JOHANSON GROUP

System and Organization Controls (SOC) 2 Type II Report

Report on Controls Placed in Operation and Test of Operating Effectiveness Relevant to the Trust Services Criteria for Security, Availability, Processing Integrity, and Confidentiality Categories

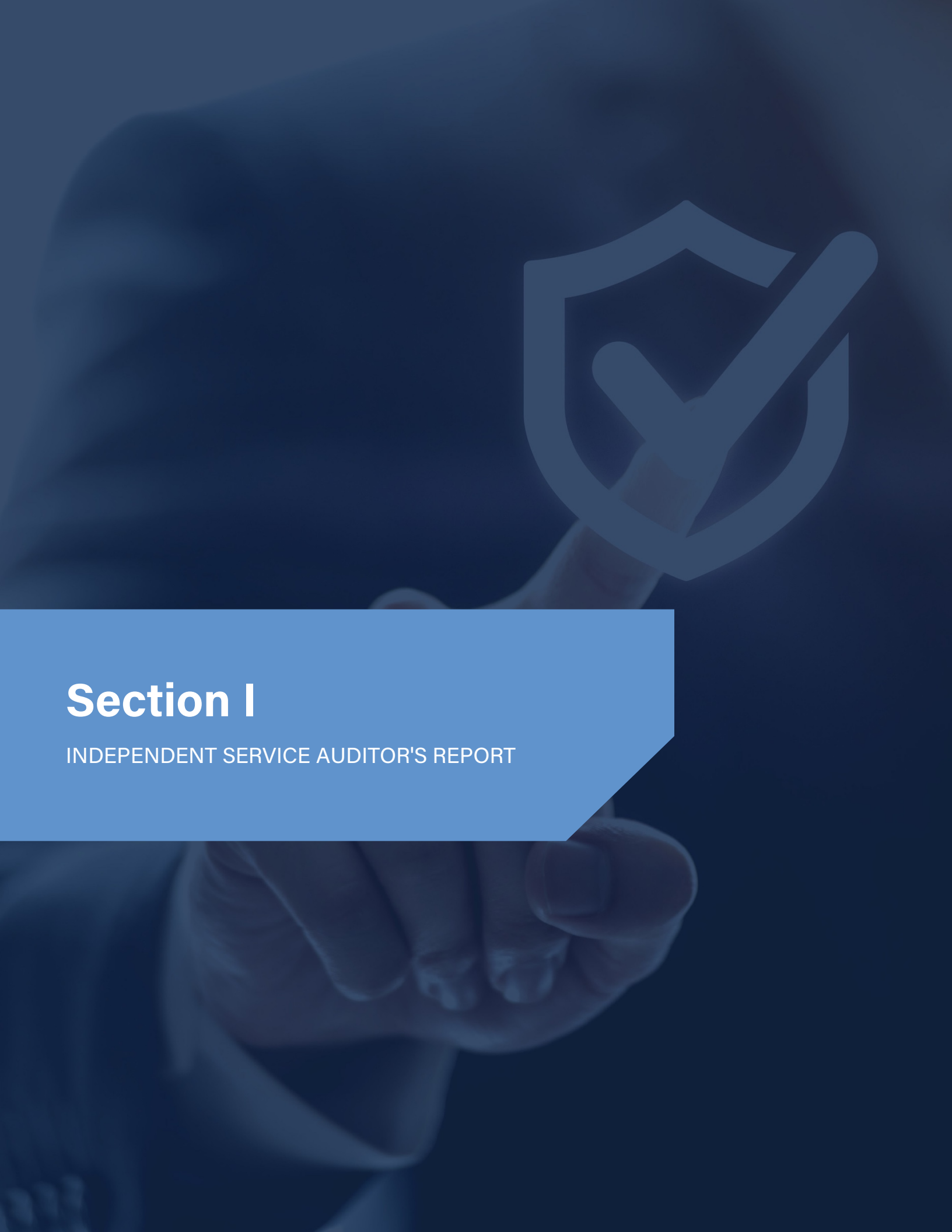
For the Period
September 01, 2022 to August 31, 2023

Together with Independent Service Auditor's Report

Report on Management's Description of

marvin

TABLE OF CONTENTS



Section I

INDEPENDENT SERVICE AUDITOR'S REPORT

Equafin Corp.

Scope

We have examined Equafin Corp.'s accompanying description of its Marvin App (system) titled "Description of Marvin App" throughout the period September 01, 2022 to August 31, 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 September 01, 2022 to August 31, 2023, to provide reasonable assurance that Equafin Corp.'s service commitments and system requirements were achieved based on trust services criteria relevant to security, availability, processing integrity, and confidentiality principles (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.*

Equafin Corp. 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 Equafin Corp., to achieve Equafin Corp.'s service commitments and system requirements based on the applicable trust services criteria. The description presents Equafin Corp.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Equafin Corp.'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 Equafin Corp., to achieve Equafin Corp.'s service commitments and system requirements based on the applicable trust services criteria. The description presents Equafin Corp.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Equafin Corp.'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

Equafin Corp. 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 Equafin Corp.'s service commitments and system requirements were achieved. Equafin Corp. has provided an assertion titled "Assertion of Equafin Corp. Management" (assertion) about the description and the suitability of design and operating effectiveness of the controls stated therein. Equafin Corp. 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 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.

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 Equafin Corp.'s Marvin App (system) that was designed and implemented throughout the period September 01, 2022 to August 31, 2023, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period September 01, 2022 to August 31, 2023, to provide reasonable assurance that Equafin Corp.'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 Equafin Corp.'s controls throughout the period.
c. The controls stated in the description operated effectively throughout the period September 01, 2022 to August 31, 2023, to provide reasonable assurance that Equafin Corp.'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 Equafin Corp.'s controls operated effectively throughout the period.

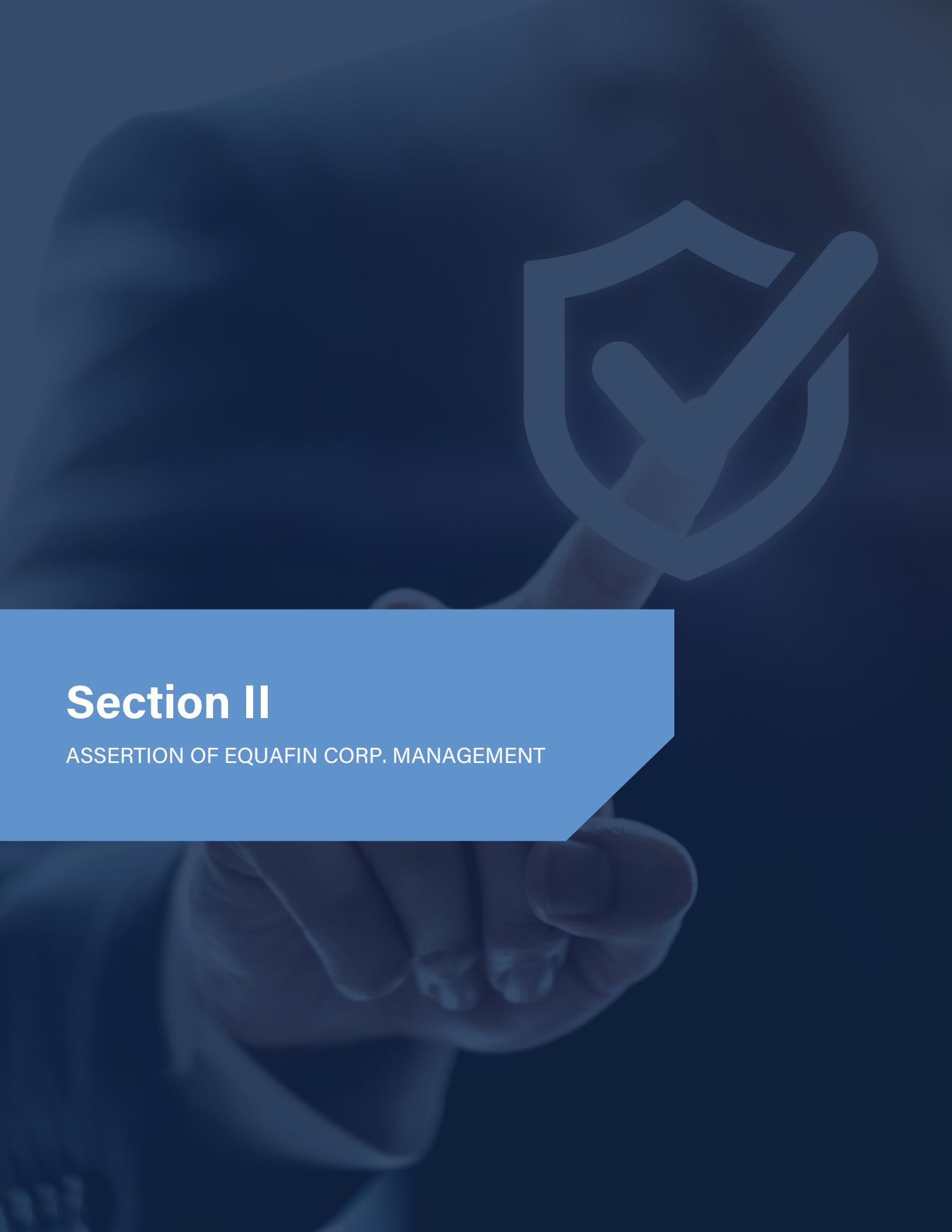
Restricted Use

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 Equafin Corp.; user entities of Equafin Corp.'s Marvin App during some or all of the period September 01, 2022 to August 31, 2023, business partners of Equafin Corp. subject to risks arising from interactions with the Equafin Corp.'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
October 25, 2023



Section II

ASSERTION OF EQUAFIN CORP. MANAGEMENT

We have prepared the accompanying description of Equafin Corp.'s "Description of Marvin App" for the period September 01, 2022 to August 31, 2023, (description) based on the criteria for a description of a service organization's system in the 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 Equafin Corp.'s Marvin App (system) that may be useful when assessing the risks arising from interactions with Equafin Corp.'s system, particularly information about system controls that Equafin Corp. 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, processing integrity, 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).*

Equafin Corp. 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 Equafin Corp., to achieve Equafin Corp.'s service commitments and system requirements based on the applicable trust services criteria. The description presents Equafin Corp.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Equafin Corp.'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 Equafin Corp., to achieve Equafin Corp.'s service commitments and system requirements based on the applicable trust services criteria. The description presents Equafin Corp.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Equafin Corp.'s controls.

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

a. The description presents Equafin Corp.'s Marvin App (system) that was designed and implemented throughout the period September 01, 2022 to August 31, 2023, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period September 01, 2022 to August 31, 2023, to provide reasonable assurance that Equafin Corp.'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 Equafin Corp.'s controls throughout that period.
c. The controls stated in the description operated effectively throughout the period September 01, 2022 to August 31, 2023, to provide reasonable assurance that Equafin Corp.'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 Equafin Corp.'s controls operated effectively throughout that period.

Equafin Corp. Management
October 25, 2023

Section III

DESCRIPTION OF MARVIN APP

TYPE OF SERVICE PROVIDED

Equafin Corp. ("Marvin App") is a hosted service that provides qualitative data analysis and feedback management capabilities to product consulting, financial, and other related teams. Built on Zoom and other conferencing platforms like Telephony (with Twilio), Google Meet, and Microsoft Teams, the Marvin App lets teams organize, manage, record, upload, or import recordings of feedback and interview sessions, transcribe them, take notes, and analyze them for patterns and insights. Marvin App has a note-taking app as well as an annotation app that makes it easy to highlight and share relevant insights from different feedback sessions. Users could also upload any files for audio or video recording and get the same features. Marvin App also provides its users, the ability to track and manage the scheduling of interviews and analyze the candidates on those interviews by their demographics.

This report includes the Marvin App. Any other services by Marvin App are not included within the scope of this report. The accompanying description includes only policies, procedures, and control activities at Marvin App with respect to the service and does not include policies, procedures, and control activities at any subservice organizations (see below for a further discussion of subservice organizations).

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Commitments are declarations made by management to customers regarding the performance of the Marvin App. Commitments are communicated in written individualized agreements and standardized contracts.

System requirements are specifications regarding how the Marvin App should function to meet Marvin App's principal commitments to user entities. System requirements are specified in the Marvin App Service Agreement and its end-user documentation, both of which are available internally to all employees and externally to all customers.

Trust Service Category	Service Commitments	System Requirements
Security	• Protection of data at rest and in transit • Regular system updates • Protection and security of the information system from unauthorized access, use, modification, disclosure, destruction, threats, or hazards	• Logical access standards • Physical access standards • Employee provisioning and de-provisioning standards • Access reviews • Encryption standards • Intrusion detection and prevention standards • Risk and vulnerability • management standards • Configuration management • Incident handling standards • Change management standards • Vendor management • System access is granted to authorized personnel only • Regular security assessments • Identification and remediation of security incidents/events

		• Perform risk assessments for both internal and external threats to the system and its information
Availability	• Maintain, monitor, and evaluate current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand • Enable the implementation of additional capacity	• Measure Current Usage • Forecast Capacity • Make Changes Based on Forecasts • Implement Alerts to Analyze Anomalies • Determine Data Requiring Backup • Perform Data Backup • Offsite Storage • Test Integrity and Completeness of Backup Data
Confidentiality	• Information designated as confidential is protected to meet the entity's objectives.	• Access management implemented • Alerting on unauthorized access to data
Processing Integrity	• Information and system processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.	• Validation for all the data uploaded and processed by the service • Monitor errors and incorrectness of data • Logging for output data distribution

THE COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICE

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

The components that directly support the Service provided to customers are as follows:

Infrastructure

Marvin App has entered into an agreement with Heroku and AWS to provide global IaaS at its Ohio sites. AWS provides physical and environmental security Services in these two regions. However, Marvin App is responsible for designing and configuring the Marvin App service's architecture within AWS and Heroku to ensure Marvin App's security and confidentiality requirements are met.

Software

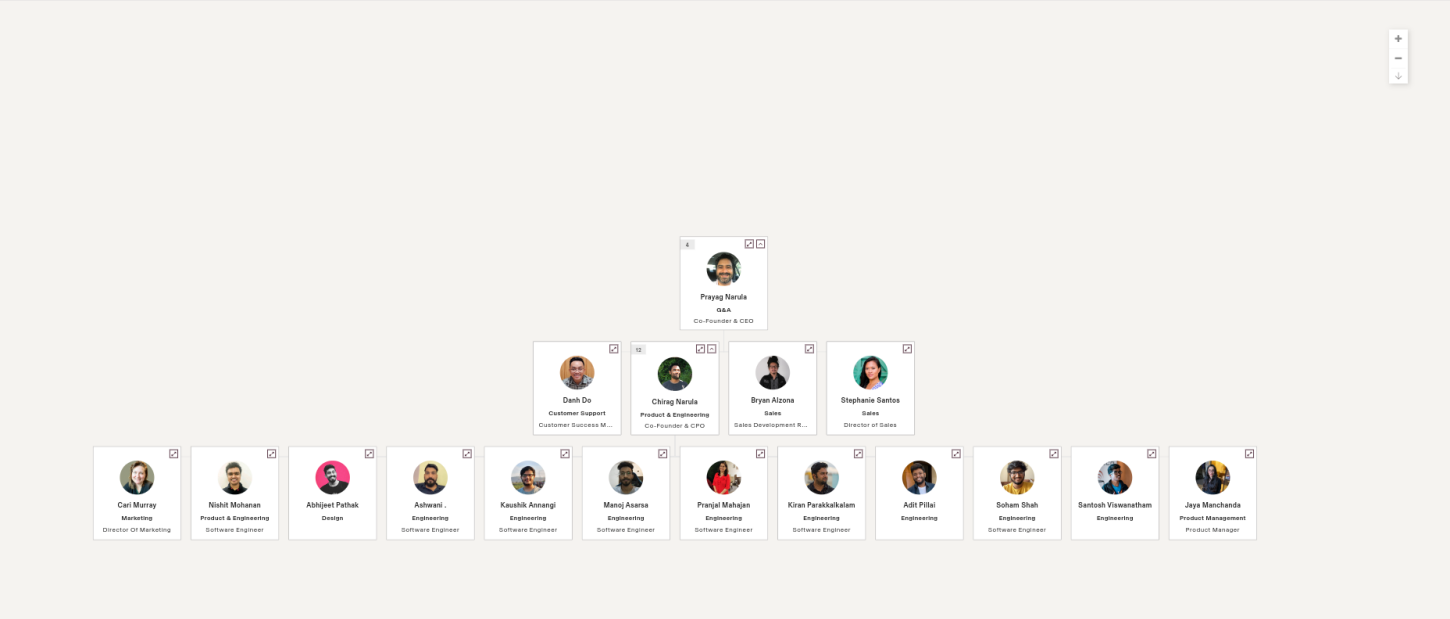
The software includes supporting operating systems and databases (AWS RDS) and Marvin App's software for two-factor authentication. Marvin App uses AWS CloudWatch and Papertrail to monitor system logs and service levels. Marvin App uses NewRelic to perform performance monitoring and Sentry.io to monitor any system errors. It uses Deepsource.io to perform security monitoring and OWASP Zap to do regular security scans. Papertrail is used for storing and managing logs. The output of these systems is routinely monitored to make sure that the systems are performing as expected.

People

Marvin App develops, manages, and secures the Marvin App Service via separate teams. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Executive Management	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives.
Engineering and Product Design	Responsible for the development, testing, deployment, daily operation, and maintenance of new code for the Marvin App Service.
DevOps	Manages infrastructure and security including access controls and security of the development and production environment for Marvin App Service.
Product Management	Responsible for the product lifecycle including adding additional product functionality.

The following organization chart reflects the internal structure of the Marvin App related to the groups discussed above:



Procedures

Procedures include the automated and manual procedures involved in the operation of the Marvin App Service.

Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, IT, human resources, etc. These procedures are drafted in alignment with the overall Information Security Policies and are updated and approved as necessary for changes in the business, no less than annually.

Procedures	
Procedure	**Description**
Logical and Physical Access	How Marvin App restricts logical and physical access, provides and removes that access, and prevents unauthorized access.
System Operations	How Marvin App manages the operation of the system and detects and mitigates processing deviations, including logical and physical security deviations.
Change Management	How Marvin App identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
Risk Mitigation	How the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

Data

Data refers to transaction streams, files, recordings, data stores, tables, and output used or processed by Marvin App. Via the platform, the customer/end-users define and control the data they load and store in the Marvin App's production network. This data is loaded into the environment and accessed remotely from customer systems via the Internet.

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts.

Marvin App has deployed secure methods and protocols for the transmission of confidential and/or sensitive information over public networks and internet databases, housing sensitive customer data to be encrypted at rest.

Following is the type of information Marvin App stores:

- The Marvin App tracks user activity and data in relation to the types of Service customers and their users use including video recordings, meeting meta-data, personal information (name, email address, and Zoom user ID), and performance metrics related to their use of the Service.
- The Marvin App service logs information about customers and their users, including Internet Protocol ("IP") addresses. Log files are immutable records of computer events about an operating system, application, or user activity, which form an audit trail. These records may be used to assist in detecting security violations, performance problems, and flaws in applications.

All other data is stored in the customer systems on the customer premises.

SYSTEM INCIDENTS

There were no identified significant system incidents that (a) were the result of controls that were not suitably designed or operating effectively to achieve one or more of the service commitments and system requirements or that (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements as of the date of this report.

THE APPLICABLE TRUST SERVICE CRITERIA AND RELATED CONTROLS

Applicable Trust Service Criteria

The Trust Service Categories that are in scope for purposes of this report are as follows:

- Security: Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the confidentiality of information or systems and affect the entity's ability to meet its objectives.
- Availability: Information and systems are available for operation and use to meet the entity's objectives.
- Confidentiality: Information designated as confidential is protected to meet the entity's objectives.
- Processing Integrity: Information and system processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.

Many of the criteria used to evaluate a system are shared amongst all the categories; for example, the criteria related to risk assessment apply to the security and confidentiality categories. As a result, the criteria for the security and confidentiality categories are organized into (a) the criteria that are applicable to both categories (common criteria) and (b) criteria applicable only to confidentiality. The common criteria constitute the complete set of criteria for the security category. For the category of confidentiality, a complete set of criteria comprises all the common criteria and all the criteria applicable only to confidentiality.

The common criteria are organized as follows:

1. *Control environment:* The criteria relevant to how the organization is structured and the processes the organization has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values, and qualifications of personnel and the environment in which they function.
2. *Communication and information:* The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system, and the obligations of those parties and users to the effective operation of the system.
3. *Risk assessment:* The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks, including the design and implementation of controls and other risk-mitigating actions, and (iv)conducts ongoing monitoring of risks and the risk management process.
4. *Monitoring activities:* The criteria relevant to how the entity monitors the system, including the suitability, design, and operating effectiveness of the controls, and acts to address deficiencies identified.
5. *Control activities:* The criteria relevant to the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.
6. *Logical and physical access controls:* The criteria relevant to how an entity restricts logical and physical access, provides and removes that access, and prevents unauthorized access.
7. *System operations:* The criteria relevant to how an entity manages the operation of the system(s) and detects and mitigates processing deviations, including logical and physical security deviations.

8. *Change management:* The criteria relevant to how an entity identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
9. *Risk mitigation:* The criteria relevant to how the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

This report is focused on the security, availability, processing integrity, and confidentiality categories, and Marvin App has elected to exclude the privacy category.

CONTROLS RELATED TO THE APPLICABLE CRITERIA

Marvin App's applicable controls supporting the security, availability, processing integrity, and confidentiality categories and related criteria are included in Section 4 of this report. Although the applicable criteria and related controls are included in Section 4, they are, nevertheless, an integral part of the organization's description of its system.

The five interrelated components of internal control at Marvin App include:

- Control Environment – sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.
- Communication and Information – are systems, both automated and manual, that support the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities.
- Risk Assessment – is the entity's identification and analysis of relevant risks to the achievement of its objectives, forming a basis for determining how the risks can be managed.
- Monitoring – is a process that assesses the quality of internal control performance over time.
- Control Activities – are the policies and procedures that help make sure that management's directives are carried out.

The Marvin App's internal control components include controls that may have a pervasive effect on the organization, an effect on specific processes, account balances, disclosures, classes of transactions or applications, or both. Some of the components of internal control include controls that have more of an effect at the entity level, while other components include controls that are primarily related to specific processes or applications. When assessing internal control, the Marvin App considers the interrelationships among the five components.

CONTROL ENVIRONMENT

Integrity and Ethical Values

Marvin App has developed a Code of Conduct that addresses acceptable business practices, conflicts of interest, and expected standards of ethical and moral behavior. Marvin App has also developed employee Confidentiality Agreements that prohibit inappropriate use and disclosure of customer or Marvin App information. These documents are provided to all new employees. All employees and contractors are required to sign a Confidentiality Agreement as well as acknowledge and agree to follow the Code of Conduct.

Marvin App management performs annual performance evaluations of personnel in order to maintain compliance with Marvin App policies and codes of conduct. Employees and contractors who violate the code of conduct are subject to disciplinary actions.

Board of Directors

The Marvin App Board of Directors oversees and advises Marvin App's corporate governance, strategy, and risk oversight. The Board of Directors, composed of the founders of the company, meets regularly to discuss matters pertinent to Marvin App's business operations, financial results, and strategic planning.

Organizational Structure

Marvin App has established lines of reporting which facilitate the flow of information to personnel. Marvin App's HR system has a built-in organization chart that sets forth Marvin App's lines of reporting and is updated automatically as organizational changes occur. The Executive Management Team empowers business functions to implement and manage functional policies, procedures, methods, and organizational structure for increasing operational effectiveness and service delivery excellence. Marvin App's organization is structured to oversee the implementation and compliance of all required financial, business, and security controls. Roles and responsibilities are segregated based on functional requirements.

Management's Philosophy and Operating Style

Marvin App's executive team takes a "hands-on" approach to running the business. The executive team is heavily involved in all phases of the business operations. Management uses a top-down approach to establish or update specific business objectives for business units and functions, including information technology, within the organization. This process includes budgeting resources and establishing metrics for the achievement of the objectives.

Authority and Responsibility

Management and employees are assigned levels of authority and responsibility to facilitate effective internal control. The Chief Executive Officer (CEO) is responsible for overseeing the control environment. The duties, responsibilities, and hierarchy of employees on the information security team are defined in a role matrix and form the foundation of Marvin App's control environment. As part of the development of specific business objectives, the Chief Product Officer is responsible for executing the Marvin App product strategy and other decisions agreed upon by the Marvin App executive team and the Board of Directors.

Human Resources

Marvin App maintains formal hiring and termination policies and procedures. Applicants with a role in the delivery of Service are hired based on their ability to satisfy the job duties and responsibilities of the position and fulfill the goals and expectations of the Marvin App. They are evaluated on their level of education, the merits of their past experiences, and their knowledge of relevant security controls and processes. All applicants must undergo a background or reference check in accordance with local law; employment is contingent upon satisfactory results. Marvin App has a process to assign key processes and technology to authorized personnel.

Upon hiring and annually thereafter, all employees must successfully complete training courses covering Marvin App's code of conduct, data protection/privacy, and basic information security practices. The training courses are designed to assist employees in identifying and responding to social engineering attacks and in avoiding inappropriate security practices.

Contractors are required to follow the same onboarding process as employees and are contractually obligated to perform the same background checks and security awareness training requirements as employees. Employees' and contractors' compliance with security awareness training requirements is monitored on an annual basis by Digital Trust & Safety.

All employees go through an annual performance review cycle. At the beginning of each review period, employees and their immediate supervisors establish goals and expectations for their job performance over the upcoming year based on the job duties, priorities, and responsibilities described.

Employees receive an annual performance review from their supervisors that assesses the employees' performance against the agreed-upon goals and expectations. Employees whose performance is not in alignment with established goals and expectations for job performance or who are not fulfilling their job responsibilities may be referred to the executive team by their supervisor to develop a performance improvement plan or feedback.

If an employee violates any Marvin App policies or otherwise acts in a manner deemed contrary to the mission and objectives of Marvin App or in violation of the code of conduct, whether purposefully or not, the employee is subject to sanctions up to and including termination of employment.

COMMUNICATION AND INFORMATION

Marvin App has implemented information and communication mechanisms to make information available regarding its business practices.

The executive team has a documented Information Security Policy and a suite of supporting Standards. These documents are updated at least annually and are made available to all employees. The internal communication of cybersecurity information for employees is according to their role in the organization. Training on the Information Security Policy is described on the Security Awareness Program site, which is available to all employees on the Marvin App site.

Marvin App has reporting mechanisms for employees to communicate potential security issues or concerns they have been involved in or witnessed (such as phishing attacks, malware, lost or stolen devices, and inappropriate information disclosure). Marvin App also has established processes to accept and address reports of software vulnerabilities, including providing a means for external entities to contact the information security group.

Marvin App obtains or generates and uses relevant information to support the functioning of internal control through the following:

- Control monitoring through periodic management reviews, internal audits, and external audits
- Vulnerability scans
- Log management tools

Marvin App limits communication of matters related to the functioning of internal systems to only those stakeholders and business partners who have a need to know such information. This information is communicated via mediums appropriate to the nature of the information and the urgency of the situation and may include conference calls, electronic mail, memoranda, or in-person meetings. In the rare instance when public disclosure of such matters would be necessary or appropriate, Marvin App's legal counsel and executive team are responsible for jointly distributing and communicating such disclosure.

Marvin App provides customers with multiple channels to report and manage service issues. Dedicated support resources are responsible for keeping these Service Requests up to date and using available escalation and communication methods to keep customers informed about their requests.

Marvin App communicates its policies and business practices to its customers in the form of service contracts and user agreements, which must be accepted before the Service is rendered. These agreements delineate the customer and Marvin App's responsibilities as they pertain to confidentiality, ownership, and other areas of liability.

Marvin App's privacy policy is provided on its website.

RISK ASSESSMENT AND MITIGATION

The executive team oversees Marvin App's global risk assessment process to identify and manage risks that could affect Marvin App's ability to provide reliable service to its clients. This process requires management to identify significant risks in their areas of responsibility and to implement measures to address those risks. In designing its controls, Marvin App has considered the risks that could prevent it from effectively addressing the criteria under the security and confidentiality trust Service categories.

Marvin App maintains a risk management framework designed to ensure risks are evaluated and that controls are reasonably designed, implemented, and operated to address all areas, as appropriate, to detect, respond to, mitigate, and recover from security events based on the assessed risks. Areas for consideration include compliance objectives, external laws and regulations, and risk appetite. Areas for evaluation include systems development, computer operations, program changes, and access to programs and data. Implemented controls include preventive and detective controls, such as manual, automated, or IT-dependent controls based on the environment in which the entity operates, the nature and scope of the entity's operations, and its specific characteristics. Marvin App 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. Marvin App's risk assessment process includes an analysis of possible threats and vulnerabilities relative to each of the objectives. The risk identification process includes consideration of both internal and external factors and their impact on the achievement of the objectives.

Marvin App considers the potential for fraud in assessing risks to the achievement of objectives. The assessment of fraud risk considers fraudulent reporting, possible loss of assets, or data and corruption resulting from the various ways that fraud and misconduct can occur. It also considers opportunities for unauthorized acquisition, use, or disposal of assets, altering of the entity's reporting records, or committing other inappropriate acts and how management and other personnel might engage in or justify inappropriate actions.

Marvin App identifies and assesses changes that could significantly impact the system of internal control. The risk identification process considers changes to the regulatory, economic, and physical environment in which Marvin App operates. Marvin App considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations, rapid growth, and new technologies on the system of internal control.

Identified risks are analyzed through a process that includes estimating the potential significance of the risk.

Marvin App's risk assessment process includes considering how the risk should be managed and whether to accept, avoid, mitigate, or share the risk. Marvin App determines mitigation strategies for the risks that have been identified and designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy.

Security risks related to external parties (such as contractors and vendors) are identified and addressed based on the Marvin App procurement process. Designated responsibilities are defined as reviewing risks associated with external parties and establishing relevant agreements. Purchase orders to engage a third party require a vendor agreement and signed NDA to be established.

Sensitive information is disclosed to a vendor or business partner only on an as-needed basis, and only if the vendor or business partner has enacted appropriate information security and privacy controls. All vendors and business partners with access to sensitive information are subject to confidentiality and privacy agreements and other contractual confidentiality provisions, which must be signed and acknowledged before access to Marvin App systems and data is granted.

Marvin App's security program manages supply chain security risk throughout the lifecycle of the relationship and provides assurance that third parties who handle and process information and facilities on Marvin App's behalf do so in accordance with legal, regulatory, and contractual requirements for security.

Adoption of a supplier's Service has inherent information security risks, which are managed by adopting the following approach:

- Categorize: Third parties are categorized according to the nature, criticality, and likelihood of risk commensurate with the adoption of their Service
- Assess: Third parties are security reviewed in accordance with their assigned risk category
- Respond: The Supplier Assurance team conducts risk assessments based on information provided in completed questionnaires and audit findings
- Monitor: All risk remediation actions identified from risk assessments are tracked through to closure. Third parties are periodically re-assessed, according to their risk categorization

MONITORING

Marvin App selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. Internal personnel conduct periodic assessments and tests of internal controls that include (a) working with process owners and IT support personnel to identify specific security threats and vulnerabilities and how the associated risk is being addressed and (b) tests of the design, implementation, and operating effectiveness of internal controls that address risks. Members of the internal assessment team have the requisite knowledge of and experience with cybersecurity risks and controls. They also subscribe to industry-standard bulletins and alerts on security, delivered through Github's dependable, DeepSource.io as well as various mailing lists.

Marvin App also uses external parties to independently evaluate the state of the control environment. Ongoing security scanning through OWASP Zap and Annual penetration tests are performed by an external service provider to identify specific technical threats and vulnerabilities and to benchmark the environment against leading cybersecurity practices. Every year, Marvin App engages a service provider to perform an independent assessment of the system program to evaluate alignment with leading industry practices and consistency with company policies in order to identify gaps and potential opportunities for improvement.

Both internal and external evaluations are made using a risk-based approach that may vary in the nature, timing, and extent of testing. The criteria for such evaluations, including the nature and frequency of such evaluations, are reviewed during the annual risk assessment and modified as needed, with consideration for changes to Marvin App's operational processes, including changes to the size, scope, and operational nature of the business, recent security threats or incidents, new or emerging risks, and changes in industry standards.

The results of all monitoring activities, regardless of source, are entered into a vulnerability tracking system for evaluation and identification of remediation activities that may be needed. Identified vulnerabilities are assessed with regard to the likelihood and magnitude of exploitation. All vulnerabilities evaluated are identified for remediation or additional monitoring. Responsibilities for corrective action plans are assigned, and completion dates are determined. The Information Security team reviews the list of open vulnerabilities on a monthly basis to monitor progress toward resolution and to identify trends and responses.

CONTROL ACTIVITIES

Marvin App's control activities are defined through its established policies and procedures. Policies are dictated through management or board member statements of what should be done to effect control.

Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. Policies serve as the basis for procedures. Control activities are deployed through policies that establish what is expected and procedures that put policies into action. A list of policies and procedures is documented in the above Procedures section.

Logical and Physical Access

Marvin App's Identity and Access Management Standard establishes the access control requirements for requesting and provisioning user access to the system. The policy requires that access be denied by default, following the least privilege principle, and be granted only upon business need. Marvin App uses authentication and authorization to restrict access to the systems and services within the environment. Each user account is unique and is identifiable to an individual user. Segregation of duties is established on critical functions within the environment to minimize the risk of unauthorized changes to production systems.

Domain-account management requests are routed to the designated asset owner or an associated employee according to established account provisioning and de-provisioning processes for approval. Typically, access is controlled through the addition of individual user accounts to established domain security groups within Rippling and Google. Based on the configuration of a security group, any access requests require explicit approval from the assigned security group owner. Requests are automatically forwarded to the security group owner for approval in the system.

Employee status data is used to facilitate the provisioning and removal of user accounts in the system. Account management processes prevent the creation of an account for individuals who do not have valid HR records. Select users can request the removal of user accounts from the system. In addition, system owners can directly remove users from Security Groups. Upon termination, employees are required to return their workstations to Marvin App. Terminated employees are removed from the Rippling, and all access is terminated.

Automated mechanisms have been implemented to manage the appropriateness of access granted to information systems. Manual periodic reviews of individual accounts and security group memberships on assets are performed by authorized individuals, as appropriate, to evaluate whether access is still required. Remediation action is taken, as necessary, based on the review.

Policies and standards have been established and implemented to enforce appropriate user account password expiration, length, complexity, and history. All Marvin App personnel are required to follow Marvin App's password policy for all domains as well as local user accounts for all assets.

Access to the production environment is controlled through a designated set of access points and restricted to the product & engineering team. Users are authenticated to access points using credentials depending on where the production assets are located. Passwords, along with two-factor authentication used to access network devices, are restricted to authorized individuals and system processes based on job responsibilities and are changed on a periodic basis.

Cryptographic controls and approved algorithms are used for information protection within the production environment and are implemented based on Marvin App's policies and standards. Cryptographic keys are managed throughout their lifecycle (e.g., ownership, generation, storage, distribution, periodic rotation, and revocation) in accordance with key management procedures.

Marvin App maintains a detailed inventory of all information systems. All such assets are assigned ownership by a designated department or team within Marvin App and prioritized based on the asset's business value and criticality to the organization. The classification process is owned by the executive and the DevOps team. Information and data assets are subject to the data management policy that defines parameters for the ownership, classification, security, storage, and retention of data. Software and hardware assets are subject to the information systems management policy that defines parameters for the acquisition, development, maintenance, security, and disposal of information system assets. Steps are taken to protect assets commensurate with the respective asset's classification and its data sovereignty. A review of asset inventory, ownership, and classification is performed at least semi-annually.

The inventory of servers is monitored and maintained by the engineering and DevOps team. On a monthly basis, the executive team checks for completeness and accuracy of the inventory to ensure that it represents the production environment appropriately. Marvin App has created and implemented processes to control the delivery and removal of information assets through a centralized ticketing system. In addition, network architecture is maintained as part of the inventory process. Metadata of the assets is collected and maintained within the inventory that provides an overview and flow of the network.

System Operations

Technical standards and baselines have been established and communicated for production system deployments. Automated mechanisms and periodic scanning have been deployed to detect and troubleshoot exceptions and/or deviations from the baseline in the production environment. Where applicable, mechanisms are in place for Service to re-image production servers with the latest baseline configuration at least on a monthly frequency. Further, OS and product teams review and update configuration settings and baseline configurations at least annually.

Marvin App has implemented procedural and technical standards for the deployment of network devices. These standards include baseline configurations for network devices, network architecture, and approved protocols and ports. Marvin App regularly monitors network devices for compliance with technical standards and potentially malicious activities.

Marvin App has implemented agent-based monitoring infrastructure and custom script-based monitoring within the environment to provide automated logging and alerting capabilities. The logging solutions are enabled on all production systems. The monitoring system detects potentially unauthorized activity and security events, such as the creation of unauthorized local users and local groups. The monitoring agents are responsible for monitoring a defined set of user and administrator events, aggregating log events, and sending the aggregated log information to a centralized log repository at regular intervals.

Marvin App has established a policy that restricts the log and monitor access to only authorized staff with a business need to access such systems. Product teams determine the specific events that need to be captured in consideration with a baseline. The administrator, the operator, and system activities performed, such as logon/logoff within the environment, are logged and monitored.

For network devices, the Marvin App monitors, logs, and reports on critical/suspicious activities and deviations from established baseline security configurations for the network devices. Predefined events are reported, tracked, and followed up on, and security data is available for forensic investigations. The logs are retained centrally for forensics-related analysis and access to the logs follows the same procedures defined above.

Marvin App has implemented an alerting system to provide real-time alerting through the automatic generation of emails and alarms based on the log information captured by the monitoring infrastructure. Product teams are responsible for configuring the events to be alerted. The event and warning logs are routinely examined for anomalous behavior, and, when necessary, appropriate actions are taken in accordance with the incident handling procedures described in the Incident Management section. The product teams manage the response to malicious events, including escalation to and engaging specialized support groups. In addition, the Marvin App monitors relevant external information to stay up-to-date with current threat scenarios and countermeasures.

Marvin App carries out internal and external scans to identify vulnerabilities and assess the effectiveness of the patch management process. These scans are used to ensure compliance with baseline configuration templates, validate that relevant patches are installed, and identify vulnerabilities. The scanning reports are reviewed by Marvin App's DevOps as well as Product teams, and remediation efforts are conducted in a timely manner.

Security patches are applied immediately or during a scheduled release to the environment based on the severity of the vulnerability. Processes are in place to evaluate patches and their applicability to the environment. Once patches have been reviewed, and their criticality level determined, product teams determine the release cadence for implementing patches without service disruption.

Product teams follow a change process to modify the underlying OS within the platform. All changes are reviewed and tested, at a minimum, for their quality, performance, impact on other systems, recovery objectives, and security features before they are moved into production using a defined release process.

Penetration testing (pen test) is performed at least annually on the system. The pen test scope is determined based on the Marvin App's areas of risk and compliance requirements.

Marvin App has implemented an Incident Management framework that includes defined processes, roles, communications, responsibilities, and procedures for detection, escalation, and response to incidents internally and to customers.

Marvin App has established Incident Response procedures and centralized tracking tools, which consist of different channels for reporting production system incidents and weaknesses. Automated mechanisms include system monitoring processes for alerting security teams per defined and configured events, thresholds, or metric triggers. Incidents may also be reported via email. Customers are made aware of their responsibilities to report incidents that shall be looked into without any negative consequences. Marvin App's incident response provides 24x7 event/incident monitoring and response Service. The teams assess the health of various components along with access to detailed information when issues are discovered.

Additionally, Marvin App conducts yearly tests of the Incident Management SOPs and response capabilities. Reports related to information security events are provided to management on a quarterly basis.

Marvin App's product teams use the established incident classification, escalation, and notification process for assessing an incident's criticality and severity and accordingly escalating to the appropriate groups for timely action. The developers and engineering team document, track, and coordinate responses to incidents. Where required, security incidents are escalated to the privacy, legal, or executive management team(s) following established forensic procedures to support potential legal action after an information security incident.

Post-mortem activities are conducted for customer-impacting incidents or incidents with high-severity ratings. The post-mortems are reviewed by the engineering team during review meetings with senior management. Incident and security post-mortem trends are reviewed and evaluated on a periodic basis, and, where necessary, the platform or security program may be updated to incorporate improvements identified as a result of incidents.

Change Management

The Change Management process has been established to plan, schedule, approve, apply, distribute, and track changes to the production environment through designated responsibilities with the objective of minimizing risk and customer impact. It further controls the integrity and reliability of the environment while maintaining the pace of change required for business purposes.

Software, system, and configuration changes, including major releases, minor releases, and hotfixes, are managed through a formal change and release management procedure and tracked using a centralized ticketing system. The categorization of these changes is based on priority and risk associated with the change. Changes are requested, approved, tracked, and implemented throughout the release lifecycle, which includes product and engineering planning, release management, deployment, and post-deployment support phases. Change requests are documented, assessed for their risks, and evaluated/approved for acceptance by the designated personnel.

Patches are released through the periodic release cycle in accordance with change and release management procedures. Emergency out-of-band security patches are expedited for more immediate release.

Formal security and quality assurance testing are performed prior to the software release through each preproduction environment (i.e., development and test/sandbox) based on defined acceptance criteria. The results of the quality assurance testing are reviewed and approved by the appropriate personnel prior to moving the release to production. Changes are reviewed for their adherence to established change and release management procedures prior to closure. Once deployed, changes are monitored for success; failed implementations are immediately rolled back, and the change is not considered complete until it is implemented and validated to operate as intended.

The Marvin App product team's software development practices, outlined in its Software Development Lifecycle (SDLC) methodology, are aligned with the Marvin App's Secure Software Development Lifecycle Standard. The Standard introduces security and privacy control specifications during the feature/component design and throughout the development process, which are reviewed through designated security roles.

Marvin App's SDLC baseline includes tasks to be performed that identify tools or processes that ensure teams are developing their Service in a secure manner. As part of onboarding onto the SDLC process, the product teams (engineering, design, and product management) work together to determine any additional SDLC steps to be performed specifically for the service. Additionally, teams are required to perform threat modeling exercises which are reviewed and approved by the security and/or system architect. Each product team has a product owner who is responsible for ensuring the appropriate completion of the SDLC tasks. The product owner reviews the SDLC tasks and gives the overall sign-off for completion of the SDLC process.

COMPLEMENTARY USER ENTITY CONTROLS (CUEC)

Marvin App's controls related to the Marvin App service cover only a portion of overall internal control for each user entity of Marvin App. It is not feasible for the criteria related to the system to be achieved solely by the Marvin App service. Therefore, each user entity's internal control should be evaluated in conjunction with the Marvin App's controls and the related tests and results described in Section 4 of this report, taking into account the related complementary user entity controls identified for the specific criterion. For user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the identified complementary user entity controls have been implemented and are operating effectively.

The user entity controls presented should not be regarded as a comprehensive list of all controls that should be employed by user entities.

Management of user entities is responsible for the following:

Criteria	Complementary User Entity Controls (CUECs)
CC2.1	• User entities have policies and procedures to report any material changes to their overall control environment that may adversely affect the service being performed by the Marvin App Service according to contractually specified time frames. • Controls to provide reasonable assurance that Marvin App is notified of changes in: ○ user entity vendor security requirements ○ the authorized user's list
CC2.3	• It is the responsibility of the user entity to have policies and procedures to: ○ inform their employees/users that their information/data is being used and stored by Marvin App. ○ determine how to file inquiries, complaints, and disputes which would get passed onto Marvin App.
CC6.1	• User entities grant access to the Marvin App system to authorized and trained personnel. • User entities deploy physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity.
CC6.6	• Controls to provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by Marvin App.

SUBSERVICE ORGANIZATIONS AND COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOC)

Marvin App uses AWS and Heroku as subservice organizations for data center colocation Services. The Marvin App controls related to the system cover only a portion of the overall internal control for each user entity of the Marvin App service. The description does not extend to the service provided by the subservice organization that provides colocation Service for IT infrastructure. Section 4 of this report and the description of the system only cover the Trust Service Criteria and related controls of Marvin App and exclude the related controls of AWS.

Although the subservice organization has been carved out for the purposes of this report, certain Trust Service Criteria are intended to be met by controls at the subservice organization. CSOCs are expected to be in place at AWS related to physical security and environmental protection, as well as backup and recovery. AWS' physical security controls mitigate the risk of fires, power loss, climate, and temperature variabilities.

Marvin App management receives and reviews the SOC 2 report of AWS and Heroku on an annual basis. In addition, through its operational activities, Marvin App management monitors the Service performed by AWS & Heroku to determine whether operations and controls expected to be implemented at the subservice organization are functioning effectively. Management also has communication with the subservice organization to monitor compliance with the service agreement, stay abreast of changes planned at the hosting facility, and relay any issues or concerns to AWS management.

It is not feasible for the criteria related to the Marvin App to be achieved solely by the Marvin App. Therefore, each user entity's internal control must be evaluated in conjunction with the Marvin App controls and related tests and results described in Section 4 of this report taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Criteria	Complementary Subservice Organization Controls (CSOCs)
CC6.4	AWS is responsible for restricting data center access to authorized personnel. AWS is responsible for the 24x7 monitoring of data centers by closed-circuit cameras and security personnel.
CC7.2	AWS is responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers. AWS is responsible for protecting data centers against disruption in power supply to the processing environment by an uninterruptible power supply (UPS). AWS is responsible for overseeing the regular maintenance of environmental protections at data centers.

REPORT USE

The description does not omit or distort information relevant to Marvin App while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

Section IV

DESCRIPTION OF TEST OF CONTROLS AND RESULTS THEREOF

Relevant trust services criteria and Equafin Corp.-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 Equafin Corp.'s controls were suitably designed and operating effectively to achieve the specified criteria for the security, availability, processing integrity, and confidentiality categories set forth in TSP Section 100, 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*, throughout the period September 01, 2022 to August 31, 2023.

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

Trust Services Criteria for the Security Category	***Description of Equafin Corp.'s Controls***	***Service Auditor Test of Controls***	***Results of Service Auditor Test of Controls***
Control Environment			
CC 1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected an employee performance evaluation to determine that the company conducts an annual evaluation for all employees.	No exceptions noted.
	The company performs reference checks on new employees.	Inspected the documentation to determine that the company performs reference checks on new employees.	No exceptions noted.
	The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.	Inspected the company's example contractor agreement to determine that it includes a code of conduct or reference to the company code of conduct.	No exceptions noted.
	The company requires contractors to sign a confidentiality agreement at the time of engagement.	Inspected documentation to determine that the company requires contractors to sign a confidentiality agreement at the time of engagement.	No exceptions noted.
	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Inspected the company's Code of Conduct to determine that it was in place, accessible to all employees, and that all employees must accept it upon hire.	No exceptions noted.
	The company requires employees to sign a confidentiality agreement during onboarding.	Inspected documentation to determine that the company requires employees to sign a confidentiality agreement during onboarding.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of Equafin Corp.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
CC 1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board members have sufficient expertise to oversee management's ability to design, implement, and operate information security controls. The board engages third-party information security experts and consultants as needed.	Inspected documentation to determine that the company's board members have sufficient expertise to oversee management's ability to design, implement, and operate information security controls.	No exceptions noted.
	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected the company's board of directors charter or policy to determine that it outlines its oversight responsibilities for internal control.	No exceptions noted.
	The company's board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the company.	Inspected the most recent board of directors meeting minutes and agenda to determine that the company's board of directors meets at least annually.	No exceptions noted.
	The company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's relevant risk. The board provides feedback and direction to management as needed.	Inspected the most recent Board of Directors meeting minutes and agenda to determine that the company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's relevant risk. The board provides feedback and direction to management as needed.	No exceptions noted.
CC 1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected a sample job description to determine that roles and responsibilities are formally assigned, documented, and made available to all employees.	No exceptions noted.
	The company maintains an organizational chart that describes the organizational structure and reporting lines.	Inspected the most recent company organization chart to determine that it describes the organizational structure and reporting lines.	No exceptions noted.
	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected the company's security policies to determine that the company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	No exceptions noted.
	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected the company's board of directors charter or policy to determine that it outlines its oversight responsibilities for internal control.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of Equafin Corp.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
CC 1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected a sample job description to determine that roles and responsibilities are formally assigned, documented, and made available to all employees.	No exceptions noted.
	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected an employee performance evaluation to determine that the company conducts an annual evaluation for all employees.	No exceptions noted.
	The company performs reference checks on new employees.	Inspected the documentation to determine that the company performs reference checks on new employees.	No exceptions noted.
	The company requires employees to complete security awareness training within thirty days of hire and annually thereafter.	Inspected documentation to determine that the company requires employees to complete security awareness training within thirty days of hire and annually thereafter.	No exceptions noted.
CC 1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected a sample job description to determine that roles and responsibilities are formally assigned, documented, and made available to all employees.	No exceptions noted.
	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected an employee performance evaluation to determine that the company conducts an annual evaluation for all employees.	No exceptions noted.
	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Inspected the company's Code of Conduct to determine that it was in place, accessible to all employees, and that all employees must accept it upon hire.	No exceptions noted.
Communication and Information			
CC 2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Inspected the vulnerability scans to determine that they were performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of Equafin Corp.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected documentation to determine that the company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively and that corrective actions are taken based on relevant findings.	No exceptions noted.
	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected the infrastructure configuration to determine that the company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	No exceptions noted.
CC 2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected a sample job description to determine that roles and responsibilities are formally assigned, documented, and made available to all employees.	No exceptions noted.
	The company communicates system changes to authorized internal users.	Inspected the internal communication to determine that the company communicates system changes to authorized internal users.	No exceptions noted.
	The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns.	Inspected documentation to determine that the company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns.	No exceptions noted.
	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's security policies to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected the company's security policies to determine that the company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of Equafin Corp.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company provides a description of its products and services to internal and external users.	Inspected documentation to determine that the company provides a description of its products and services to internal and external users.	No exceptions noted.
	The company requires employees to complete security awareness training within thirty days of hire and annually thereafter.	Inspected documentation to determine that the company requires employees to complete security awareness training within thirty days of hire and annually thereafter.	No exceptions noted.
	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that they are documented and reviewed at least annually by management.	No exceptions noted.
CC 2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected the company website to determine that the company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	No exceptions noted.
	The company has written agreements in place with vendors and related third parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected the company's written agreements with vendors and related third parties to determine that they include confidentiality and privacy commitments applicable to that entity.	No exceptions noted.
	The company notifies customers of critical system changes that may affect their processing.	Inspected the company website to determine that they notify customers of critical system changes that may affect their processing.	No exceptions noted.
	The company provides a description of its products and services to internal and external users.	Inspected documentation to determine that the company provides a description of its products and services to internal and external users.	No exceptions noted.
	The company provides guidelines and technical support resources relating to system operations to customers.	Inspected the company website to determine that they provide guidelines and technical support resources relating to system operations to customers.	No exceptions noted.
	The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).	Inspected documentation to determine that the company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of Equafin Corp.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
Risk Assessment			
CC 3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management program to determine that it provides guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected documentation to determine that the company specifies its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.
CC 3.2 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.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the company's business continuity/disaster recovery (BC/DR) plan to determine that it was in place and approved and that the company tests it at least annually.	No exceptions noted.
	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management program to determine that it provides guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
	The company has a vendor management program in place. Components of this program include critical third-party vendor inventory, vendor's security and privacy requirements, and review of critical third-party vendors at least annually.	Inspected the company's vendor management program to determine that it provides a process for documenting and managing vendor relationships, an inventory of critical third-party vendors, vendor security and privacy requirements, and an annual review of critical third-party vendors.	No exceptions noted.
	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected documentation of the company's risk assessments to determine that: these are performed on an annual basis, threats and changes to service commitments are identified and the risks are formally assessed, and the potential for fraud and how fraud may impact the achievement of objectives are considered.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of Equafin Corp.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
CC 3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management program to determine that it provides guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected documentation of the company's risk assessments to determine that: these are performed on an annual basis, threats and changes to service commitments are identified and the risks are formally assessed, and the potential for fraud and how fraud may impact the achievement of objectives are considered.	No exceptions noted.
CC 3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the company's configuration management procedure to determine that it was in place and ensured that system configurations were deployed consistently throughout the environment.	No exceptions noted.
	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management program to determine that it provides guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the company's penetration testing to determine that it was performed at least annually and that a remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	No exceptions noted.
	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected documentation of the company's risk assessments to determine that: these are performed on an annual basis, threats and changes to service commitments are identified and the risks are formally assessed, and the potential for fraud and how fraud may impact the achievement of objectives are considered.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of Equafin Corp.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
Monitoring Activities			
CC 4.1 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.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Inspected the vulnerability scans to determine that they were performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	No exceptions noted.
	The company has a vendor management program in place. Components of this program include critical third-party vendor inventory, vendor's security and privacy requirements, and review of critical third-party vendors at least annually.	Inspected the company's vendor management program to determine that it provides a process for documenting and managing vendor relationships, an inventory of critical third-party vendors, vendor security and privacy requirements, and an annual review of critical third-party vendors.	No exceptions noted.
	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected documentation to determine that the company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively and that corrective actions are taken based on relevant findings.	No exceptions noted.
	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the company's penetration testing to determine that it was performed at least annually and that a remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	No exceptions noted.
CC 4.2 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.	The company has a vendor management program in place. Components of this program include critical third-party vendor inventory, vendor's security and privacy requirements, and review of critical third-party vendors at least annually.	Inspected the company's vendor management program to determine that it provides a process for documenting and managing vendor relationships, an inventory of critical third-party vendors, vendor security and privacy requirements, and an annual review of critical third-party vendors.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of Equafin Corp.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected documentation to determine that the company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively and that corrective actions are taken based on relevant findings.	No exceptions noted.
Control Activities			
CC 5.1 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.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management program to determine that it provides guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that they are documented and reviewed at least annually by management.	No exceptions noted.
CC 5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's systems development life cycle (SDLC) methodology to determine that it governs the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements.	No exceptions noted.
	The company's access control policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access.	Inspected the company's Access Control Policy to determine that it was in place, and approved, and documented requirements for adding, modifying, and removing user access.	No exceptions noted.
	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that they are documented and reviewed at least annually by management.	No exceptions noted.
CC 5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and procedures that put policies into action.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected a sample job description to determine that roles and responsibilities are formally assigned, documented, and made available to all employees.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of Equafin Corp.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management program to determine that it provides guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's systems development life cycle (SDLC) methodology to determine that it governs the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements.	No exceptions noted.
	The company has a vendor management program in place. Components of this program include critical third-party vendor inventory, vendor's security and privacy requirements, and review of critical third-party vendors at least annually.	Inspected the company's vendor management program to determine that it provides a process for documenting and managing vendor relationships, an inventory of critical third-party vendors, vendor security and privacy requirements, and an annual review of critical third-party vendors.	No exceptions noted.
	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the company's retention and disposal procedures to determine that it provides guidance on secure retention and disposal of company and customer data.	No exceptions noted.
	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's security policies to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the changes to software and infrastructure components to determine that they were authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions noted.
	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected documentation to determine that the company specifies its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of Equafin Corp.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company's data backup policy documents requirements for the backup and recovery of customer data.	Inspected the data backup policy to determine that it documents requirements for backup and recovery of customer data.	No exceptions noted.
	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that they are documented and reviewed at least annually by management.	No exceptions noted.
Logical and Physical Access			
CC 6.1 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.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected user access to in-scope system components to determine that they are based on job role and function or require a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.
	The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the company's data classification policy to determine that it ensures that confidential data is properly secured and restricted to authorized personnel.	No exceptions noted.
	The company maintains a formal inventory of production system assets.	Inspected documentation to determine that the company maintains a formal inventory of production system assets.	No exceptions noted.
	The company requires authentication to production data stores to use authorized secure authentication mechanisms, such as a unique SSH key.	Inspected the company's authentication to production data stores to determine that they use authorized secure authentication mechanisms, such as a unique SSH key.	No exceptions noted.
	The company requires authentication to systems and applications to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the company's authentication to systems and applications to determine that they use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the company's authentication to the production network to determine that they use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
	The company requires passwords for in-scope system components to be configured according to the company's policy.	Inspected the company's passwords for in-scope system components to determine that it is configured according to the company's policy.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of Equafin Corp.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company restricts access to migrate changes to production to authorized personnel.	Inspected access to migrate changes to production to determine that the company restricts privileged access to authorized personnel.	No exceptions noted.
	The company restricts privileged access to databases to authorized users with a business need.	Inspected access to databases to determine that the company restricts privileged access to authorized users with a business need.	No exceptions noted.
	The company restricts privileged access to encryption keys to authorized users with a business need.	Inspected the company's Cryptography Policy to determine that the company restricts privileged access to encryption keys to authorized users with a business need, and reviewed the access logs, user permissions, user profiles, and the access request process to verify that only authorized users with legitimate business need can access encryption keys.	No exceptions noted.
	The company restricts privileged access to the application to authorized users with a business need.	Inspected access to the application to determine that the company restricts privileged access to authorized users with a business need.	No exceptions noted.
	The company restricts privileged access to the firewall to authorized users with a business need.	Inspected the firewall configuration to determine that the company restricts privileged access to authorized users with a business need.	No exceptions noted.
	The company restricts privileged access to the operating system to authorized users with a business need.	Inspected access to the operating system to determine that the company restricts privileged access to authorized users with a business need.	No exceptions noted.
	The company restricts privileged access to the production network to authorized users with a business need.	Inspected access to the production network to determine that the company restricts privileged access to authorized users with a business need.	No exceptions noted.
	The company's access control policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access.	Inspected the company's Access Control Policy to determine that it was in place, and approved, and documented requirements for adding, modifying, and removing user access.	No exceptions noted.
	The company's data stores housing sensitive customer data are encrypted at rest.	Inspected the company's data stores housing sensitive customer data to determine that they are encrypted at rest.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of Equafin Corp.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company's network is segmented to prevent unauthorized access to customer data.	Inspected the company's network configuration to determine that it is segmented to prevent unauthorized access to customer data.	No exceptions noted.
	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Inspected the company's production systems to determine that they can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	No exceptions noted.
	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company's production systems to determine that they can only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
CC 6.2 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.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the termination checklist to determine that access is revoked for terminated employees within SLAs.	No exceptions noted.
	The company conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the access reviews for the in-scope system components to determine that access is restricted appropriately. Required changes are tracked to completion.	No exceptions noted.
	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected user access to in-scope system components to determine that they are based on job role and function or require a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.
	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the company's authentication to the production network to determine that they use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of Equafin Corp.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company's access control policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access.	Inspected the company's Access Control Policy to determine that it was in place, and approved, and documented requirements for adding, modifying, and removing user access.	No exceptions noted.
CC 6.3 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.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the termination checklist to determine that access is revoked for terminated employees within SLAs.	No exceptions noted.
	The company conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the access reviews for the in-scope system components to determine that access is restricted appropriately. Required changes are tracked to completion.	No exceptions noted.
	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected user access to in-scope system components to determine that they are based on job role and function or require a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.
	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the company's authentication to the production network to determine that they use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
	The company's access control policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access.	Inspected the company's Access Control Policy to determine that it was in place, and approved, and documented requirements for adding, modifying, and removing user access.	No exceptions noted.
CC 6.4 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.	The entity 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 implemented and maintained by subservice organizations.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of Equafin Corp.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
CC 6.5 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.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the termination checklist to determine that access is revoked for terminated employees within SLAs.	No exceptions noted.
	The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	Inspected the company's Asset Management Policy to determine that it provides guidance for proper asset disposal. 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 exceptions noted.
	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the company's retention and disposal procedures to determine that it provides guidance on secure retention and disposal of company and customer data.	No exceptions noted.
	The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	Inspected documentation to determine that the company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	No exceptions noted.
CC 6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result, identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the infrastructure supporting the service to determine that they are patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.
	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the company's authentication to the production network to determine that they use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
	The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.	Inspected the firewall rulesets to determine that it is reviewed at least annually. Required changes are tracked to completion.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of Equafin Corp.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the company's intrusion detection system to determine that it is configured to continuously monitor the company's network and early detection of potential security breaches.	No exceptions noted.
	The company uses firewalls and configures them to prevent unauthorized access.	Inspected the company's firewall configuration to determine that they prevent unauthorized access.	No exceptions noted.
	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the company's secure data transmission protocols to determine that they encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.
	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Inspected the company's network and system hardening standards to determine that they are reviewed at least annually based on industry best practices.	No exceptions noted.
	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Inspected the company's production systems to determine that they can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	No exceptions noted.
	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company's production systems to determine that they can only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
CC 6.7 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.	The company encrypts portable and removable media devices when used.	Inspected the company's portable and removable media devices to determine that they are encrypted when used.	No exceptions noted.
	The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.	Inspected the company's mobile device management (MDM) system to determine that it is in place to centrally manage mobile devices supporting the service.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of Equafin Corp.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the company's secure data transmission protocols to determine that they encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.
CC 6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.	Inspected the company's anti-malware technology to determine that it is configured to be updated routinely, logged, and installed on all relevant systems.	No exceptions noted.
	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's systems development life cycle (SDLC) methodology to determine that it governs the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements.	No exceptions noted.
	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result, identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the infrastructure supporting the service to determine that they are patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.
System Operations			
CC 7.1 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.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Inspected the vulnerability scans to determine that they were performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	No exceptions noted.
	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the company's configuration management procedure to determine that it was in place and ensured that system configurations were deployed consistently throughout the environment.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of Equafin Corp.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the changes to software and infrastructure components to determine that they were authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions noted.
	The company's formal policies outline the requirements for the following functions related to IT / Engineering: vulnerability management and system monitoring.	Inspected the company's formal policies to determine that they outline the requirements for IT-related functions such as vulnerability management and system monitoring.	No exceptions noted.
	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected documentation of the company's risk assessments to determine that: these are performed on an annual basis, threats and changes to service commitments are identified and the risks are formally assessed, and the potential for fraud and how fraud may impact the achievement of objectives are considered.	No exceptions noted.
CC 7.2 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.	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected the infrastructure monitoring tool to determine that it is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	No exceptions noted.
	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Inspected the vulnerability scans to determine that they were performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	No exceptions noted.
	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result, identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the infrastructure supporting the service to determine that they are patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of Equafin Corp.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the company's intrusion detection system to determine that it is configured to continuously monitor the company's network and early detection of potential security breaches.	No exceptions noted.
	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected the infrastructure configuration to determine that the company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	No exceptions noted.
	The company's formal policies outline the requirements for the following functions related to IT / Engineering: vulnerability management and system monitoring.	Inspected the company's formal policies to determine that they outline the requirements for IT-related functions such as vulnerability management and system monitoring.	No exceptions noted.
	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the company's penetration testing to determine that it was performed at least annually and that a remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	No exceptions noted.
CC 7.3 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.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's security policies to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the company's security and privacy incidents to determine that they are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
CC 7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Inspected the vulnerability scans to determine that they were performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of Equafin Corp.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result, identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the infrastructure supporting the service to determine that they are patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.
	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's security policies to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
	The company tests its incident response plan at least annually.	Inspected the company's incident response plan to determine that it is tested at least annually.	No exceptions noted.
	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the company's security and privacy incidents to determine that they are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
CC 7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the company's business continuity/disaster recovery (BC/DR) plan to determine that it was in place and approved and that the company tests it at least annually.	No exceptions noted.
	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's security policies to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
	The company tests its incident response plan at least annually.	Inspected the company's incident response plan to determine that it is tested at least annually.	No exceptions noted.
	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the company's security and privacy incidents to determine that they are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of Equafin Corp.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
Change Management			
CC 8.1 The entity authorizes, designs, develops acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Inspected the vulnerability scans to determine that they were performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	No exceptions noted.
	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's systems development life cycle (SDLC) methodology to determine that it governs the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements.	No exceptions noted.
	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result, identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the infrastructure supporting the service to determine that they are patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.
	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the changes to software and infrastructure components to determine that they were authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions noted.
	The company restricts access to migrate changes to production to authorized personnel.	Inspected access to migrate changes to production to determine that the company restricts privileged access to authorized personnel.	No exceptions noted.
	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Inspected the company's network and system hardening standards to determine that they are reviewed at least annually based on industry best practices.	No exceptions noted.
	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the company's penetration testing to determine that it was performed at least annually and that a remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of Equafin Corp.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
Risk Mitigation			
CC 9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management program to determine that it provides guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
	The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	Inspected the Business Continuity and Disaster Recovery Plans to determine that they outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	No exceptions noted.
	The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	Inspected the company's cybersecurity insurance to determine that it was in place to mitigate the financial impact of business disruptions.	No exceptions noted.
	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected documentation of the company's risk assessments to determine that: these are performed on an annual basis, threats and changes to service commitments are identified and the risks are formally assessed, and the potential for fraud and how fraud may impact the achievement of objectives are considered.	No exceptions noted.
CC 9.2 The entity assesses and manages risks associated with vendors and business partners.	The company has a vendor management program in place. Components of this program include critical third-party vendor inventory, vendor's security and privacy requirements, and review of critical third-party vendors at least annually.	Inspected the company's vendor management program to determine that it provides a process for documenting and managing vendor relationships, an inventory of critical third-party vendors, vendor security and privacy requirements, and an annual review of critical third-party vendors.	No exceptions noted.
	The company has written agreements in place with vendors and related third parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected the company's written agreements with vendors and related third parties to determine that they include confidentiality and privacy commitments applicable to that entity.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of Equafin Corp.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
Additional Criteria for Availability			
A 1.1 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.	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected the infrastructure monitoring tool to determine that it is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	No exceptions noted.
	The company evaluates system capacity on an ongoing basis, and system changes are implemented to help ensure that processing capacity can meet demand.	Inspected documentation to determine that the company evaluates system capacity on an ongoing basis, and system changes are implemented to help ensure that processing capacity can meet demand.	No exceptions noted.
A 1.2 The entity authorizes, designs, develops acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the company's business continuity/disaster recovery (BC/DR) plan to determine that it was in place and approved and that the company tests it at least annually.	No exceptions noted.
	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management program to determine that it provides guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
	The company has environmental monitoring devices in place and configured to automatically generate an alert to management for environmental incidents.	Inspected documentation to determine that the company has environmental monitoring devices in place and configured to automatically generate an alert to management for environmental incidents.	No exceptions noted.
	The company's data backup policy documents requirements for the backup and recovery of customer data.	Inspected the data backup policy to determine that it documents requirements for backup and recovery of customer data.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of Equafin Corp.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected documentation of the company's risk assessments to determine that: these are performed on an annual basis, threats and changes to service commitments are identified and the risks are formally assessed, and the potential for fraud and how fraud may impact the achievement of objectives are considered.	No exceptions noted.
A 1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the company's business continuity/disaster recovery (BC/DR) plan to determine that it was in place and approved and that the company tests it at least annually.	No exceptions noted.
	The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	Inspected the Business Continuity and Disaster Recovery Plans to determine that they outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	No exceptions noted.
	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the company's intrusion detection system to determine that it is configured to continuously monitor the company's network and early detection of potential security breaches.	No exceptions noted.
	The company's data backup policy documents requirements for the backup and recovery of customer data.	Inspected the data backup policy to determine that it documents requirements for backup and recovery of customer data.	No exceptions noted.
Additional Criteria for Processing Integrity			
PI 1.1 The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.	A Data Integrity Policy and procedure has been established that provides guidelines with respect to data integrity and how to define data necessary to support a product or service.	Inspected the company's Data Integrity Policy to determine that it has been established and that it provides guidelines with respect to data integrity and how to define data necessary to support a product or service.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of Equafin Corp.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	The organization has formal agreements with its customers to define the completeness and accuracy of the system data outputs and the definition of the data. The agreements include procedures and responsibilities that need to be performed by the organization and the customers to ensure that the data is accurate and complete during the output. Any deviations from expected results are followed up, evaluated, and resolved in a timely manner.	Inspected the company's formal agreements with its customers to determine that it defines the completeness and accuracy of the system data outputs and the definition of the data. The agreements include procedures and responsibilities that need to be performed by the organization and the customers to ensure that the data is accurate and complete during the output. Any deviations from expected results are followed up, evaluated, and resolved in a timely manner.	No exceptions noted.
	The organization maintains an inventory of production information assets including details on asset ownership, data classification, and location. The asset inventory listing is reviewed and updated by management on an as-needed basis.	Inspected company records to determine that the organization maintains an inventory of production information assets including details on asset ownership, data classification, and location. The asset inventory listing is reviewed and updated by management on an as-needed basis.	No exceptions noted.
PI 1.2 The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.	Input record counts are traced from entry to final processing on a daily basis. Any differences in input record counts are traced from entry to final processing on a daily basis and are investigated further for timely resolution.	Inspected the company's data reconciliation to determine that input record counts have been traced from entry to final processing on a daily basis. Any differences in input record counts that are traced from entry to final processing on a daily basis are investigated further for timely resolution.	No exceptions noted.
	System inputs are measured and recorded completely, accurately, and timely to meet the entity's processing integrity commitments and system requirements.	Inspected the company's system inputs to determine that it has been measured and recorded completely, accurately, and timely to meet the entity's processing integrity commitments and system requirements.	No exceptions noted.
PI 1.3 The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.	Data is processed completely, accurately, and timely as authorized to meet the entity's processing integrity commitments and system requirements.	Inspected the company's data verification records to determine that data has been processed completely, accurately, and timely as authorized to meet the entity's processing integrity commitments and system requirements.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of Equafin Corp.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
	Organization has implemented a system to detect errors that occur during processing. An incident management process is invoked for timely resolution of identified issues in accordance with the system commitments.	Inspected the company's log of system errors and Incident Management Policy to determine that the organization has implemented a system to detect errors that occur during processing. An incident management process is invoked for timely resolution of identified issues in accordance with the system commitments.	No exceptions noted.
PI 1.4 The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.	Data is stored and maintained completely, accurately, and in a timely manner for its specified life span to meet the entity's processing integrity commitments and system requirements.	Inspected the records of data storage configurations, and data lifetime configuration to determine that data is stored and maintained completely, accurately, and in a timely manner for its specified life span to meet the entity's processing integrity commitments and system requirements.	No exceptions noted.
	Processes have been implemented for the distribution of output data to intended users only in accordance with system commitments. The distribution of output data is tracked and logged.	Inspected company records to determine that processes have been implemented for the distribution of output data to intended users only in accordance with system commitments. The distribution of output data is tracked and logged.	No exceptions noted.
	Weekly full-system and daily incremental backups are performed using an automated system and replicated to an offsite location. Backups are monitored for failure using an automated system.	Inspected the company's weekly full-system and daily incremental backups to determine that it had been performed using an automated system and replicated to an offsite location. Backups are monitored for failure using an automated system.	No exceptions noted.
PI 1.5 The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.	Customer data is encrypted at rest (stored and backed up) using strong encryption technologies.	Inspected the company's encryption settings for customer data at rest to determine that it has been encrypted at rest (stored and backed up) using strong encryption technologies.	No exceptions noted.
	Organization archives system records related to the input or output processing in accordance with defined retention and archival procedures.	Inspected the company's retention and archival procedures to determine that the organization archives system records related to the input or output processing in accordance with defined retention and archival procedures.	No exceptions noted.

Trust Services Criteria for the Security Category	*Description of Equafin Corp.'s Controls*	*Service Auditor Test of Controls*	*Results of Service Auditor Test of Controls*
Additional Criteria for Confidentiality			
C 1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the company's data classification policy to determine that it ensures that confidential data is properly secured and restricted to authorized personnel.	No exceptions noted.
	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the company's retention and disposal procedures to determine that it provides guidance on secure retention and disposal of company and customer data.	No exceptions noted.
	The company has written agreements in place with vendors and related third parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected the company's written agreements with vendors and related third parties to determine that they include confidentiality and privacy commitments applicable to that entity.	No exceptions noted.
	The company prohibits confidential or sensitive customer data, by policy, from being used or stored in non-production systems/environments.	Inspected confidential or sensitive customer data, by policy, to determine that it is prohibited from being used or stored in non-production systems/environments.	No exceptions noted.
	The company requires authentication to systems and applications to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the company's authentication to systems and applications to determine that they use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
C 1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	Inspected the company's Asset Management Policy to determine that it provides guidance for proper asset disposal. 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 exceptions noted.
	The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	Inspected documentation to determine that the company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	No exceptions noted.