

JOHANSON GROUP

System and Organization Controls (SOC) 2 Type II Report on Management's Description of its The Credit Bureau Platform

And the Suitability of Design of Controls and Test of Operating Effectiveness of Controls Placed in Operation Relevant to Security

For the Period
December 18, 2025 to March 17, 2026

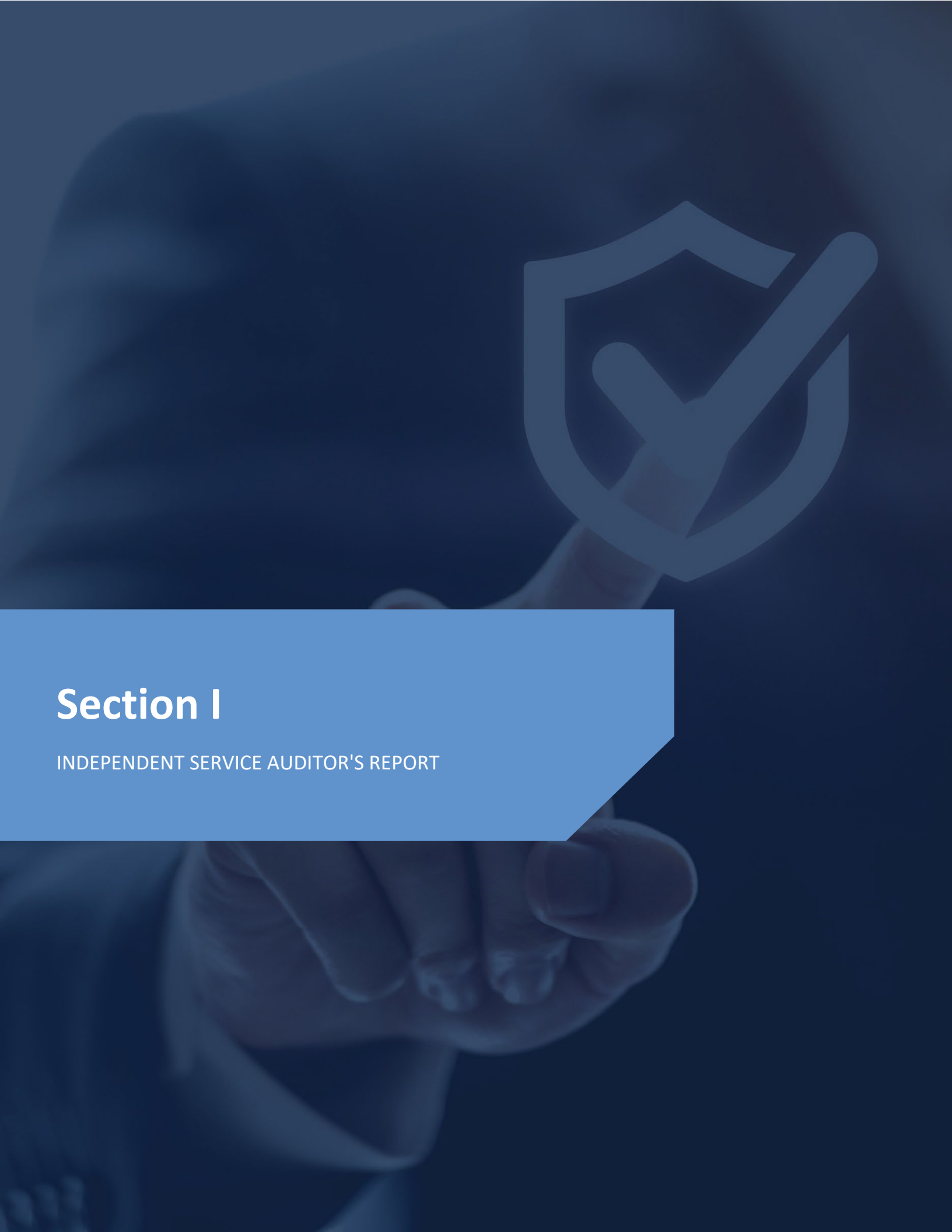
Together with Independent Service Auditor's Report

CONGRUIT

TABLE OF CONTENTS

I.	Independent Service Auditor's Report	3
II.	Assertion of Congruit Credit Management	7
III.	Description of The Credit Bureau Platform	9
IV.	Description of Test of Controls and Results Thereof	21





Section I

INDEPENDENT SERVICE AUDITOR'S REPORT

Congruit Credit

Scope

We have examined Congruit Credit's accompanying description of its The Credit Bureau Platform (system) titled "Description of The Credit Bureau Platform" throughout the period December 18, 2025 to March 17, 2026 (description) based on the criteria for a description of a service organization's system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (With Revised Implementation Guidance — 2022)* in AICPA, *Description Criteria*, (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period December 18, 2025 to March 17, 2026, to provide reasonable assurance that Congruit Credit's service commitments and system requirements were achieved based on trust services criteria relevant to Security principles (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*.

Congruit Credit uses a subservice organization, to provide data center facility and hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Congruit Credit, to achieve Congruit Credit's service commitments and system requirements based on the applicable trust services criteria. The description presents Congruit Credit's controls, the applicable trust services criteria and the types of complementary subservice organization controls assumed in the design of Congruit Credit'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 Congruit Credit, to achieve Congruit Credit's service commitments and system requirements based on the applicable trust services criteria. The description presents Congruit Credit's controls, the applicable trust services criteria and the complementary user entity controls assumed in the design of Congruit Credit'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

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

Service Auditor's Responsibilities

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

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 and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Test of Controls

The specific controls tested and the nature, timing, and results of those tests are presented in the section of our report titled "Description of Test of Controls and Results Thereof."

Opinion

In our opinion, in all material respects,

a. The description presents Congruit Credit's The Credit Bureau Platform (system) that was designed and implemented throughout the period December 18, 2025 to March 17, 2026 in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period December 18, 2025 to March 17, 2026, to provide reasonable assurance that Congruit Credit's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period and if the subservice organization and user entities applied the complementary controls assumed in the design of Congruit Credit's controls throughout the period.

c. The controls stated in the description operated effectively throughout the period December 18, 2025 to March 17, 2026, to provide reasonable assurance that Congruit Credit'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 Congruit Credit's controls operated effectively throughout the period.

Restricted Use

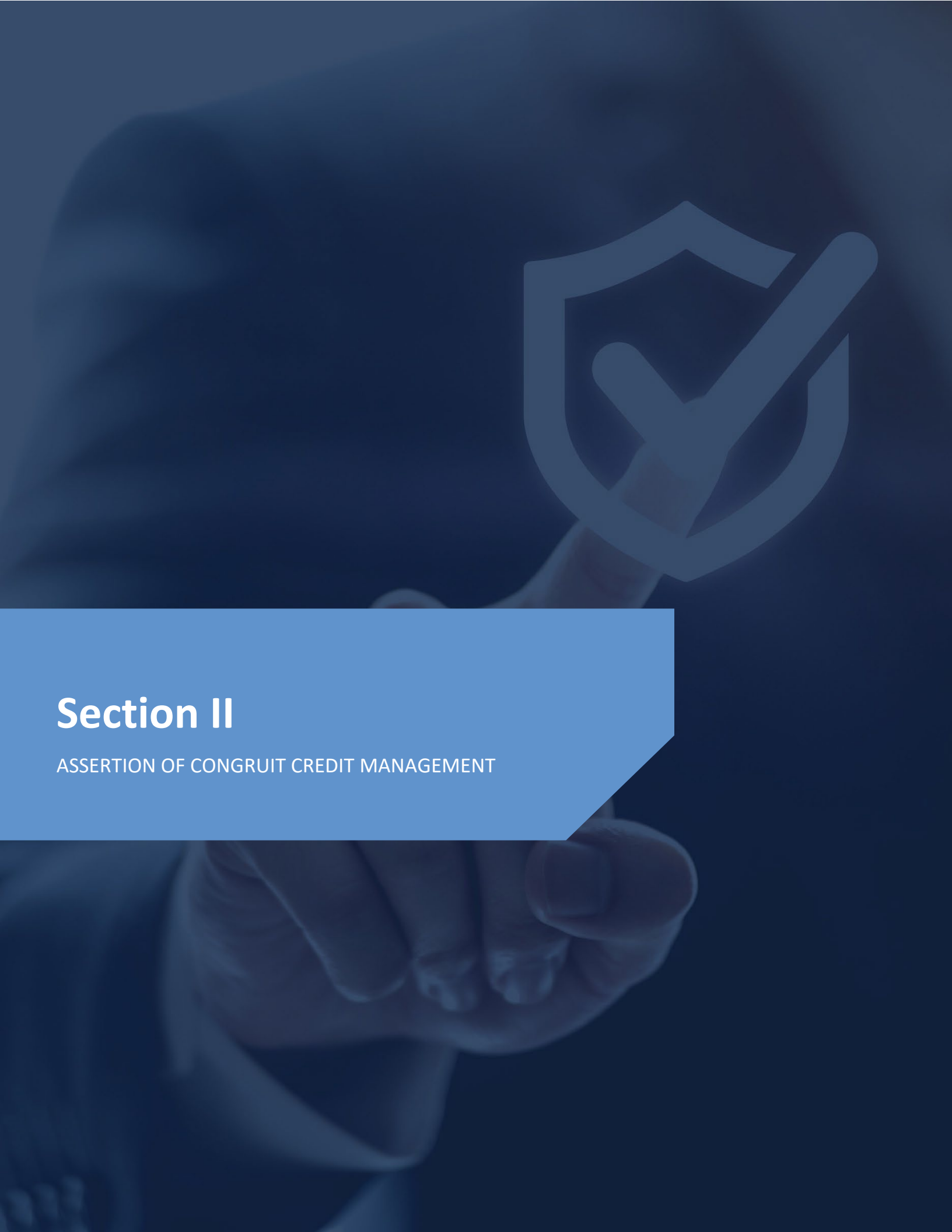
This report, including the description of tests of controls and results thereof in the section of our report titled “Description of Test of Controls and Results Thereof” is intended solely for the information and use of Congruit Credit; user entities of Congruit Credit's The Credit Bureau Platform during some or all of the period December 18, 2025 to March 17, 2026, business partners of Congruit Credit subject to risks arising from interactions with the Congruit Credit's processing 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, 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.

JohansonGroup LLP

Colorado Springs, Colorado
April 15, 2026



Section II

ASSERTION OF CONGRUIT CREDIT MANAGEMENT

We have prepared the accompanying description of Congruit Credit's "Description of The Credit Bureau Platform" for the period December 18, 2025 to March 17, 2026, (description) based on the criteria for a description of a service organization's system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (With Revised Implementation Guidance — 2022)* in AICPA, *Description Criteria* (description criteria). The description is intended to provide report users with information about Congruit Credit's The Credit Bureau Platform (system) that may be useful when assessing the risks arising from interactions with Congruit Credit's system, particularly information about system controls that Congruit Credit 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 (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*.

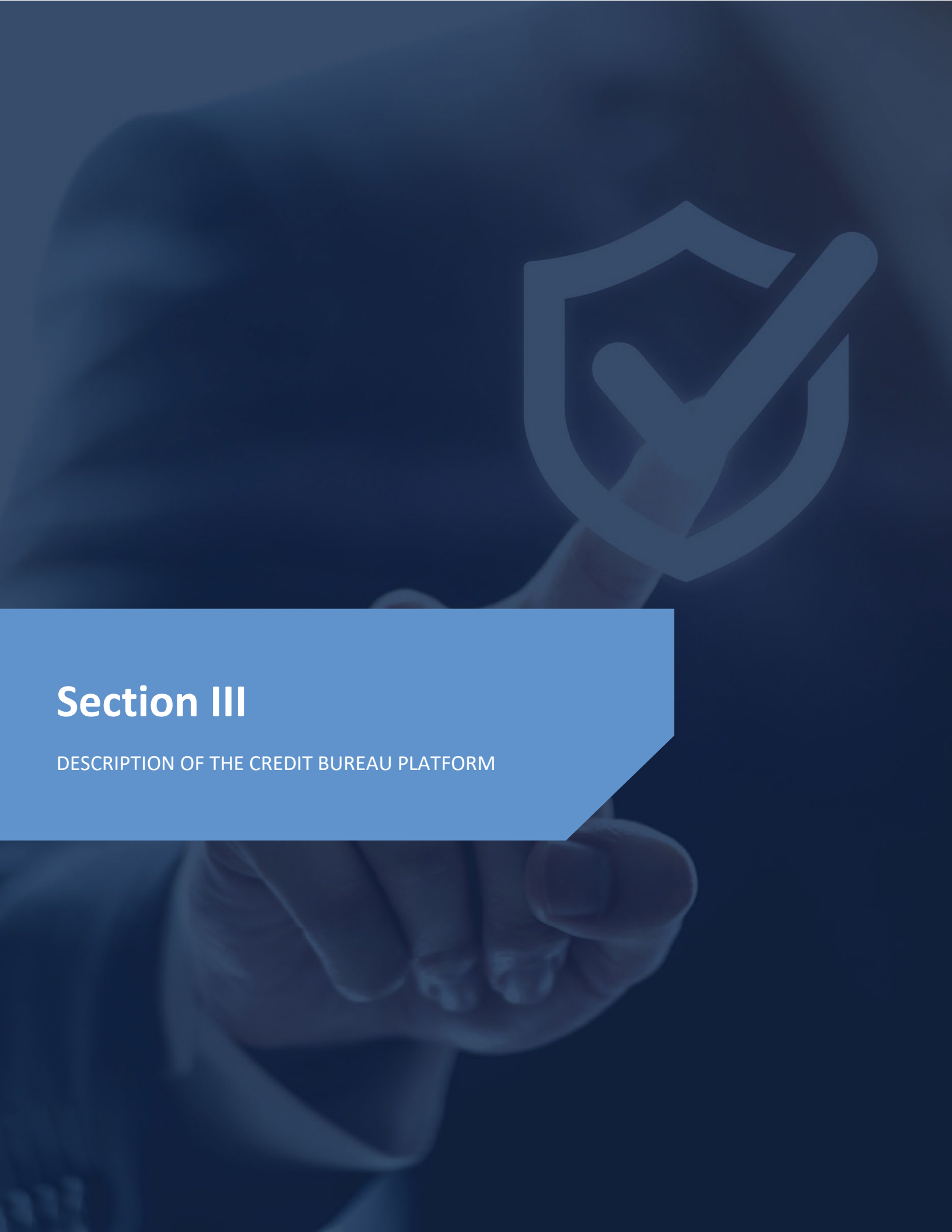
Congruit Credit uses a subservice organization to provide data center facility and hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Congruit Credit, to achieve Congruit Credit's service commitments and system requirements based on the applicable trust services criteria. The description presents Congruit Credit's controls, the applicable trust services criteria and the types of complementary subservice organization controls assumed in the design of Congruit Credit'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 Congruit Credit, to Congruit Credit's service commitments and system requirements based on the applicable trust services criteria. The description presents Congruit Credit's controls, the applicable trust services criteria and the complementary user entity controls assumed in the design of Congruit Credit's controls.

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

a. The description presents Congruit Credit's The Credit Bureau Platform (system) that was designed and implemented throughout the period December 18, 2025 to March 17, 2026, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period December 18, 2025 to March 17, 2026, to provide reasonable assurance that Congruit Credit'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 Congruit Credit's controls throughout that period.
c. The controls stated in the description operated effectively throughout the period December 18, 2025 to March 17, 2026, to provide reasonable assurance that Congruit Credit'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 Congruit Credit's controls operated effectively throughout that period.

Congruit Credit Management
April 15, 2026



Section III

DESCRIPTION OF THE CREDIT BUREAU PLATFORM

COMPANY BACKGROUND

Congruit was incorporated as a Delaware C Corp on 9/10/2024 by Tim Ranney. The founders are described as:

- Tim Ranney, serial subprime entrepreneur, who founded Clarity Services in 2008 which was acquired by Experian in 2017. Tim is CEO at Congruit.
- Chris Lamb, technology executive who has founded and worked in several startups in financial and advertising services. He was also VP Engineering at Clarity Services. Chris is CTO at Congruit.
- Jim James, technology executive who has founded and worked in several startups in travel and financial services. He was CTO at Clarity Services. Jim is CIO at Congruit.
- All three live in Saint Petersburg, FL. However, most staff live in other states and the company is remote-first and does not have a dedicated office network or environment.

DESCRIPTION OF SERVICES OVERVIEW OR SERVICES PROVIDED

Congruit's core product, the credit bureau platform, is a SaaS which provides:

- credit reports to lenders who want to make loans to consumers
- lender submits a consumer's loan application to Congruit's API
- Congruit creates a credit report for that consumer and returns it to the lender
- Congruit stores the credit inquiry and associated data

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Congruit makes service commitments to its customers, their consumers, and various laws administered by federal and state regulatory agencies. The system services are subject to the Security, Confidentiality, Availability, Processing Integrity, and Privacy commitments established internally for its services. Commitments to user entities are documented and communicated principally through contracts.

Confidentiality commitments include:

- The use of encryption technologies to protect system data both at rest and in transit
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties
- Confidential information must be used only for the purposes explicitly stated in agreements between Congruit and user entities.

Availability commitments include:

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components
- Responding to customer requests in a reasonably timely manner
- Business continuity and disaster recovery plans that include detailed instructions, recovery time objectives, roles, and responsibilities
- Operational procedures supporting the achievement of availability commitments to user entities

Security Commitments

Security commitments include:

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role

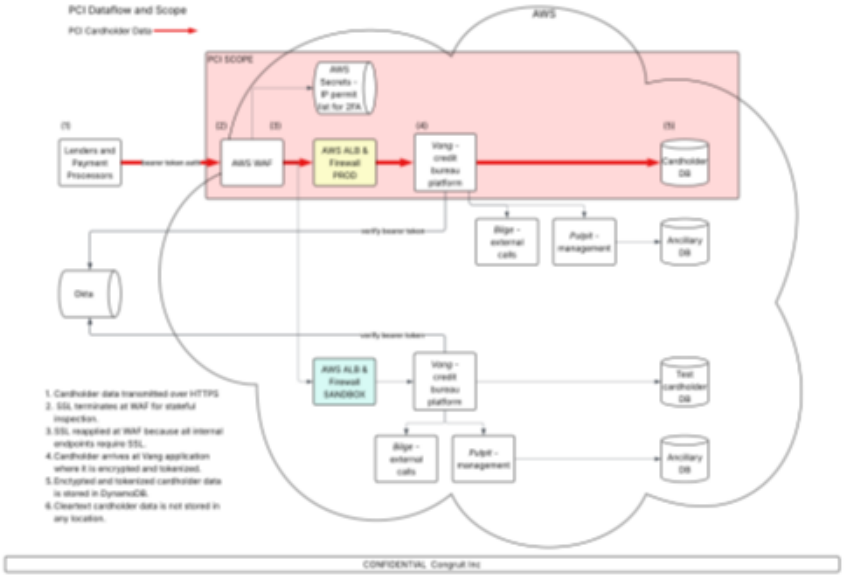
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system
- Regular vulnerability scans over the system and network, and penetration tests over the production environment
- Operational procedures for managing security incidents and breaches, including notification procedures
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal
- Uptime availability of production systems

Components of the System

- *Infrastructure* – The collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the service organization used to provide the services.
- *Software* - The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.
- *People* - The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- *Data* – The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- *Procedures* – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

Infrastructure

Congruit is entirely implemented in the cloud. There is no physical inventory except for staff laptops. The network is described in this diagram:



Primary Infrastructure		
Hardware	**Type**	**Purpose (optional)**
AWS S3, Redshift, Dynamo DB, Kenesis, etc.	Cloud hosting	cloud services for all operational portions of our service using VPC that protects the network from unauthorized external access
AWS Guard Duty	Security	Perimeter security and data exfiltration
AWS WAF	Security	Web Application Firewall

Software

Primary Software		
System/Application	**Operating System**	**Purpose**
Pager Duty	Event Management	Pages on-call engineers
Instatus	Uptime	Uptime monitoring service
Auth0 (Okta)	Authentication	Managed MFA access for onboard authorized users
Jira	Ticketing	Code governance and control
GitHub	Source control	Source code management and security, deployment pipelines
Cobalt	Pen testing and scanning	Vulnerability Control
Confluence	Communications	Internal Documentation
Entra (O365)	Active directory	Identity Management
Gusto	Payroll	Payroll and training
SharePoint	Communication	Internal Documentation
Sentry	Code Bug Tracking	Production Failure Monitoring
Slack	Communication	Internal Messaging

People

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

Congruit has a staff of approximately 10 organized in the following functional areas:

- Engineering
- Sales

- Product and Analytics
- Backoffice

Management - Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.

CEO - Tim Ranney
Controller - Cathi Jackson
CTO - Chris Lamb
Sales - Paul Mitchell

Operations - Responsible for maintaining the availability of production infrastructure, and managing access and security for production infrastructure. Only members of the Operations team have access to the production environment. Members of the Operations team may also be members of the Engineering team.

Information Technology - Responsible for managing laptops, software, and other technology involved in employee productivity and business operations.

Product Development - Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality.

Data

Data at Congruit consists of:

- credit inquiries from lenders
- posts on consumer credit files
- furnished data from lenders and other partners

Category	Description	Examples
Public	Public information is not confidential and can be made public without any implications for Congruit	• Press releases • Public website
Internal	Access to internal information is approved by management and is protected from external access.	• Internal memos • Design documents • Product specifications • Correspondences
Customer data	Information received from customers for processing or storage by Congruit. Congruit must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Customer operating data • Customer PII • Consumer PII • Anything subject to a confidentiality agreement with a customer
Company data	Information collected and used by Congruit to operate the business. Congruit must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Legal documents • Contractual agreements • Employee PII • Employee salaries

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

All employees and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, Congruit has policies and procedures in place for the secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

PROCESSES AND PROCEDURES

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by appropriate management. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

Physical Security

Congruit's production servers are maintained by AWS. The physical and environmental security protections are the responsibility of AWS. Congruit reviews the attestation reports and performs a risk analysis of AWS on at least an annual basis.

Logical Access

Congruit provides employees and contractors access to infrastructure via a role-based access control system, to ensure uniform, least privilege access to identified users and to maintain simple and repeatable user provisioning and deprovisioning processes. Access to these systems is split into two levels: User, and No Access. User access and roles are reviewed on an annual basis to ensure least privilege access.

Management is responsible for provisioning access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing Congruit's policies, completing security training. These steps must be completed with 5 days of hire. When an employee is terminated, the CIO is responsible for deprovisioning access to all in scope systems within 3 days for that employee's termination.

Computer Operations - Backups

Customer data is backed up and monitored by the Engineering team for completion and exceptions. If there is an exception the CTO performs troubleshooting to identify the root cause and either rerun the backup or as part of the next scheduled backup job.

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

Computer Operations - Availability

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

Congruit internally monitors all applications, including databases, and cloud storage to ensure that service delivery matches SLA requirements.

Congruit utilizes vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open-source dependencies and maintains an internal SLA for responding to those issues.

Change Management

Congruit maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Data Communications

Congruit has elected to use AWS to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. AWS simplifies our logical network configuration by providing an effective firewall around all Congruit's application containers, with the only ingress from the network via HTTPS connections to API endpoints.

AWS also automates the provisioning and deprovisioning of containers to match the desired configuration; if an application container fails, it will be automatically replaced, regardless of whether that failure is in the application or on underlying hardware.

Congruit uses an external security firm to perform quarterly vulnerability scans and annual penetration testing} to look for unidentified vulnerabilities, and the product engineering team responds to any issues identified via the regular incident response and change management process.

BOUNDARIES OF THE SYSTEM

The scope of this report includes the credit bureau platform operated in AWS facilities but carves out the infrastructure provided by AWS.

THE APPLICABLE TRUST SERVICES CRITERIA AND THE RELATED CONTROLS

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 entity to meet its objectives. 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.

CONTROL ENVIRONMENT

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Congruit's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Congruit's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for select employees in elevated risk areas as a component of the hiring process.

Commitment to Competence

Congruit's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

Management's Philosophy and Operating Style

The Congruit management team must balance two competing interests: continuing to grow and develop in a cutting edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly-sensitive data and workflows our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way Congruit can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally any regulatory changes that may require Congruit to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business.

Organizational Structure and Assignment of Authority and Responsibility

Congruit's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Congruit's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

Human Resource Policies and Practices

Congruit's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Congruit's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

RISK ASSESSMENT PROCESS

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

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Congruit's system; as well as the nature of the components of the system result in risks that the criteria will not be met. Congruit addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Congruit's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

INFORMATION AND COMMUNICATION SYSTEMS

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

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

Structured data is communicated internally via SaaS applications and project management tools. Finally, Congruit uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

MONITORING CONTROLS

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

On-Going Monitoring

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

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

Reporting Deficiencies

Our internal risk management tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

CHANGES TO THE SYSTEM

No significant changes have occurred to the services provided to user entities in the last 3 months preceding the end of the review date.

INCIDENTS

No significant incidents have occurred to the services provided to user entities in the last 3 months preceding the end of the review date.

CRITERIA NOT APPLICABLE TO THE SYSTEM

All relevant trust services criteria (Security) were applicable to The Credit Bureau Platform's.

SUBSERVICE ORGANIZATIONS

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

SUBSERVICE DESCRIPTION OF SERVICES

AWS provides cloud hosting services to support the physical infrastructure of Congruit's services.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

Congruit Credit's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Congruit Credit's services to be solely achieved by Congruit Credit control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Congruit Credit.

The following subservice organization controls have been implemented by each subservice organization and included in this report to provide additional assurance that the trust services criteria are met.

Category	Criteria	Control
Subservice Organization Controls – Amazon Web Services (AWS)		
Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Closed circuit television camera (CCTV) is used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
		Access to server locations is managed by electronic access control devices.

Congruit management, along with the subservice provider, will define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Congruit performs monitoring of the subservice organization controls, including the following procedures

- Reviewing and reconciling output reports
- Holding periodic discussions with vendors and subservice organization(s)
- Making regular site visits to vendor and subservice organization(s') facilities
- Testing controls performed by vendors and subservice organization(s)

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

COMPLEMENTARY USER ENTITY CONTROLS

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

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

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



Section IV

DESCRIPTION OF TEST OF CONTROLS AND RESULTS THEREOF

Relevant trust services criteria and Congruit Credit's related controls are an integral part of management's system description and are included in this section. Johanson Group LLP performed testing to determine if Congruit Credit's controls were suitably designed and operating effectively to achieve the specified criteria for the Security category set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA, Trust Services Criteria, throughout the period December 18, 2025 to March 17, 2026.

Tests of the controls included inquiry of appropriate management, supervisory and staff personnel, observation of Congruit Credit activities and operations, and inspection of Congruit Credit documents and records. The results of those tests were considered in the planning, the nature, timing, and extent of Johanson Group LLP's testing of the controls designed to achieve the relevant trust services criteria. As inquiries were performed for substantially all Congruit Credit controls, this test was not listed individually for every control in the tables below.

Trust Services Criteria	Description of Congruit Credit's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
CC1.0 - Control Environment			
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	The Company has a documented Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire.	1. Inspected the entity's Code of Conduct to determine that the entity had a formal Code of Conduct approved by management and accessible to all employees. 2. Obtained a population of new hires across the entire audit period, and selected a sample according to our sampling guidance. 3. Inspected signed agreement for the selected sample of new hires during the audit period to determine it was acknowledged upon hiring.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that there were no new hire employees during the review period.
CC1.1.2	New hires are subjected to background and/or reference checks as a condition of their employment, as permitted by local laws.	1. Obtained a population of new hires across the entire audit period, and selected a sample according to our sampling guidance. 2. For the sample selected, inspected evidence that a background check was completed for the new hire(s) prior to their start date.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that there were no new hire employees during the review period.
CC1.1.3	The Company Managers complete performance reviews for employees at least annually.	1. Obtained a population of current employees during the audit period, and selected a sample according to our sampling guidance. 2. Inspected the performance review(s) for the selected sample of employees to determine that performance review was conducted within the past year.	No exceptions noted.
CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	The Company's Board of Directors (or equivalent) are separate and independent from the company's management.	1. Obtained and inspected the Board of Directors Roster to determine they were independent from management.	No exceptions noted.

Trust Services Criteria	Description of Congruit Credit's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	The Company has a documented organization chart which outlines the roles, functional responsibilities and reporting lines for the entity personnel.	1. Obtained and inspected the Organization Chart to determine that reporting lines, authorities, and responsibilities.	No exceptions noted.
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	Job skill requirements/qualifications are documented in job descriptions, and candidates' abilities to meet these requirements are evaluated as part of the hiring and performance review processes.	1. Inquire with Mangement to confirm that job requirements are evaluated during the hiring process. 2. Obtained and inspected one sample of a job description to confirm that job requirements/skills are defined.	No exceptions noted.
CC1.4.2	New hires are subjected to background and/or reference checks as a condition of their employment, as permitted by local laws.	1. Obtained a population of new hires across the entire audit period, and selected a sample according to our sampling guidance. 2. For the sample selected, inspected evidence that a background check was completed for the new hire(s) prior to their start date.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that there were no new hire employees during the review period.
CC1.4.3	The Company requires employees to complete the Security Awareness training at least annually.	1. Obtained a population of current employees during the audit period, and selected a sample according to our sampling guidance. 2. Inspected evidence for selected employees to confirm that they completed the Security Awareness training within the last year.	No exceptions noted.
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	The Company Managers complete performance reviews for employees at least annually.	1. Obtained a population of current employees during the audit period, and selected a sample according to our sampling guidance. 2. Inspected the performance review(s) for the selected sample of employees to determine that performance review was conducted within the past year.	No exceptions noted.
CC1.5.2	The Company requires employees to complete the Security Awareness training at least annually.	1. Obtained a population of current employees during the audit period, and selected a sample according to our sampling guidance. 2. Inspected evidence for selected employees to confirm that they completed the Security Awareness training within the last year.	No exceptions noted.
CC1.5.3	The Company has a documented Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire.	1. Inspected the entity's Code of Conduct to determine that the entity had a formal Code of Conduct approved by management and accessible to all employees.	No events to test. Note: Testing of the control activity disclosed that the control was

Trust Services Criteria	Description of Congruit Credit's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
		2. Obtained a population of new hires across the entire audit period, and selected a sample according to our sampling guidance. 3. Inspected signed agreement for the selected sample of new hires during the audit period to determine it was acknowledged upon hiring.	suitably designed and that there were no new hire employees during the review period.
CC2.0 - Communication and Information			
CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	The Company performs continuous control activity monitoring though the use of a GRC Platform or manual controls testing to ensure controls are operating effectively.	Inspected the continuous control monitoring dashboard (or equivalent) to determine that the entity performs control monitoring to gain assurance that controls are in place and operating effectively.	No exceptions noted.
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	The entity has approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible to all employees.	1. Obtained a population of new hires across the entire audit period, and selected a sample according to our sampling guidance. 2. Inspected the evidence of acknowledgement of security policies for the selection of new hires.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that there were no new hire employees during the review period.
CC2.2.2	The Company requires employees to complete the Security Awareness training at least annually.	1. Obtained a population of current employees during the audit period, and selected a sample according to our sampling guidance. 2. Inspected evidence for selected employees to confirm that they completed the Security Awareness training within the last year.	No exceptions noted.
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).	Inspected the company Master Service Agreement (MSA) or Terms of Service (TOS) to determine that the company and customer responsibilities are described in the agreements.	No exceptions noted.
CC2.3.2	The entity provides a process to external users for reporting security, confidentiality, integrity and availability failures, incidents, concerns, and other complaints.	Inspected the support page to determine that the entity provides a process to external users for reporting security, confidentiality, integrity and availability failures, incidents, concerns, and other complaints.	No exceptions noted.

Trust Services Criteria	Description of Congruit Credit's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
CC3.0 - Risk Assessment			
CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	The management formally documents and reviews the company's commitments and the operational, reporting, and compliance objectives to ensure they align with the company's objectives and are used as part of the annual risk assessment.	Inspected the company records to determine that the management formally documents and reviews the company's commitments and the operational, reporting, and compliance objectives to ensure they align with the company's objectives and are used as part of the annual risk assessment.	No exceptions noted.
CC3.1.2	The company conducts an internal control review annually to ensure controls are functioning as expected.	Inspected the company records to determine that the company conducts an internal control review annually to ensure controls are functioning as expected.	No exceptions noted.
CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2.1	As part of the risk assessment, vulnerabilities and threats are identified corresponding to risks. With vendors and partners needed to conduct business in the Cloud, these entities are analyzed for potential vulnerabilities. Risks are subsequently rated using a risk evaluation process and are documented in a risk register, along with mitigation strategies, for management review.	Inspected the risk assessment to determine that a risk assessment was completed on an annual basis and identified and ranked potential threats to the system.	No exceptions noted.
CC3.2.2	A systems inventory is maintained that includes physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles.	Inspected the company systems inventory and determines that it is maintained and includes physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles.	No exceptions noted.
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	Management considers the potential for fraudulent activity as part of the annual risk review process.	Inspected the company records to determine that management considers the potential for fraudulent activity as part of the annual risk review process.	No exceptions noted.
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	As part of the risk management process, management considers the impact of changes to the system. Risks that are identified are rated using a risk evaluation process that accounts for changes in risk from the prior year, and are formally documented.	Inspected the company records to determine that as part of the risk management process, management considers the impact of changes to the system. Risks that are identified are rated using a risk evaluation process that accounts for changes in risk from the prior year, and are formally documented.	No exceptions noted.
CC4.0 - Monitoring Activities			
CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	The Company's continuously monitors to detect any security events, latency, network	1. Inspected the entity's monitoring dashboard (or equivalent) to determine that the entity continuously monitors to	No exceptions noted.

Trust Services Criteria	Description of Congruit Credit's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	performance, and virtual server performance issues.	detect any security events, latency, network performance, and virtual server performance issues.	
CC4.1.2	Capacity monitoring is performed to ensure that use of resources is within acceptable limits and below maximum utilization for a resource.	Inspected the company records to determine that capacity monitoring is performed to ensure that use of resources is within acceptable limits and below maximum utilization for a resource.	No exceptions noted.
CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC4.2.1	Control owners perform an annual self-evaluation of the effectiveness of controls, which are reviewed for management action and/or input to the risk management process.	Inspected the Annual Internal Control Self-Assessment to determine that control owners perform an annual self-evaluation of the effectiveness of controls, which are reviewed for management action and/or input to the risk management process.	No exceptions noted.
CC4.2.2	The entity provides a process to external users for reporting security, confidentiality, integrity and availability failures, incidents, concerns, and other complaints.	Inspected the company records to determine that planned changes and updates are communicated as part of the development roadmap.	No exceptions noted.
CC5.0 - Control Activities			
CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	The Company makes changes as appropriate to address any identified risks. These issues are considered and prioritized as part of a regular development planning process. Assigned Control owners update control activities to mitigate the risks identified during the annual risk assessment process.	Inspected the company records to determine that the company makes changes as appropriate to address any identified risks. These issues are considered and prioritized as part of a regular development planning process. Assigned Engineering owners develop control activities to mitigate the risks identified during the annual risk assessment process.	No exceptions noted.
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	Assigned risk owners develop control activities over technology to support the achievement of objectives as an output from the risk assessment performed on an annual basis.	Inspected the company records to determine that assigned risk owners develop control activities over technology to support the achievement of objectives as an output from the risk assessment performed on an annual basis.	No exceptions noted.
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	Information system security and management policies are formally documented and reviewed on an annual basis that identifies information required to support the functioning of internal control and achievement of objectives.	Inspected the company records to determine that information system security and management policies are formally documented and reviewed on an annual basis that identifies information required to support the functioning of internal control and achievement of objectives.	No exceptions noted.

Trust Services Criteria	Description of Congruit Credit's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
CC5.3.2	An employee sanction procedure is in place and documented within the employee handbook communicating that an employee may be terminated for noncompliance with the handbook, code of conduct or security policy.	Inspected the company records to determine that an employee sanction procedure is in place and documented within the employee handbook communicating that an employee may be terminated for noncompliance with the handbook, code of conducy or security policy.	No exceptions noted.
CC6.0 - Logical and Physical Access Controls			
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.1.1	The company has established an Access Security Policy that governs access to systems and infrastructure.	Obtained and inspected the Access Control Policy determine that the entity had a defined, formal access management process that governs access to systems and infrastructure.	No exceptions noted.
CC6.1.2	The in-scope systems and application are configured to authenticate users with a unique user account and enforce minimum password requirements.	Inspected the password configurations to determine that the in-scope systems and applications are configured to authenticate users with a unique user account and enforce minimum password requirements or SSH public key authentication.	No exceptions noted.
CC6.2 - 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			
CC6.2.1	New hire access is granted based on job responsibility and is requested, documented, and authorized by management prior to start date.	1. Obtained a population of new hires across the entire audit period, and selected a sample according to our sampling guidance. 2. For the sample selected, inspected evidence that the new hire's access was properly approved prior to their start date.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that there were no new hire employees during the review period.
CC6.2.2	Access changes are properly approved.	1. Obtained a population of access changes across the entire audit period, and selected a sample according to our sampling guidance. 2. For the sample selected, inspected evidence that the access change was properly approved.	No exceptions noted.
CC6.2.3	Terminated user access rights are disabled by IT following termination notification from HR. All access changes, including terminations, are documented and tracked in the Help Desk ticket system.	1. Obtained a population of terminated users across the entire audit period, and selected a sample according to our sampling guidance. 2. For the sample selected, inspected evidence that the terminated user's access was properly removed in a timely manner.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that there were no terminations during the review period.

Trust Services Criteria	Description of Congruit Credit's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
CC6.2.4	User access roles and privileges are reviewed and approved or updated by management on an annual basis.	Inspected the annual user access review to determine that annual reviews of the entity's critical systems and associated user access rights were performed to ensure access was appropriate, or to modify access where required.	No exceptions noted.
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of			
CC6.3.1	User access roles and privileges are reviewed and approved or updated by management on an annual basis.	Inspected the annual user access review to determine that annual reviews of the entity's critical systems and associated user access rights were performed to ensure access was appropriate, or to modify access where required.	No 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 Company does not operate any physical hardware such as servers and network devices but rather uses subservice organizations and relies on its own controls for physical access.	Not Applicable - Control is Carved Out	Control is implemented and maintained by subservice organization.
CC6.4.2	The entity requires a visitor sign-in procedure for access to the data center.	Not Applicable - Control is Carved Out	Control is implemented and maintained by subservice organization.
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CC6.5.1	Media handling and disposal procedures are in place to guide personnel in performing sanitization procedures on all accounts where production data resides so that data and software is unrecoverable prior to retiring the asset.	Inspected the company records to determine that media handling and disposal procedures are in place to guide personnel in performing sanitization procedures on all accounts where production data resides so that data and software is unrecoverable prior to retiring the asset.	No exceptions noted.
CC6.5.2	Electronic media containing confidential information is purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	1. Obtained a population of media disposals across the entire audit period, and selected a sample according to our sampling guidance. 2. For the sample selected, inspected evidence that the electronic media containing confidential information is purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed and that no disposal/destruction events occurred, therefore, there were no disposal tickets during the review period.
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	The Company perimeter protection systems are configured to deny unauthorized traffic from external sources and does not provide special access privileges to those outside of its hosted project.	Inspected the company records to determine that the perimeter protection systems are configured to deny unauthorized traffic from external sources and does not provide special	No exceptions noted.

Trust Services Criteria	Description of Congruit Credit's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
		access privileges to those outside of its hosted project.	
CC6.6.2	Web servers use TLS encryption for web communication sessions.	Inspected the company records to determine that web servers use TLS encryption for web communication sessions.	No exceptions noted.
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CC6.7.1	Encryption technologies such as VPN, TLS, and SFTP are used to protect communications and data during transmission.	Inspected the company records to determine that encryption technologies such as VPN, TLS, and SFTP are used to protect communications and data during transmission.	No exceptions noted.
CC6.7.2	The company has established an Access Security Policy that governs access to systems and infrastructure.	Obtained and inspected the Access Control Policy determine that the entity had a defined, formal access management process that governs access to systems and infrastructure.	No exceptions noted.
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8.1	The company utilizes anti-malware software which is centrally managed and deployed on client machines and is monitored for unauthorized or malicious software installations.	Inspected the company records to determine that it utilizes anti-malware software which is centrally managed and deployed on client machines and is monitored for unauthorized or malicious software installations.	No exceptions noted.
CC6.8.2	The company has established an Access Security Policy that governs access to systems and infrastructure.	Obtained and inspected the Access Control Policy determine that the entity had a defined, formal access management process that governs access to systems and infrastructure.	No exceptions noted.
CC7.0 - System Operations			
CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC7.1.1	The Company performs network vulnerability scans on at least an annual basis, and remediates critical vunerabilities identified in a timely manner.	Inspected the scan results and on-going remediation to determine that vulnerability scans were performed at least annually to identify security issues and were remediated timely.	No exceptions noted.
CC7.1.2	Annual penetration testing is conducted by an independent third party on the network and on the Platform application.	Inspected annual penetration testing to determine if it was conducted by an independent third party on the network and on the Platform application.	No exceptions noted.
CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether			
CC7.2.1	An Intrusion Detection System (or equivalent) is in place to alert personnel to unauthorized modifications of critical system files, configuration files, and content files.	Inspected the infrastructure monitoring configurations and monitoring rulesets to determine that An Intrusion Detection System (or equivalent) is in place to alert personnel to unauthorized modifications of critical system files, configuration files, and content files.	No exceptions noted.

Trust Services Criteria	Description of Congruit Credit's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
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	IT Operations personnel review identified security events to determine impact and to recommend remediation, if necessary.	Inspected the security event tickets to determine that IT Operations personnel review identified security events to determine impact and to recommend remediation, if necessary.	No events to test. Note: Testing of the control activity disclosed that the control was suitably designed, and no security or privacy incidents were noted during the review period.
CC7.3.2	The company has incident response policies and processes documented to handle security and or data breach incidents.	Inspected the Incident Response Policy to determine that the company has policies and processes documented to handle security and or data breach incidents.	No exceptions noted.
CC7.4 - The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	The company has incident response policies and processes documented to handle security and or data breach incidents.	Inspected the Incident Response Policy to determine that the company has policies and processes documented to handle security and or data breach incidents.	No exceptions noted.
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	The company has recovery plans in place to provide processes for recovery systems as needed after incidents or other types of outages.	Inspected the Business Continuity Planning and Disaster Recovery Policy to determine that the company has recovery plans in place to provide processes for recovery systems as needed after incidents or other types of outages.	No exceptions noted.
CC8.0 - Change Management			
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	Change requests are submitted via a Change Request form and are entered into a ticket system for tracking. Management approval is obtained and documented in each change ticket.	1. Obtained a population of access changes across the entire audit period, and selected a sample according to our sampling guidance. 2. For the samples selected, inspected the change tickets to determine that change requests are submitted via a Change Request form and are entered into a ticket system for tracking. Management approval is obtained and documented in the selected change tickets.	No exceptions noted.
CC8.1.2	The Platform application development and testing are done in separate environments from production.	Inspected the production and development environment configurations to determine that the system application development and testing are done in separate environments from production.	No exceptions noted.
CC8.1.3	Change management policies and procedures are in place to guide personnel in the request, documentation, testing, and approval of	Inspected the Change Management / SDLC Policy & Procedure to determine that policies and procedures are in place	No exceptions noted.

Trust Services Criteria	Description of Congruit Credit's Controls	Service Auditor Test of Controls	Results of Service Auditor Test of Controls
	changes. The policies and procedures also outline the requirement for segregation of duties such that authorization, development, testing and implementation are segmented functions within the process.	to guide personnel in the request, documentation, testing, and approval of changes. The policies and procedures also outline the requirement for segregation of duties such that authorization, development, testing and implementation are segmented functions within the process.	
CC9.0 - Risk Mitigation			
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	The Company has developed a written business continuity plan and disaster recovery plan with procedures to protect against disruptions caused by an unexpected event.	Inspected the company records to determine that the company has developed a written business continuity plan and disaster recovery plan with procedures to protect against disruptions caused by an unexpected event.	No exceptions noted.
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	The Company management reviews the Annual SOC 2 report (or SOC 1) for its hosted data center to confirm that outsourced controls are appropriately designed and operating effectively.	Inspected the company records to determine that the management reviews the annual SOC report for its hosted data center to confirm that outsourced controls are appropriately designed and operating effectively.	No exceptions noted.
CC9.2.2	A vendor management process is in place and requires signed contract for vendors and includes (1) scope of services and product specifications, (2) roles and responsibilities, (3) compliance requirements, and (4) service levels where applicable.	Inspected the Vendor Review to determine that a vendor management process is in place and requires signed contract for vendors and includes (1) scope of services and product specifications, (2) roles and responsibilities, (3) compliance requirements, and (4) service levels where applicable.	No exceptions noted.