients to manage civil engineering and construction projects and is used for contracting, cost estimation, bid management, payment certifications, and inspection report capabilities. Enterprise accounts can manage internal users without the assistance from Builterra team, but support is available if needed. The platform is capable of storing images and text and designing custom reports and billing and contains the following key areas:

- Inspect
- Tender
- Project
- Ad hoc Reports
- Photo Map
- Workflow
- Training
- User Management

After signing a contract, clients for Builterra are assigned a support person and must fill out a spreadsheet to collect the requirements needed to build their solution. Onboarding is documented with Freshdesk tickets. The process includes client personnel for training, projects to be setup in the Builterra platform, start date, report needs, and logo for the reports. All clients' initial enterprise account is responsible for internal user accounts.

For customer offboarding, clients can choose to stop paying for their Builterra license. The support team is notified to provide clients with their documents and all data is retained, unless stated otherwise, for three years following separation.

Contractual Commitments

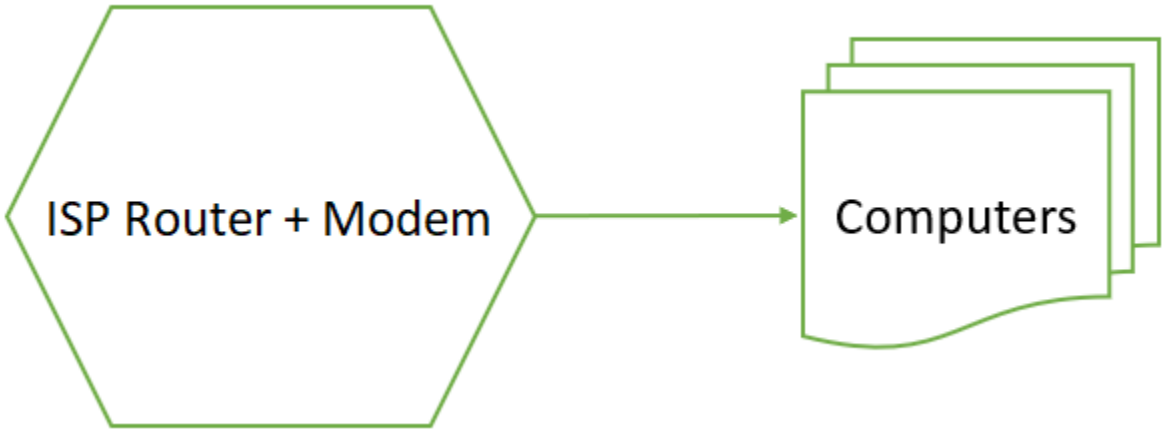
The organization maintains their Terms of Service on the company website that customers are able to access and review. The terms outlines service agreements, service management, and the scope of service for all customers. Additionally, AEC displays its privacy policy to communicate its privacy requirements and detail the use of client information.

System Design

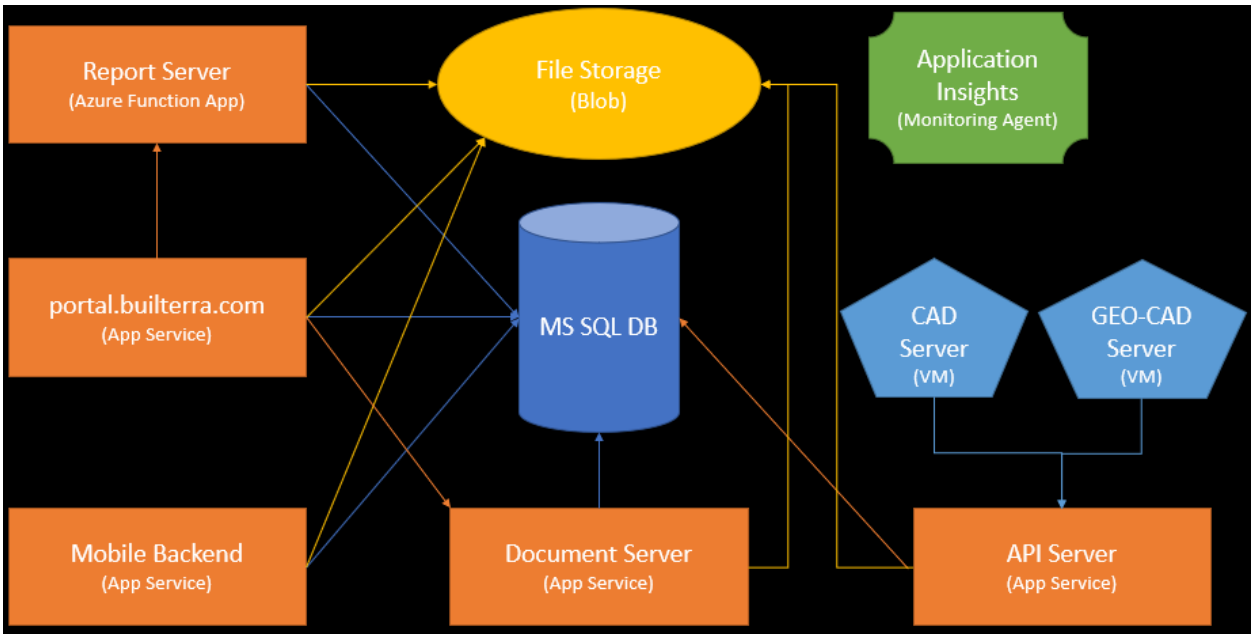
AEC designs its construction contract administration platform system to meet its regulatory and contractual commitments. These commitments are based on the services that AEC provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that AEC has established for its services. AEC establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in AEC' system policies and procedures, system design documentation, and contracts with clients.

Infrastructure

AEC uses diagrams to depict its system infrastructure and show server connections. The diagram below is the network diagram:



The server diagram (below) shows connection between servers and the connections between each one.



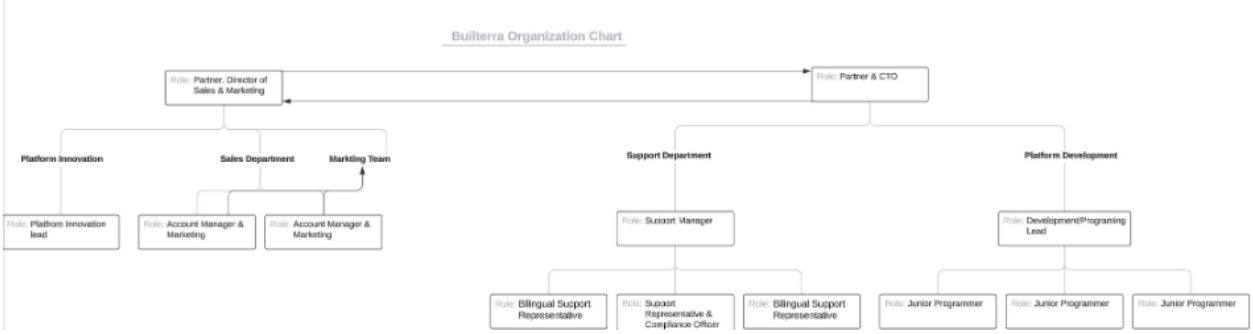
Software

AEC relies on various critical software to perform its services. The organization tracks and lists all software in the Approved Software List spreadsheet. The list includes the name, version, vendor, function, and notes. AEC relies on the following critical software:

- Salesforce
- Freshdesk
- QuickBooks
- Eventbrite
- Campaign Monitor
- Hunter.io
- Linking Sales Navigation
- Last Pass
- Microsoft 365
- OneDrive
- Indeed
- Visual Studio
- Speechelo
- SendGrid
- MailChimp
- Castanet

People

The organization functions under a traditional structure with direct reporting lines to both Founding Partners. Both partners oversee specific business areas within the company and provide company oversight and direction. The Organization Chart (below) depicts the structure and reporting lines for the organization:



Data

The organization receives and processes data from clients through the Builterra platform. No sensitive data is required to use the platform, but it may be used to store billing information. To ensure data security, AEC uses secure encryption methods for data at rest and in transit. The organization uses AES 256 encryption for data within the database and Transport Layer Security (TLS) 1.2 for traffic data, and HTTP is redirected to HTTPS.

Additionally, AEC has established a data classification policy in order to identify and store all received data. All data is classified as either Public, Internal Use, Restricted, or Confidential. This process allows guidance for the retention timelines, as outline in the organization's data retention policy. The policy defines the following schedules:

- Public: Seven years
- Internal: Use seven years
- Restricted: Only retained when necessary and needed
- Confidential: Only retained when necessary and needed

Processes and Procedures

Management has developed and communicated procedures to guide the provision of the organization's services. Changes to procedures are performed annually and authorized by management. These procedures cover the following key security life cycle areas:

- Data classification
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, user functionality, master passwords, powerful utilities, and security devices

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

The security, availability, and confidentiality categories and applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Security, availability, and confidentiality criteria and controls designed, implemented, and operated to meet them ensure that the system is protected against unauthorized access (both physical and logical). The controls supporting the applicable trust services security, availability, and confidentiality criteria are included in section IV of this report. Although the applicable trust services criteria and related controls are included in section IV, they are an integral part of AEC's description of its construction contract administration platform system.

Control Environment

Management Philosophy

AEC has established a code of conduct and an employee handbook within the Master Policy List. The document communicates all behavior and conduct expectations and the Employee Handbook also contains a discipline policy that includes discipline procedures up to termination. The organization distributes the policy to employees during onboarding, and employees are required to acknowledge the document upon receipt.

Security, Availability, and Confidentiality Management

The organization's security, availability, and confidentiality requirements are managed using a combination of documented policies and procedures, management oversight, and network systems and hardware. These management practices are implemented in all areas of the control environment to protect systems, data, and personnel and to ensure compliance with industry best practices and standards.

Security, Availability, and Confidentiality Policies

All policies and procedures are hosted within the Master Policy List, a comprehensive document that the organization uses for information security guidance. The Compliance Team is responsible for reviewing and approving the Master Policy List and all policies within. The following policies are included within the Master Policy List:

- Acceptable Use & Hardening Policy
- Classification Policy
- Internal Information Security Policy
- Systems' Users, Groups, and Domain Policy
- Business Continuity Policy
- Vendor Management Policy
- Web Application Security Policy
- Password Policy
- Builterra Password Policy
- Backup and Recovery Policy
- Acceptable Encryption Policy
- Managing User Access Policy
- Hiring Policy
- Office Change Management
- Minimum Access Policy
- Privacy Agreement Policy
- Employee Background Check Policy
- Incident Reporting Policy
- Software Development Policy
- Employee Code of Ethics Policy

Personnel Security

The organization has established a designated hiring manager depending on the department. All employees follow a set onboarding process to ensure security and includes policy acknowledgements, background checks, and training. Employees are provided the Employee Handbook and Code of Conduct, as well as other related Human Resources (HR) documents for acknowledgement. AEC also provides security awareness training for all employees to complete upon hire and annually thereafter.

All employees are required to undergo a background check prior to hire. AEC has an official policy to conduct background checks with the following screenings:

- Identity
- Employment education
- Social Security number (SSN)
- Residency

Additionally, employees are required to acknowledge the Employee Non-Disclosure Agreement (NDA) during the onboarding process. The NDA outlines the confidentiality expectations for employees and requires secure protection for all company and client data.

For termination, AEC maintains the Employee Termination Checklist for guidance for managing voluntary and involuntary terminations. The checklist is used to collect information for the date, manager, department, and reason for resignation/termination. All access is removed for the employee upon termination.

Change Management

AEC maintains a policy within the Master Policy List to maintain secure system configurations. The organization uses Microsoft Intune for mobile device management and enforcing hardening standards and uses Microsoft Defender for all antivirus and anti-malware software. Additionally, the Founding Partner & Director of Platform Development and the Compliance Officer stay up to date with Microsoft industry standards for system configurations.

Any changes to the system follow the change management policy within the Master Policy List, which provides governance for all change processes. All changes must be defined and documented and change implementation must be approved by the Compliance Team. There are five levels of Change priorities which include:

- Critical: A change that, if not implemented immediately, will leave the organization open to significant risk.
- High: A change that is important for the organization and must be implemented soon to prevent a significant negative impact on the ability to conduct business.
- Medium: A change that must be implemented to gain benefit from the changed service.
- Low: A change that is not pressing but would be advantageous.
- Ignored: A change that was suggested but not implemented at the time.

Application Development

AEC follows a set software development life cycle (SDLC) to outline the processes for application development. The SDLC is comprised of phases for the development process and includes the following:

- Planning Phase (Requirement Gathering & Analysis)
- System and Technical Design Phase
- Development Phase
- Testing Phase
- Deployment Phase

Additionally, AEC maintains separate environments for the development, staging, and production environments. All new software and updates undergo a risk assessment, and based on the risk assessment, the application design process is developed. This process extends not only to the creation and maintenance of use accounts and permissions within the application, but also the following areas:

- Data input validation controls
- Data flow
- Data output
- Interfaces with other systems
- Reporting
- Time stamps
- Logging
- Batch and transaction counters
- Monitoring facilities
- Use of cryptography

Application Change Management

All changes are documented, reviewed, tested, and approved before deployment. The organization maintains a formal change management process to control changes to all critical information resources. Changes are prioritized based on benefits, urgency, effort required, and potential impact to operations. Additionally, changes must have a backout plan in the event that rollback needs to occur.

System Monitoring

A web application firewall is installed and the organization restricts all inbound and outbound traffic. Whitelisting is used for employee IPs and enforced with the firewall. Additionally, both antivirus and anti-malware software have been installed with Microsoft Intune and Microsoft Defender on all workstations.

AEC uses a third-party penetration testing company (CyberHunter) to run bi-annual penetration tests, typically after any major releases. CyberHunter also performs monthly vulnerability scans for all company systems. Internally, the organization uses Nessus Essentials for all workstations to create vulnerability scans based on the computer's looping host IP. The Founding Partner & Director of Platform Development receives alerts for all Azure health and critical events. Nessus Essentials also performs quarterly scans on all workstations. The reports are sent to the

Compliance office, and any high or critical vulnerabilities are sent to the relevant personnel for review and troubleshooting.

A vulnerability management policy is outlined within the Master Policy List that details the remediation process. All remediations follow the Vulnerability Remediation Timeline:

- Critical vulnerabilities must be reviewed and resolved unless the risk the accepted within 48 hours.
- High vulnerabilities must be reviewed and resolved unless the risk the accepted within 72 hours.
- Any lower impact vulnerabilities must be reviewed and considered for remediation but it is not required to do so for low, medium, and information vulnerabilities.
- Acceptance of vulnerabilities can be performed by the Office Manager and the Lead Developer.

Problem Management

The organization maintains a formal incident response policy within the Master Policy List as the Incident Reporting Policy. The policy provides guidance and procedures for identifying and managing incidents and also provides instructions for security incident response including definitions, procedures, responsibilities, and performance measures. After an incident is reported, the Chief Technology Officer assigns a severity level that is used to determine the level of remediation effort required:

- High: the incident is potentially catastrophic to the organization and/or disrupts the organization's day-to-day operations; a violation of legal, regulatory, or contractual requirements is likely.
- Medium: the incident may cause harm to one or more business units within the organization and/or cause delays to a business unit's activities.
- Low: the incident is a clear violation of organizational security policy but does not substantively impact the business.

Additionally, AEC also enforces incident response training for all personnel to ensure that the plan remains current and effective for incident response. The procedure is tested bi-annually and all logs are reviewed during a quarterly SOC 2 meeting.

Data Backup and Recovery

AEC performs regular system and data backups according to a set backup policy defined within the Master Policy List. The policy ensures that backup copies are created at defined intervals and regularly tested. All backup data must be stored encrypted with the AES-256 symmetric encryption algorithm, and backup copies must be stored in an environmentally protected and access-controlled secure location that is offsite from the location of the originating asset. Stored copies must be stored with a short description that includes the backup date and resource name and all stored copies of data must be made available upon authorized request. The organization maintains 35 days of full daily backups and maintains three years of a monthly backup in Azure. Additionally, the organization tests backup restoration at least annually to ensure that all systems are recoverable.

AEC also maintains a business continuity plan and a sub-policy for the disaster recovery plan (DRP). Each manager must perform a business risk assessment and a DRP for each key business system within their area of responsibility and each DRP includes the following:

- Key business processes
- Applicable risk to availability
- Prioritization of recovery
- Recovery Time Objectives (RTOs)
- Recovery Point Objectives (RPOs)

System Account Management

AEC implements logical access controls to ensure that systems, networks, and accounts are secured. Multi-factor authentication (MFA) is required for all system logins and an account lockout policy locks all accounts for five minutes after five invalid login attempts. All accounts adhere to a password policy that enforces the use of complex passwords and has established a minimum length requirement. The last five passwords are remembered and cannot be reused by a user.

All access is restricted based on a need-to-share basis and access permissions are assigned by role. Access is issued during the onboarding process with the approval of the Founding Partner & Director of Platform Development. All internal access is managed with Microsoft 365 and is administered by the Compliance Officer and the Founding Partner & Director of Platform Development.

Customers are responsible for setting up user accounts and user access controls following initial training. The organization documents requirements for adding and removing a subscriber account within the Builterra SaaS platform, including the use of unique user IDs and unique passwords. The documentation specifies that once training is complete, it is the responsibility of the customer to manage and maintain user access. If termination of access is necessary, the customer is provided an opportunity to retrieve data, then the instance is removed and the customer data is deleted.

Risk Assessment Process

AEC conducts a formal risk assessment for the business and follows set procedures for identifying risks. The risk assessment steps are as follows:

- The Compliance Team meets for a scheduled roundtable meeting with both partners and the Compliance Officer.
- The Compliance Team then discusses all potential risks, and the partners are responsible for deeming risks as acceptable or unacceptable:
    - Acceptable risks are to be discussed and given careful consideration
    - Unacceptable risks are to be included within the Risk Assessment Matrix
    - Unacceptable risks then undertake the steps documented with the Risk Assessment Matrix, such as categorization, who has access to the risk, risk scores, and mitigation

The Risk Assessment Matrix tracks, ranks, and details all identified risks to the business. The following details are listed for each risk:

- Category
- Hazard
- Risk
- Who has access to the risk
- Mitigation
- Probability Score
- Consequence Score
- Risk Score
- Date of Last Review

Information and Communication Systems

All information security-related policies and procedures are maintained within the Master Policy List, which is maintained by the Compliance Team. All policies are reviewed and approved at least annually with a revision tabled maintained at the beginning of the document and individual revision tables for each policy within. The internal Information Security Policy is included in the document and defines data and information classification, access controls, standard security software and tools approved for use, and security awareness training requirements.

All policies are distributed to employees during the onboarding process and major changes to the policies are communicated annually via email. Employees are required to acknowledge company policies upon significant changes to further communicate company expectations.

Vendor Management

AEC maintains a vendor management policy within the Master Policy List that provides vendor onboarding and due diligence processes for all third-party services that the organization may employ. The organization also addresses the risk of vendors as part of the risk assessment and during the onboarding process. When vendors are being selected, the organization considers cost-effectiveness, functionality, risk, financial viability, compliance, and performance. All vendors are evaluated at least annually and are tracked within the Vendor Tracking Spreadsheet.

Monitoring Controls

The organization sets a tone for compliance and expectations for employees within the Employee Handbook. The handbook also includes a discipline policy for all employees that detail discipline procedures up to termination for all personnel. All employees undergo a performance evaluation annually and management monitors performance throughout the year. Additionally, the organization monitors system performance health and service quality. The relevant personnel receive daily emails regarding the health, security, and compliance of the production Azure environment for review.

Changes to the System During the Period

There were no changes that are likely to affect report users' understanding of the construction contract administration platform system during the period from December 1, 2022, through November 30, 2023.

COMPLEMENTARY USER-ENTITY CONTROLS

AEC's services are designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at the user organization is necessary to achieve control objectives included in this report. AEC's management makes control recommendations to user organizations and provides the means to implement these controls in many instances. AEC also provides best practice guidance to clients regarding control element outside the sphere of AEC responsibility.

This section describes additional controls that should be in operation at user organizations to complement the AEC controls. Client Consideration recommendations include:

- User organizations should implement sound and consistent internal controls regarding general IT system access and system usage appropriateness for all internal user organization components associated with AEC.

- User organizations should practice removal of user accounts for any users who have been terminated and were previously involved in any material functions or activities associated with AEC's services.

- Transactions for user organizations relating to AEC's services should be appropriately authorized, and transactions should be secure, timely, and complete.

- For user organizations sending data to AEC, data should be protected by appropriate methods to ensure confidentiality, privacy, integrity, availability, and non-repudiation.

- User organizations should implement controls requiring additional approval procedures for critical transactions relating to AEC's services.

- User organizations should report to AEC in a timely manner any material changes to their overall control environment that may adversely affect services being performed by AEC.

- User organizations are responsible for notifying AEC in a timely manner of any changes to personnel directly involved with services performed by AEC. These personnel may be involved in financial, technical, or ancillary administrative functions directly associated with services provided by AEC.

- User organizations are responsible for adhering to the terms and conditions stated within their contracts with AEC.

- User organizations are responsible for developing, and if necessary, implementing a business continuity and disaster recovery plan (BCDRP) that will aid in the continuation of services provided by AEC.

The list of user organization control considerations presented above and those presented with certain specified control objectives do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations. Therefore, each client's system of internal controls must be evaluated in conjunction with the internal control structure described in this report.

SECTION IV:
TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

APPLICABLE TRUST SERVICES CRITERIA RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY

Although the applicable trust services criteria and related controls are presented in section IV, "Trust Services Categories, Criteria, Related Controls, and Tests of Controls," they are an integral part of AEC's system description throughout the period December 1, 2022, to November 30, 2023.

Security

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

Security refers to the protection of

i. information during its collection or creation, use processing, transmission, and storage and

ii. systems that use electronic information to process, transmit or transfer, and store information to enable the achievement of AEC's service commitments and system requirements. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Availability

The trust services criteria relevant to availability address the need for information and systems to be available for operation and use to achieve the service organization's service commitments and system requirements.

Availability refers to the accessibility of information used by AEC's systems, as well as the products or services provided to its customers. While the availability objective does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems), it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Confidentiality

The trust services criteria relevant to confidentiality address the need for information designated as confidential to be protected to achieve the service organization's service commitments and system requirements.

Confidentiality addresses AEC's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from AEC's control in accordance with management's objectives. Information is confidential if the custodian of the information is

required to limit its access, use, and retention and restrict its disclosure to defined parties. Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons.

Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Trust Services Criteria for the Security, Availability, and Confidentiality Categories			
Control Environment			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC1.1	The entity demonstrates a commitment to integrity and ethical values.		
CC1.1.1	Ethical and business expectations are demonstrated during the onboarding process, within policies, and during meetings.	Interviewed the Compliance Officer and the Founding Partner & Director of Platform Development and determined that organization establishes tone for compliance and security through onboarding, policies, and meetings Reviewed the Master Policy List (dated October 10, 2023) and verified that the organization maintains a Code of Ethics and Code of Conduct for executives and staff to follow Observed evidence of signed acknowledgements for the Master Policy List and the Employee Handbook and verified that the organization sets tone for compliance and security through onboarding, policy, and meetings	No Relevant Exceptions Noted
CC1.1.2	The Employee Handbook and the code of conduct contains employee behavior and performance expectations.	Interviewed the Compliance Officer and determined that the handbook is provided to employees during the onboarding and file share process and all new staff are required to sign the Employee Handbook, confidentiality agreement, and policies Reviewed the Official Employee Handbook (dated May 30, 2023) and verified that the organization has established an employee handbook that contains the following topics: • Employee conduct • Conflict of interests • Intellectual Property • Proprietary Information • Confidential Information • Performance Evaluations • Reprimand or Termination • Progressive Discipline	No Relevant Exceptions Noted

		• Receipt of handbook Reviewed the Master Policy List and verified that the organization maintains a Code of Ethics and Code of Conduct for executives and staff to follow Observed evidence of signed acknowledgements for the Master Policy List and the Employee Handbook and verified that the organization sets the tone for compliance and security through onboarding, policy, and meetings	
CC1.1.3	The organization maintains a formal onboarding process for all new hires.	Interviewed the Compliance Officer and determined that all new staff are onboarded with the Founding Partners and the Hiring Manager Reviewed the Internal Onboarding Checklist (dated June 27, 2023) and verified that the organization follows an internal onboarding checklist for new hires that collects information for resources, software, training, and telephone requirements Observed the new-hire checklist (dated October 11, 2023) and verified that the organization uses checklist for onboarding new hires to ensure that the organization obtains employee handbook, confidentiality, and policy agreements for all new hires	No Relevant Exceptions Noted
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
CC1.2.1	The Founding Partners are responsible for company oversight and monitoring internal control.	Interviewed the Compliance Officer and determined that the Founding Partners provide company oversight Observed the Organization Chart (dated November 6, 2023) and verified that it depicts clear reporting lines with both Founding Partners at the top	No Relevant Exceptions Noted
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		

CC1.3.1	The organization has established a Compliance Team that meets internally to discuss security and compliance weekly.	Interviewed the Compliance Officer and the Director of Platform Development and determined that both roles make up the Compliance Team that meets weekly to discuss security and compliance, and the Director of Platform Development is ultimately responsible for compliance and security Observed evidence of the weekly Compliance Team meeting and verified that the Compliance Team hosts a weekly meeting to discuss compliance and security	No Relevant Exceptions Noted
CC1.3.2	The organization has established clear reporting lines and defines company structure.	Observed the Organization Chart and verified that the organization maintains a typical hierarchical structure which outlines roles in the following keys areas: • Platform Innovation • Sales • Marketing • Support • Platform Development	No Relevant Exceptions Noted
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
CC1.4.1	Employees must complete required security training for security awareness and malware protections.	Interviewed the Compliance Officer and determined that security training is required for all staff upon hire and annually thereafter Observed completed security training documents (dated October 11, 2023) and verified that employees complete security training annually and the organization provides covert malware training	No Relevant Exceptions Noted
CC1.4.3	The organization requires departmental-dependent training.	Interviewed the Founding Partner & Director of Platform Development and determined that periodic developer training is conducted to keep up to date with industry best practices Interviewed the Compliance Officer and determined that additional training depends on the department, including	No Relevant Exceptions Noted

		developer, cybersecurity, and IT training Reviewed the Master Policy List and verified that the organization has a policy to train all personnel in cybersecurity Observed evidence of a standing weekly training session and verified that the organization conducts continuous training weekly Observed completed training (dated October 16, 2023) and verified that the organization conducts IT staff training	
CC1.4.4	All employees undergo a background check prior to hire.	Reviewed the Master Policy List and verified that the organization has an official policy to conduct background checks for candidates during hiring process, and background screenings may include the following: • Verification for identity • Employment education • Social Security number (SSN) • Residency Observed the new-hire checklist and verified that the organization conducts background checks for new employees	No Relevant Exceptions Noted
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
CC1.5.1	The Employee Handbook provides guidance for disciplinary actions up to termination.	Interviewed the Compliance Officer and the Founding Partner & Director of Platform Development and determined that organization implements discipline up to termination for non-compliance of company policies and the Employee Handbook Reviewed the Employee Handbook and verified that it outlines discipline actions up to termination for employees that are not meeting policy and handbook requirements	No Relevant Exceptions Noted

CC1.5.2	The organization monitors performance and health of its services to ensure operational quality.	Interviewed the Founding Partner & Director of Platform Development regarding standard operation procedures and determined that the organization receives daily emails regarding the health, security, and compliance of the production Azure environment Observed evidence of daily Azure emails within the audit period and verified that the organization monitors health, security, and compliance of the production Azure environment daily	No Relevant Exceptions Noted
CC1.5.3	All employees undergo an annual performance evaluation.	Interviewed the Compliance Officer and determined that performance reviews are completed annually Observed completed performance reviews for company personnel (3 out of 7) and verified that the organization monitors employee performance at least annually	No Relevant Exceptions Noted

Trust Services Criteria for the Security, Availability, and Confidentiality Categories			
Communication and Information			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
CC2.1.1	The organization maintains secure environments for processing and generating data.	Reviewed company network diagrams (dated October 12, 2023) and verified that the organization maintains a diagram that shows secure critical resources, services, and databases for the Azure production, staging, and development environments	No Relevant Exceptions Noted
CC2.1.2	The organization follows a data classification policy to identify receiving data.	Reviewed the Master Policy List and verified that the organization maintains a data classification policy to govern how data is handled and retained, and all data is classified under one of the following categories: • Public • Internal Use • Restricted • Confidential	No Relevant Exceptions Noted
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
CC2.2.1	The organization communicates information and security expectations to employees.	Interviewed the Compliance Officer and the Founding Partner & Director of Platform Development and determined that organization establishes tone for compliance and security through onboarding, policies, and meetings Observed evidence of signed acknowledgements for the Master Policy List and the Employee Handbook and verified that the organization sets tone for compliance and security through onboarding, policy, and meetings Observed the Weekly Meeting Agenda (dated September 22, 2023) and verified that the organization meets weekly to discuss the following topics: • Business	No Relevant Exceptions Noted

		• Risk • Compliance • Security	
CC2.2.2	Job descriptions are communicated to employees to outline the required roles and responsibilities.	Reviewed company job descriptions and verified that the organization maintains job descriptions for all critical positions Observed company job descriptions (dated October 11, 2023) and verified that the organization outlines roles and responsibilities in job descriptions	No Relevant Exceptions Noted
CC2.2.3	Confidentiality requirements are communicated to employees upon hire with a non-disclosure agreement (NDA).	Reviewed the Employee NDA and verified that the organization issues a standard NDA for employees to agree to not disclose all client or company information	No Relevant Exceptions Noted
CC2.2.4	All policies contained within the Master Policy List are accessible to employees within the company OneDrive.	Interviewed the Compliance Officer and determined that the Master Policy List is distributed in the company OneDrive policy folder for review reference Observed the OneDrive policy folder and verified that the organization distributes the Master Policy List to all personnel	No Relevant Exceptions Noted
CC2.2.5	The organization conducts incident response training bi-annually.	Interviewed the Compliance Officer and determined that the organization trains staff bi-annually on how to report incidents Reviewed the Master Policy List and verified that the organization has a policy that requires all users to be trained for reporting potential incidents in a timely manner Observed completed incident response plan training documents (dated February 2, 2023) and verified that the organization has conducted incident response team training	No Relevant Exceptions Noted
CC2.2.6	The organization hosts regular business continuity plan meetings.	Interviewed the Compliance Officer regarding business continuity and determined that the organization conducts business continuity plan meetings with all personnel to discuss	No Relevant Exceptions Noted

		potential disruptions to the organization Observed the slide deck from the most recent business continuity plan meeting and verified that the organization hosts regular business continuity plan meetings	
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.		
CC2.3.1	The organization has established a relevant method of communication for managing client issues and incidents.	Interviewed the Compliance Officer regarding external communications for client issues and incidents and determined that the organization provides an email for clients to communicate issues and incidents Observed the web application site and verified that the organization provides an email address for clients to communicate issues or incidents	No Relevant Exceptions Noted

Trust Services Criteria for the Security, Availability, and Confidentiality Categories			
Risk Assessment			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
CC3.1.1	The Founding Partners consider tolerances for risks.	Reviewed the Master Policy List and verified that the Founding Partners are responsible for determining which risks are acceptable or not	No Relevant Exceptions Noted
CC3.2	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	The organization meets to conduct the risk assessment process at least annually or upon significant changes.	Interviewed the Compliance Officer regarding the risk management program and determined that the organization meets at least annually or when major changes are needed Reviewed the Risk Matrix (dated October 5, 2023) and verified that the organization has conducted a risk assessment using Azure for their cloud hosting Reviewed the Master Policy List and verified that the organization has an official policy for the business to assess risks with business operations and partners Observed the Risk Matrix and verified that the organization has conducted a risk assessment for the following areas: • Accounting • Human Resources (HR) • Legal • Home Office • Fraud • Third parties • Development • IT • SaaS solution • Sales	No Relevant Exceptions Noted

CC3.2.2	The organization tracks, ranks, and details risks in a risk register.	Interviewed the Compliance Officer and determined that the risk policy is reviewed and a risk matrix is used to manage risk with compliance and partners Reviewed the Master Policy List and verified that risks are documented in a risk assessment matrix where each risk is scored and plans are documented for remediation Reviewed the Risk Matrix and verified that the organization has conducted a risk assessment within their Azure cloud production environment Observed the Risk Matrix and verified that the organization uses a five-by-five matrix scoring which scores risks based on probability, likelihood and severity and includes a list of assets, hazards, and risk score	No Relevant Exceptions Noted
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
CC3.3.1	The organization addresses the risk of fraud.	Interviewed the Compliance Officer regarding incidents of fraud and determined that the organization assesses the risk of fraud Observed the Risk Matrix and verified that the organization has conducted a risk assessment for fraud	No Relevant Exceptions Noted
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.		
CC3.4.1	The organization assesses change risks as part of the risk management process.	Reviewed the Master Policy List and verified that the organization reviews all risks if there is a significant change to business practices to address any related risks	No Relevant Exceptions Noted

Trust Services Criteria for the Security, Availability, and Confidentiality Categories			
Monitoring Activities			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.		
CC4.1.1	The organization undergoes an independent third-party security and compliance audit.	Interviewed the Compliance Officer and the Founding Partner & Director of Platform Development and determined that the organization undergoes compliance and security audits through a third party to confirm industry standards for information security have been applied Observed summarizing results from the most recent third party security audit and verified that the organization annually seeks a security and compliance audit to ensure effective controls	No Relevant Exceptions Noted
CC4.1.2	The organization undergoes external web application scans.	Interviewed the Compliance Officer regarding vulnerability management and determined that the organization uses CyberHunter to conduct monthly external application scanning Interviewed the Founding Partner & Director of Platform Development and determined that web application testing is conducted monthly Observed a sample of external web application scan results (10 of 12) and verified that the organization undergoes an external penetration test for the web application	No Relevant Exceptions Noted
CC4.2	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.		
CC4.2.1	Alerts are sent to IT contacts to investigate and remediate issues.	Interviewed the Compliance Officer and determined that Azure is configured to alert the Compliance Officer and the Founding Partner & Director of Platform Development for any issues within the environment	No Relevant Exceptions Noted

		Observed Azure network monitoring and verified that Azure is configured to alert the Compliance Officer and the Founding Partner & Director of Platform Development for any issues within the environment Observed evidence of daily Azure health and monitoring emails and verified that the organization has automated daily emails to inform the Compliance Officer and the Founding Partner & Director of Platform Development of any issues with their Azure environments security, health, and current operating status	

Trust Services Criteria for the Security, Availability, and Confidentiality Categories			
Control Activities			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC5.1	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	The organization has established an information security policy to ensure that risk mitigation activities are governed and documented.	Interviewed the Compliance Officer regarding the Information Security Policy determined that the Master Policy List contains all information security policies Reviewed the Master Policy List and verified that the organization maintains a collection of information security policies in a singular document that is approved by the Founding Partner and Director of Platform Development	No Relevant Exceptions Noted
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.		
CC5.2.1	The organization has developed a software development process that follows the Open Worldwide Application Security Project (OWASP) Top 10.	Interviewed the Founding Partner & Director of Platform Development and determined that the organization has an outlined software development lifecycle (SDLC) in policy Reviewed the Master Policy List and verified that the organization has a policy for the software development process that includes change management and follows the OWASP Top 10 to identify vulnerabilities Reviewed the Master Policy List and verified that the software development process is documented in Azure DevOps with the following phases: • Planning • Development • Deployment • Maintenance	No Relevant Exceptions Noted
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		

CC5.3.1	All policies are contained within the Master Policy List and must be approved by the relevant personnel.	Interviewed the Compliance Officer regarding the Information Security Policy determined that the Master Policy List contains all information security policies Reviewed the Master Policy List and verified that the organization maintains a collection of all information security policies in a singular document that is approved by the Founding Partner and Director of Platform Development Observed the revision history table and verified that the Master Policy List is approved by the Director of Platform Development	No Relevant Exceptions Noted
CC5.3.2	All policies must be reviewed and approved by the Compliance Team.	Interviewed the Compliance Officer and determined that all policies are developed, reviewed, and approved by the Compliance Team Reviewed the Master Policy List and verified that the organization maintains a collection of all information security policies in a singular document that is approved by the Founding Partner and Director of Platform Development	No Relevant Exceptions Noted

Trust Services Criteria for the Security, Availability, and Confidentiality Categories			
Logical and Physical Access Controls			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
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	The organization uses Microsoft Entra to manage access controls and tracks controls with a ticketing system.	Interviewed the Compliance Officer and determined that internal access is controlled using Microsoft 365, which is administered by the Compliance Officer and the Founding Partner & Director of Platform Development Observed user access controls and verified that the organization enforces access control using Microsoft Entra and Microsoft Entra controls Azure and Microsoft user access to systems and resources Observed evidence of access controls and verified that Builterra has access controls that are customizable through tickets from clients	No Relevant Exceptions Noted
CC6.1.2	Encryption keys are managed within the Azure Key Vault that only authorized personnel can access.	Interviewed the Compliance Officer and determined that all encryption keys are maintained using Azure Key Vault Reviewed the Master Policy List and verified that the organization has a policy for encryption standards, key creation, and maintaining key confidentiality Observed the Azure Key Vault configuration (dated November 6. 2023) and verified that the organization maintains keys using Azure Key Vault and access to the vault is limited to the Founding Partner & Director of Platform Development and Compliance Officer Observed the Access Key Inventory (dated November 3, 2023) and verified	No Relevant Exceptions Noted

		that the organization tracks keys and certificates within a spreadsheet that lists the last rotation date	
CC6.1.3	All data at rest must be encrypted.	Interviewed the Compliance Officer and determined that all data is stored in the Azure cloud environment and must be encrypted using AES 256 Observed the Cloudflare web application firewall configuration and verified that the organization implements Transport Layer Security (TLS) 1.2 with AES 256 and SHA 256 for encryption	No Relevant Exceptions Noted
CC6.1.4	The organization tracks encryption keys to ensure that keys are securely managed and rotated.	Observed the Access Key Inventory and verified that the organization tracks keys and certificates within a spreadsheet that lists the last rotation date, and all keys and certificates have been rotated within the last 12 months	No Relevant 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.		
CC6.2.1	The organization maintains a password policy that details requirements for employees.	Reviewed the Master Policy List and verified that the organization has an official policy for password configuration that details the following password requirements: • Minimum length of 10 characters • Multi-factor authentication (MFA) • Common passwords are not allowed • Complex passwords Observed the password configurations and verified that the organization enforces the following password requirements: • Complex passwords • MFA • Minimum length of 12 characters • Last five passwords remembered • Account lockout after five failed attempts	No Relevant Exceptions Noted

CC6.2.3	Access controls are issued during the onboarding process.	Interviewed the Compliance Officer regarding access control systems and determined that Builterra access controls are set during onboarding by either the support team or the client Reviewed the Master Policy List and verified that access is controlled by the Founding Partners and HelpDesk	No Relevant 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	The organization assigns access based on role.	Interviewed the Compliance Officer and determined that new user access is granted based on role and approved by the Founding Partner & Director of Platform Development Reviewed the Master Policy List and verified that the organization maintains a formal access policy that requires access permissions to be based on need-to-share rather than need-to-know for confidential data	No Relevant Exceptions Noted
CC6.3.2	User access is revoked upon employee termination.	Interviewed the Compliance Officer and determined that access is removed immediately upon terminations and all terminations are conducted with the approval of the Founding Partner & Director of Platform Development Reviewed the Employee Termination Checklist and verified that the organization follows a template for employee termination that collects the following information: • Date • Manager • Department • Reason for resignation or termination • Logical access resources that must be disabled	No Relevant Exceptions Noted
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.		

CC6.4.1	The organization restricts access to physical media and destroys it when it is no longer needed.	Interviewed the Compliance Officer and determined that the organization maintains a media destruction policy Reviewed the Master Policy List and verified that the organization has a policy to destroy physical media such as paper, CDs and DVDs, USB Drives, hard drives, and other storage which may contain sensitive information *Note: No data was disposed of during the audit period.*	Not Tested
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	The organization securely disposes of data on company workstations and systems when it is no longer in use.	Interviewed the Compliance Officer regarding data disposal and determined that the organization maintains unused workstations and wipes devices before distributing them to employees Reviewed the Master Policy List and verified that the organization must digitally destroy media, such as hard drives and removable media, that contains company information based on National Institute of Standards of Technology (NIST) best practices *Note: No data was disposed of during the audit period.*	Not Tested
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
CC6.6.1	MFA is required to login to the system environments.	Observed a login demonstration to each environment and verified that the organization has implemented MFA for login Observed a demonstration of the Azure platform and verified that the organization has implemented MFA for Azure environment login Observed MFA configurations and verified that MFA is required for Microsoft and Azure	No Relevant Exceptions Noted

CC6.6.2	The organization restricts inbound and outbound traffic and redirects HTTP.	Observed the Cloudflare web application firewall and verified that the organization controls inbound and outbound traffic, and all HTTP is redirected to HTTPS Observed the Azure remote connection IP list (November 9, 2023) and verified that the organization limits access to the Azure production environment using whitelisted IPs for employee systems Observed a login demonstration to Microsoft and verified that organization login procedures require encryption using HTTPS	No Relevant Exceptions Noted
CC6.6.3	Accounts are locked after five failed login attempts.	Observed Microsoft and Azure account configurations and verified that user accounts are locked for five minutes after five failed login attempts Observed the password configurations and verified that accounts are locked after five failed attempts	No Relevant Exceptions Noted
CC6.6.4	The organization has installed a web application firewall.	Observed the Cloudflare web application firewall configuration and verified that the organization has implemented a web application firewall to protect against distributed denial-of-service (DDOS) attacks and redirects ports and protocols for the Builterra application	No Relevant 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.		
CC6.7.1	Secure encryption standards are required for data in transit.	Interviewed the Compliance Officer regarding data security and determined that all traffic is encrypted using TLS 1.2 HTTPS using Cloudflare Reviewed company network diagrams and verified that the organization maintains a diagram that shows secure critical resources, services, and databases for the Azure production, staging, and development environments	No Relevant Exceptions Noted

		Observed the Cloudflare web application firewall configuration and verified that the organization implements TLS 1.2 with AES 256 and SHA 256 for encryption	
CC6.7.2	The development, staging, and production environments are separate.	Interviewed the Founding Partner & Director of Platform Development and determined that the organization maintains separate environments for development, staging, and production Observed the Server Diagram (dated October 2023) and verified that the organization maintains separate staging, development, and production environments	No Relevant Exceptions Noted
CC6.7.3	The organization has secure email configurations.	Observed the Microsoft email protection configuration and verified that the organization has implemented email protection for potentially harmful attachments and links	No Relevant Exceptions Noted
CC6.7.4	The organization restricts the use of removeable media for all systems.	Observed Microsoft Intune configurations and verified that the organization has blocked removable media for all seven Windows systems	No Relevant 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.		
CC6.8.1	Devices and systems are managed with Microsoft Intune.	Interviewed the Compliance Officer and determined that hardening standards are enforced using Microsoft Intune and Security Center Reviewed the Master Policy List and verified that systems are managed with Microsoft Intune	No Relevant Exceptions Noted
CC6.8.2	The organization implements network segmentation.	Observed evidence of the Azure virtual network configuration (dated October 14, 2023) and verified that the organization segments virtual networks within the Azure environment Observed Microsoft Intune and Defender configurations and verified that logs are maintained for Microsoft Defender in Azure	No Relevant Exceptions Noted

CC6.8.3	The organization has installed antivirus and anti-malware software.	Reviewed the Master Policy List and verified that the organization has a policy to maintain patching, antivirus, and anti-malware software that is managed by Microsoft Defender Observed Microsoft Intune and Defender configurations and verified that the organization has implemented Intune and Defender to protect systems against malware and antivirus protections for all seven Windows systems	No Relevant Exceptions Noted

Trust Services Criteria for the Security, Availability, and Confidentiality Categories			
System Operations			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
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	The organization uses Azure Sentinel for security orchestration, automation, and response (SOAR).	Observed evidence of the Azure Sentinel configuration (dated November 1, 2023) and verified that the organization has implemented Sentinel for SOAR to protect the Azure cloud environment	No Relevant Exceptions Noted
CC7.1.2	The organization conducts vulnerability scans.	Interviewed the Compliance Officer regarding vulnerability management and determined that the organization uses Nessus Essentials to scan workstations Observed a sample of external scans reports (10 out of 12) and verified that the organization manages vulnerabilities using third-party and industry standard tools to identify and remediate vulnerabilities Observed internal scan reports and verified that the organization conducts internal vulnerability scans and performs remediation activities	No Relevant Exceptions Noted
CC7.1.3	The organization follows a set hardening and configuration policy that is reviewed annually.	Interviewed the Compliance Officer regarding hardening standards and determined that configuration standards are reviewed annually and are outlined in the hardening standard policy Observed the monthly configuration review of the Security Center dashboard (dated October 20, 2023) and verified that the Founding Partner & Director of Platform Development conducts a monthly Azure configuration review to ensure best practices are implemented	No Relevant 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	The organization uses Azure Monitoring and Sentinel for monitoring the environment.	Interviewed the Compliance Officer regarding network monitoring and determined that the organization implements Azure Monitoring and Azure Sentinel for the logging and monitoring of the Azure environments Observed Azure network monitoring and verified that the organization implements Azure Monitoring and Azure Sentinel for logging and monitoring of the Azure environments	No Relevant 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.		
CC7.3.1	The Compliance Officer and the Founding Partner & Director of Platform Development receive monitoring alerts for any issues within the Azure environment.	Interviewed the Compliance Officer and determined that Azure is configured to alert the Compliance Officer and the Founding Partner & Director of Platform Development for any issues within the environment Observed Azure network monitoring and verified that Azure is configured to alert the Compliance Officer and the Founding Partner & Director of Platform Development for any issues within the environment Observed evidence of daily Azure health and monitoring emails and verified that the organization has automated daily emails to inform the Compliance Officer and the Founding Partner & Director of Platform Development of any issues with their Azure environments security, health, and current operating status	No Relevant 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	The organization maintains an incident response policy.	Interviewed the Compliance Officer regarding incident response and determined that the organization	No Relevant Exceptions Noted

		maintains an official plan to respond to incidents Reviewed the Master Policy List and verified that it contains procedures for incident reporting and response Reviewed the Incident Reporting Policy Checklist and verified that the Founding Partner & Director of Platform Development is the incident response team member	
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.		
CC7.5.1	The organization performs system patches for immediate remediation.	Interviewed the Compliance Officer and determined that remediation is conducted and systems are patched as soon as practical and the organization immediately updates the application if it impacts the Builterra application Reviewed the Master Policy List and verified that the organization has an official policy to patch systems as soon as practical and to immediately update the application if it impacts the Builterra application, and patching is managed and implemented with Intune Observed the system patching status for all systems and verified that company systems are updated through patching deployments	No Relevant Exceptions Noted
CC7.5.2	The organization uses tools to remediate findings from vulnerability scans and penetration tests.	Interviewed the Compliance Officer regarding vulnerability management and determined that the organization uses Nessus Essentials to scan workstations and uses CyberHunter to conduct monthly external application scanning Observed external web application scan results (10 out of 12) and verified that the organization is managing vulnerabilities using third-party and industry standard tools to identify and remediate vulnerabilities	No Relevant Exceptions Noted

CC7.5.3	The organization tests the incident response plan at least annually.	Reviewed the Master Policy List and verified that incident response must be tested at least annually Observed the incident response testing report (dated October 2023) and verified that the organization has conducted a tabletop testing exercise for the incident response plan	No Relevant Exceptions Noted

Trust Services Criteria for the Security, Availability, and Confidentiality Categories			
Change Management			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.		
CC8.1.1	Azure DevOps is used to for versioning and source control.	Interviewed the Founding Partner & Director of Platform Development and determined that Azure DevOps is used for source control, versioning, and deployment to the Azure environments Observed four changes completed in Azure DevOps and verified that the organization conducts and documents change management in Azure DevOps	No Relevant Exceptions Noted
CC8.1.2	All changes must be reviewed and approved before being implemented.	Reviewed the Master Policy List and verified that the organization maintains a change management policy for systems and software development that requires all changes to be reviewed, assessed for impact, and approved before deployment	No Relevant Exceptions Noted

Trust Services Criteria for the Security, Availability, and Confidentiality Categories			
Risk Mitigation			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
CC9.1.1	The organization has a current cybersecurity insurance plan.	Reviewed a cybersecurity insurance invoice (dated June 3, 2023) and verified that the organization has five million in cybersecurity insurance through June 3, 2024	No Relevant Exceptions Noted
CC9.2	The entity assesses and manages risks associated with vendors and business partners.		
CC9.2.1	The organization has established a vendor management policy and tracks all vendors.	Interviewed the Compliance Officer regarding vendor management and determined that the organization has a policy to review current vendors once a year and considers the relative risks prior to engagement with new critical third parties Reviewed the Master Policy List and verified that the organization maintains a vendor management policy that outlines how current and potential vendors must be evaluated, selected, engaged with, and managed based on cost, risk, and performance Observed the Vendor Tracking Spreadsheet and verified that the organization maintains a list of third parties	No Relevant Exceptions Noted
CC9.2.2	The organization evaluates all vendors to ensure compliance and service expectations are met.	Reviewed the Master Policy List and verified that vendor compliance with industry and regulatory standards must be evaluated and ongoing monitoring must be conducted to determine if expectations and service-level agreements (SLAs) are being met Observed the Vendor Tracking Spreadsheet (dated October 16, 2023) and verified that the organization conducts annual due diligence for vendors used for the Builterra platform	No Relevant Exceptions Noted

Additional Criteria for Availability			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
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	The organization monitors and logs the Azure environments to maintain performance health and quality.	Interviewed the Compliance Officer regarding network monitoring and determined that the organization implements Azure Monitoring and Azure Sentinel for the logging and monitoring of the Azure environments Observed Azure network monitoring and verified that the organization implements Azure Monitoring and Azure Sentinel for logging and monitoring of the Azure environments	No Relevant Exceptions Noted
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.		
A1.2.1	The organization performs regular backups for all systems and information.	Interviewed the Compliance Officer regarding backups and determined that the organization maintains 35 days of full daily backups and maintains three years of a monthly backup in Azure Reviewed the Master Policy List and verified that the organization has a policy for backup and recovery to prevent the loss of data in case of accidental deletion, corruption, failure, or disaster Observed Azure backups and verified that the organization maintains 35 days of full daily backups and maintains three years of a monthly backup in Azure	No Relevant Exceptions Noted
A1.2.2	The organization encrypts all backup data.	Reviewed the Master Policy List and verified that data backup must be stored with AES 256 encryptions Observed Azure backup configurations and verified that all backups are encrypted with AES 256	No Relevant Exceptions Noted

A1.2.3	The organization maintains geographically diverse backups.	Observed Azure backup configurations and verified that the organization maintains geographically diverse backups in the Azure environment	No Relevant Exceptions Noted
A1.2.4	The organization has established a business continuity plan.	Reviewed the Master Policy List and verified that the organization has an official policy to address risks to the business and to recover from disasters that impact the Builterra platform Reviewed the Master Policy List and verified that the policy includes the following: • Risk assessment • Business impact analysis • Annual testing Reviewed the Master Policy List and verified that the policy includes the following: • Roles and responsibilities • Restoration plans • Priorities • Cost of downtime	No Relevant Exceptions Noted
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.		
A1.3.1	The organization performs restoration tests for backups at least annually.	Interviewed the Compliance Officer and determined that restoration testing is conducted annually Reviewed the Master Policy List and verified that the organization confirms quarterly backup verification through periodic testing Observed evidence of restoration testing and verified that the organization has tested restoration of the SQL database	No Relevant Exceptions Noted
A1.3.2	The organization tests the business continuity plan.	Interviewed the Compliance Officer and determined that the organization tests the business continuity plan and testing includes account system disruptions for QuickBooks and Salesforce Observed evidence of business continuity plan testing (dated November 3, 2023) and verified that	No Relevant Exceptions Noted

		the organization has tested the ability to continue to deliver services when a critical function is unavailable Observed evidence of a completed business continuity plan tabletop exercise (dated September 5, 2023) and verified that the organization has conducted tabletop business continuity plan testing for power outages, unavailability of Salesforce, and QuickBooks service outage	

Additional Criteria for Confidentiality			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.		
C1.1.1	The organization has established a data retention policy.	Reviewed the Master Policy List and verified that the organization maintains a data retention policy based on classification level: • Public: Seven years • Internal use: Seven years • Restricted: Only retained when necessary and needed • Confidential: Only retained when necessary and needed	No Relevant Exceptions Noted
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.		
C1.2.1	The organization securely disposes of confidential data on company workstations and systems when it is no longer in use.	Interviewed the Compliance Officer regarding data disposal and determined that the organization maintains unused workstations and wipes devices before distributing them to employees Reviewed the Master Policy List and verified that the organization must digitally destroy media, such as hard drives and removable media, that contains company information based on NIST best practices *Note: No data was disposed of during the audit period.*	Not Tested