coral

SYSTEM AND ORGANIZATION CONTROLS (SOC) 3 REPORT ON MANAGEMENT'S ASSERTION RELATED TO ITS

Platform

Relevant to Security

For the period August 7, 2024 to November 7, 2024

TOGETHER WITH INDEPENDENT AUDITORS' REPORT

Prepared by:

Sensiba

Table of Contents

1. Independent Service Auditors' Report

To the Management of Coral LLC (Coral)

Scope

We have examined Coral's accompanying assertion titled "Assertion of Coral Management" (assertion) that the controls within Coral's Platform (system) were effective throughout the period August 7, 2024 to November 7, 2024, to provide reasonable assurance that Coral's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA*, Trust Services Criteria.*

Service Organization's Responsibilities

Coral 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 Coral's service commitments and system requirements were achieved. Coral has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Coral is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditors' Responsibilities

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

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.

- Assessing the risks that controls were not effective to achieve Coral’s service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Coral’s service commitments and system requirements based on the applicable trust services criteria.

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

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

Inherent Limitations

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 were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the 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.

Opinion

In our opinion, management’s assertion that the controls within Coral’s Platform were effective throughout the period August 7, 2024 to November 7, 2024, to provide reasonable assurance that Coral’s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Sensiba LLP

San Jose, California

January 30, 2025

2. Assertion of Coral Management

We are responsible for designing, implementing, operating, and maintaining effective controls within the Coral LLC (Coral) Platform (system) throughout the period August 7, 2024 to November 7, 2024, to provide reasonable assurance that Coral's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "Description of Coral's Platform," (description) and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period August 7, 2024 to November 7, 2024, to provide reasonable assurance that Coral's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus - 2022)* in AICPA*, Trust Services Criteria.*

Coral's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in the accompanying system description.

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

We assert that the controls within the system were effective throughout the period August 7, 2024 to November 7, 2024, to provide reasonable assurance that Coral's service commitments and system requirements were achieved based on the applicable trust services criteria.

Signed by Coral Management

January 30, 2025

3. Description of Coral’s Platform

Company Background

The Coral Platform was founded with the mission of transforming the U.S. healthcare system by creating an open marketplace that connects employers, health plans, and top-tier providers. It offers a platform where self-funded employer medical plans and payers can access a vast network of over 5,000 locations, including independent ambulatory surgical centers, hospitals, and specialists. Coral simplifies the healthcare process by providing upfront pricing transparency and faster payments for providers, all while reducing the complexity and costs typically associated with healthcare claims.

The platform enables both providers and payers to engage in direct contract programs, allowing them to bypass intermediaries and lower healthcare costs by 20-30%. Providers can offer their services to a growing pool of over 5 million individuals, while payers benefit from streamlined processes and improved patient care. Coral’s innovative features include communication tools, referral management, and customizable workflows, making it easier for users to manage healthcare services efficiently.

Founded in 2016, Coral has processed over 500,000 appointments and continues to grow, with its mission to reduce friction and improve care for everyone involved

Services Provided

The Coral Platform is a multi-user software-as-a-service (SaaS) application that facilitates the management and processing of healthcare referrals between payers and providers. The platform enables seamless interactions and automated workflows across all stages of the referral process, including:

- Marketplace of Providers: Qualified payers search our marketplace of healthcare providers who offer bundled-priced healthcare services tailored to specific needs.
- Referral Management: Payers send referrals to selected providers. The Coral Platform automates the routing, tracking, and monitoring of referrals.
- End-to-End Process Handling: The platform handles all communication between the payer and provider, from the initial referral to the conclusion of services.
- Invoicing and Payment: Coral Platform manages the invoicing process, ensuring that payments are processed securely and efficiently. Providers submit their invoices, and the system facilitates payment status tracking between payers and providers.
- Data and Reporting: The platform provides real-time dashboards, summaries, and exportable reports for both payers and providers. Users can view referral statuses, financial information, and compliance with regulatory requirements.
- Compliance and Security: Coral Platform is designed to ensure all interactions are compliant with healthcare regulations, including HIPAA and SOC2. The system uses encryption and secure channels for all data exchanges.

Principal Service Commitments and System Requirements

Coral Platform designs its processes and procedures to meet the service commitments it makes to user entities, as well as the laws and regulations that govern healthcare services. The key service commitments and system requirements include:

- Security and Access Control: Coral Platform employs role-based access control to ensure that users only access the information necessary for their role. This protects sensitive healthcare information and limits exposure to unauthorized personnel.
- Data Encryption: Customer data is protected through encryption both at rest and in transit. All sensitive healthcare and personal data are encrypted using industry-standard technologies, ensuring compliance with HIPAA and SOC2 regulations.
- Service Availability: Coral Platform is designed for high availability and reliability. Redundant infrastructure and automated failover mechanisms are in place to minimize downtime and ensure that services always remain available to users.
- Operational Requirements: The platform follows strict operational guidelines, including regular system updates, patching, and monitoring to ensure continuous compliance with security requirements and operational excellence.
- User Agreements and SLAs: Service commitments, including security and availability, are documented and communicated in the form of EULA and AUP. These documents clearly define the terms of service and the responsibilities of both Coral and its customers.
- Regulatory Compliance: Coral Platform adheres to the requirements set forth by HIPAA, SOC2, and other relevant healthcare regulations. Regular audits and assessments ensure that the platform meets all legal and compliance requirements.

Components of the System

Infrastructure

Primary Infrastructure		
Hardware	Type	Purpose
GCP	Kubernetes Clusters	Hosts the platform’s services.
GCP	SQL Instances	Databases that store the data collected for processing.
GCP	Storage Bucket	Long term storage for data retention.
GCP	Load balancer	Act as ingress to Kubernetes Clusters.
GCP	VPC, Firewall	Network services for our clusters routing of data.
GCP	Cloud network security	For security and network zoning.
GCP	Cloud DNS	Hosts DNS zones and names.

Primary Infrastructure		
Hardware	Type	Purpose
GCP	Cloud Logging	Log retention and log lookup and creation of alerts based on defined rule sets.
GCP	Container Registry	Storage for docker images

Software

Primary Infrastructure	
Software	Purpose
Google GSuite SSO	Provides Single Sign-On (SSO) authentication for internal users accessing cloud resources.
Github Version Control	GIT repository manager
Github Actions	Automation for CI/CD pipelines
Nexus	Artifact storage
Sonarqube	Code quality checking
Terraform	Infrastructure as code.
Prometheus	Platform monitoring
Slack	Communications
Keycloak	sign-on with identity and access management
Jenkins	Automation, CI/CD Pipelines

People

Coral Platform services are supported by various teams:

- Corporate: Includes executives and administrative staff responsible for financial management, compliance, and legal matters.
- Operations: Handles day-to-day platform functions, such as payer-provider interactions, referrals, and issue resolution.
- IT Support: Provides technical support, infrastructure management, and ensures platform availability. Teams include help desk, infrastructure, and system administration.
- Security: Monitors security threats, ensures regulatory compliance, and maintains security policies.
- Development: Responsible for developing and maintaining platform software and integrations, including feature enhancements and bug fixes.
- Product Support: Responsible for replying to customer inquiries and supporting the platform users regarding any service offered by the platform.
- DevOps: Manages the deployment pipelines, infrastructure as code (IaC), continuous integration/continuous deployment (CI/CD) processes, and ensures that development, testing, and production environments are consistently up to date and secure.
- On-ground support: 1st line support responsible for visiting new clients and providing employee training. This team handles initial client interactions and basic troubleshooting.

The 2nd line support team addresses more complex issues that require deeper technical expertise, typically escalated from the 1st line. 3rd line support, which includes Quality Control (QC) and Development teams is engaged for advanced problem-solving and technical challenges that cannot be resolved by the previous support levels.

Data

Data Source	Purpose
Healthcare Transaction Data	This includes but not limited to referral requests, status updates, and provider information.
Invoices and Payments	All financial transactions related to services between payers and providers.
System Logs and Error Logs	Collected for monitoring, troubleshooting, and auditing purposes.
Encrypted Backups	All data is backed up and stored securely using modern encryption techniques.

Processes, Policies and Procedures

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

Physical Security

All data is hosted by Google Cloud Platform (GCP). GCP data centers do not allow GCP employees physical access. At present, GCP does not maintain any office space and all work is conducted remotely.

Logical Access

Coral Platform uses a role-based security model to control access to system resources. The logical access control processes and procedures include:

- **Role-Based Access Control (RBAC)**: All users are assigned roles that dictate the level of access they have within the system. Access to sensitive data is restricted based on the user's role, ensuring users can only access information necessary for their job function.
- **User Identification and Authentication**:
  - All system users must authenticate using **Google GSuite SSO (Single Sign-On)** before accessing any system resources.
  - For systems that do not support SSO, users must authenticate with strong passwords that comply with Coral's password policies.

- **Multi-Factor Authentication (MFA)**: Users accessing cloud resources must enable token-based multi-factor authentication (MFA) for an additional layer of security.
- **Secure Access to Cloud Resources**:
  - All access to cloud-based services, including GCP resources, is secured using SSL-encrypted connections.
  - Access to administrative interfaces is restricted to authorized personnel with elevated privileges, which are reviewed periodically.
- **Access Provisioning**:
  - Access requests are processed and granted based on predefined roles. Two days prior to a new employee's start date, their manager provides a list of required access permissions.
  - The permissions are reviewed annually to ensure employees only retain the necessary access for their roles.
- **Periodic Reviews**:
  - On an annual basis, access rules are reviewed by Coral's operations and security teams. Any modifications to privileged roles are made based on this review to ensure only authorized personnel have elevated access.
- **Deactivation of Access**:
  - When employees leave the company, their access to all system resources is automatically revoked on their last day of employment. Access revocation is handled through the HR system, which integrates with the access management platform.

Computer Operations – Backups

Coral Platform has established processes and procedures to ensure that customer data is securely backed up and available in case of system failures or disasters. These processes include:

- **Backup Frequency**: Data backups are performed regularly according to predefined schedules. The backup frequency is designed to minimize data loss and ensure timely recovery of critical information.
- **Backup Storage Location**: Backups are stored securely in **Google Cloud Platform (GCP)** storage buckets and Databases, which are encrypted using GCP's Key Management Service (KMS) to ensure that only authorized personnel can access the backup data.
- **Encryption**: All backup data is encrypted both at rest and in transit using industry-standard encryption algorithms. Access to the encryption keys is tightly controlled using GCP's Identity and Access Management (IAM) permissions.
- **Automated Monitoring**: Backup jobs are monitored automatically, and any failures or exceptions trigger alerts to Coral's DevOps team. In case of a failure, the team investigates the root cause and re-runs the backup job as part of the next scheduled backup process.

- **Backup Testing**: Regular backup restoration tests are conducted to ensure that data can be recovered in case of a failure or disaster. This helps verify the integrity and reliability of the backups.
- **Data Retention**: Coral Platform follows a data retention policy that ensures backups are kept for a specific period based on regulatory requirements and business needs. After the retention period, backup data is securely deleted.

Computer Operations – Availability

Coral Platform has implemented several processes and procedures to ensure the availability of its services. These include:

- **Redundant Infrastructure**: The Coral Platform is hosted on **Google Cloud Platform (GCP)**, utilizing multiple availability zones and redundant Kubernetes clusters. This setup ensures that if one zone or zone experiences an issue, services can continue running in another zone or cluster without interruption.
- **Capacity Monitoring**: Coral monitors the capacity of its infrastructure, including computing resources, storage, and network bandwidth. This helps ensure that the system is operating efficiently and that there is enough capacity to meet customer demands.
- **Incident Response and Recovery**: Incident response policies and procedures are in place to guide personnel in reporting and responding to incidents affecting availability, such as system outages or infrastructure failures. Coral has an established incident escalation matrix to ensure timely responses to service disruptions.
- **Automated Failover**: The platform has automated failover mechanisms for critical components. In the event of a failure, redundant systems automatically take over to maintain service availability.
- **Patch Management**: A formal patch management process is implemented to ensure that the system remains up to date with security patches and software updates. Coral analyzes users' pattern to patch systems seamlessly without down time or service disruptions.
- **Disaster Recovery**: Coral has a disaster recovery plan in place that includes procedures for restoring services in case of a catastrophic failure. Regular disaster recovery tests are conducted to ensure the plan's effectiveness.

Change Control

Coral Platform follows a structured and documented change control process to manage application and infrastructure changes. These processes include:

- **Approval Process**: Management approval is required for all changes before they are deployed to production. Approvals are documented through the ticketing system, which tracks all stages of the change control process.

- **Change Requests and Initiation**: All changes to the Coral Platform, whether application or infrastructure-related, are initiated through formal change requests that are tracked on a central ticketing system. Each request includes a description of the change, its purpose, and any potential impact on users.
- **Development and Testing**:
  - Changes are developed in a controlled environment separate from the production system.
  - All changes undergo testing, including Quality Assurance (QA) and User Acceptance Testing (UAT), to ensure they function as intended before being deployed to production.
- **Version Control**: Coral uses version control software to maintain source code integrity. The system tracks changes to code and maintains a history of all modifications, allowing rollback if necessary.
- **Patch Management**: The patch management process ensures that Coral's systems remain up to date with the latest security patches and software updates. Before applying patches, Coral reviews the potential impact on system availability and security.
- **Deployment to Production**: Changes are deployed to production after being tested on a staging environment and monitored to make sure that the changes do not adversely disrupt the production environment.
- **Documentation**: Detailed documentation is maintained for all changes, including testing results. This ensures traceability and accountability for any changes made to the system.

Data Communications

Coral Platform has implemented robust data communication protocols to ensure secure and reliable communication between its systems and users. These include:

- **Firewall Protection**: Firewalls are in place to filter unauthorized inbound and outbound traffic. The firewall rules are configured to allow only explicitly authorized connections and expose only necessary services, minimizing exposure to potential threats.
- **Network Address Translation (NAT)**: Coral utilizes NAT to manage internal IP addresses, ensuring that internal systems are not directly exposed to the public internet.
- **Secure Communication Channels**: All communication between Coral Platform and external systems (e.g., user devices, healthcare provider systems) is secured using SSL/TLS encryption, ensuring data integrity and confidentiality during transmission.
- **Infrastructure and Administration Access**: Authorized employees can securely access the platform administration panels remotely through a secured connection using SSL/TLS, Accounts used are protected by MFA and Identity and Access management rules for authorization.
- **Penetration Testing**: Regular penetration tests are conducted to assess the security posture of the Coral Platform. These tests identify vulnerabilities in the system that could be exploited by malicious actors, and findings are patched and tested to ensure the platform's security.

- **Vulnerability Scanning**: Vulnerability scanning is performed quarterly. These scans assess Coral's network and systems to ensure there are no unpatched vulnerabilities or security misconfigurations.
- **Incident Response**: In case of a detected security incident, Coral's incident response team is notified immediately. The team follows established incident response procedures to mitigate the issue and ensure the security of the system.

Boundaries of the System

The scope of this report includes the Services performed by Coral. This report does not include the data center hosting services provided by GCP.

The applicable trust services criteria and the related controls:

Common Criteria (Security)
Security refers to the protection of information during its collection or creation, use, processing, transmission, and storage and systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Control Environment

Integrity and Ethical Values

Coral Platform places a high emphasis on integrity and ethical values in its control environment. Specific activities implemented include:

- **Code of Conduct**: Coral Platform has a formally documented Code of Conduct that communicates the company's values and ethical standards. Employees are required to sign an acknowledgment confirming they understand and adhere to these principles.
- **Confidentiality Agreements**: Employees are required to sign confidentiality agreements as part of their onboarding process, committing not to disclose proprietary or client information to unauthorized parties.
- **Background Checks**: As part of the hiring process, Coral conducts background checks to ensure that employees meet the company's ethical and security standards.

Commitment to Competence

Coral's management defines competence as the knowledge and skills necessary to perform assigned tasks. Control activities include:

- **Defined Roles and Responsibilities**: Management establishes clear role descriptions with specific skills and knowledge requirements, ensuring that employees are well-equipped for their positions.
- **Ongoing Training**: Coral provides regular training programs to keep employees up to date with the latest skills, technologies, and compliance requirements, ensuring they can effectively perform their duties.

Management's Philosophy and Operating Style

Management at Coral fosters a culture of risk awareness and careful business decision-making. Specific control activities include:

- **Management Briefings**: Management regularly conducts briefings on regulatory and industry changes that impact the services provided ensuring that the team stays updated and compliant.
- **Executive Meetings**: Senior leadership holds weekly meetings to discuss business risks, strategic initiatives and issues that could impact the platform or the company's objectives.

Organizational Structure and Assignment of Authority and Responsibility

Coral has an organizational structure that supports its operational goals and assigns authority and responsibility effectively:

- **Organizational Charts**: These charts are in place to define roles, responsibilities and reporting structures ensuring that authority is clearly communicated.
- **Role-Based Accountability**: Employees are made aware of their responsibilities and reporting lines are established to ensure accountability for their actions.

Human Resource Policies and Practices

Coral's human resource policies focus on ethical business practices, employee retention and high operational efficiency. Control activities include:

- **Onboarding Process**: New employees sign acknowledgment forms for the employee handbook and confidentiality agreements during orientation.
- **Employee Evaluations**: Performance evaluations are conducted annually to assess employee competence and adherence to company standards.
- **Termination Procedures**: When employees leave the company, a formal termination checklist is followed to ensure proper deactivation of access to company systems and the return of company property.

Risk Assessment Process

Coral Platform has a formalized risk assessment process in place to identify, evaluate, and manage risks that may impact the ability to provide secure, compliant, and reliable services. This process is integrated across all operations and includes continuous evaluation of both internal and external risks. Key aspects of the risk assessment process include:

- **Identification of Risks**: Coral Platform identifies risks across various domains, including operational, strategic, compliance, and technical risks. The process involves a cross-functional team including management, security, DevOps and operations personnel who assess potential vulnerabilities or weaknesses that could impact service delivery.
- **Risk Categories**:
  - **Operational Risk**: Regular reviews are conducted to assess risks related to operational changes such as staffing, process modifications, and technological updates. Coral also identifies risks from system failures or outages, ensuring contingency plans are in place for maintaining service levels.
  - **Strategic Risk**: Management actively monitors trends and shifts in the healthcare and technology sectors. This includes the adoption of new technologies, changes in business models, and industry competition. Strategic risks are evaluated based on their potential impact on Coral's long-term objectives and market positioning.
  - **Compliance Risk**: Coral adheres to stringent healthcare and data privacy regulations such as HIPAA, SOC2, and others. The risk assessment process regularly reviews legal and regulatory changes, ensuring that Coral remains compliant and that systems are adapted to meet evolving requirements.
  - **Financial Risk**: Management evaluates risks that could impact financial stability, including operational inefficiencies, market changes, and unexpected costs related to service interruptions or security breaches.
- **Risk Impact and Likelihood Evaluation**: Each identified risk is assessed based on its potential impact and the likelihood of occurrence. Coral assigns risk ratings, allowing the management team to prioritize risks that pose the greatest threat to operations or compliance.
- **Risk Mitigation Strategies**: Coral develops mitigation strategies for each identified risk. This includes implementing new controls, updating processes, or making adjustments to existing systems. For operational risks, Coral has documented procedures for responding to incidents,
- including redundancy and failover mechanisms to ensure continuous service availability.
- **Risk Monitoring**: The risk management team continuously monitors the environment to identify emerging risks. Coral uses various monitoring tools, including infrastructure monitoring (Datadog) and security assessments, to detect and respond to risks in real-time. Regular internal audits are conducted to ensure risk mitigation measures remain effective.
- **Communication of Risks**: Identified risks and their mitigation strategies are communicated regularly to key stakeholders, including senior management and department heads. Risk assessments are documented and reviewed at quarterly management meetings to ensure ongoing awareness and timely action.
- **Continuous Improvement**: Coral's risk assessment process is dynamic evolving with changes in the business environment. Post-incident reviews are conducted to analyze the effectiveness of risk mitigation strategies, and the findings are incorporated into the risk management framework for future improvements.

Information and Communications Systems

Coral's information and communication systems ensure that all necessary information is identified, captured, processed and shared promptly:

- **Weekly Operational Calls**: Operational staff hold regular calls to discuss efficiencies, review policies and communicate any strategic changes.
- **On Ground Meetings**: Bi-annual meetings are held with staff to provide company updates and address issues that impact operations or employee roles and any changes.
- **Security Policies**: Security policy updates are communicated to the appropriate teams via email to ensure that everyone is aware of changes to the control environment and ensuring the adherence to security best practices.

Monitoring Controls

Coral Platform has implemented comprehensive monitoring controls to ensure the effectiveness of its internal control environment and to maintain continuous compliance with regulatory requirements. Monitoring is an ongoing process that ensures controls are functioning as intended and are updated when necessary.

The key elements of the monitoring controls include:

- **Continuous Monitoring**:
  - Coral Platform uses automated monitoring tools to continuously assess the performance and security of its infrastructure. Tools such as **Google Cloud Logger** monitor system uptime, performance metrics and alert the operations team in real-time about potential issues, such as performance degradation or security anomalies.
  - **Drata** is used to monitor Coral's compliance with frameworks like SOC2 and HIPAA. Drata continuously assesses Coral's security posture, compliance with internal policies and adherence to regulatory standards, notifying relevant personnel of any deviations or issues that require immediate attention.
  - Coral performs automated vulnerability scans on a regular basis to identify any potential security gaps in its infrastructure. These scans are conducted using third-party security tools and any identified issues are addressed as part of Coral's incident response plan.
- **Ongoing Evaluations**:
  - Coral's management conducts regular evaluations of the controls implemented within the system. These evaluations focus on ensuring the system adheres to operational, security, and compliance standards. Any identified deviations from the expected outcomes are documented and addressed promptly.
  - System logs and audit trails are reviewed periodically by both the security and DevOps teams to detect unusual behavior. These logs are automatically generated and include details about system access, configuration changes and transaction data. Any anomalies trigger alerts that are escalated for investigation.
- **Corrective Actions**:
  - When monitoring tools or reviews identify an issue, Coral follows a well-defined process to address the issue. Corrective actions are initiated based on the severity of the problem, with high-priority issues being escalated immediately to

    - senior management and relevant teams. Issues identified through **Drata** are tracked to resolution to ensure compliance deviations are addressed before they pose significant risk.
    - All corrective actions are documented in an internal tracking system, allowing the management team to review the effectiveness of the response and implement necessary process improvements. These actions are also discussed in periodic management review meetings to identify trends and prevent future occurrences.
- **Regular Audits and Reviews**:
    - Coral conducts both internal and external audits to ensure that its control environment is effective and compliant with relevant regulations. Internal audits are performed by the compliance team using tools like Drata to evaluate processes, procedures, and system configurations. These audits help in identifying areas that require improvement or enhancement.
    - External audits are performed annually by third-party auditors as part of Coral's SOC2 and HIPAA compliance requirements. The audit reports provide an independent validation of the platform's control environment and its alignment with regulatory standards.
- **Employee Monitoring and Awareness**:
    - Employee adherence to security policies and procedures is closely monitored. Coral uses a combination of automated monitoring and manual reviews to track employee access to sensitive systems and data. Access logs are reviewed regularly to ensure compliance with role-based access control policies.
    - Employees are provided with ongoing training and updates about security policies, ensuring that they remain informed about the latest threats and best practices. This helps maintain a high level of security awareness across the organization.
- **Incident Response Monitoring**:
    - Coral Platform has a formal incident response plan that is integrated with its monitoring systems. Any detected anomalies or potential security breaches trigger the incident response process, which involves alerting relevant personnel, isolating the issue, and resolving it as quickly as possible. The incident response plan is regularly tested to ensure its effectiveness in addressing real-time threats.
- **Reporting Deficiencies**:
    - Monitoring tools and audits may identify deficiencies in the control environment. When deficiencies are identified, they are recorded in Coral's internal tracking system and are prioritized based on their potential impact. High-severity issues are addressed immediately, while lower-priority issues are scheduled for remediation as part of routine maintenance.
    - Management reviews reported deficiencies in quarterly risk management meetings, where corrective actions are discussed and tracked to ensure resolution. Any trends identified during these meetings are used to improve overall processes and controls within the organization.
- **Compliance Monitoring with Drata**:
    - Drata continuously monitors Coral's adherence to SOC2 and HIPAA frameworks, tracking compliance across all areas, including security, availability, and confidentiality. Any gaps or non-compliance issues are flagged by Drata and resolved through well-documented procedures. Drata's platform also provides dashboards that offer real-time visibility into compliance status for management and external auditors.

- Compliance reports generated by Drata are used to inform management of Coral’s ongoing compliance posture, ensuring that any necessary actions are taken proactively to prevent issues from escalating.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

Criteria Not Applicable to the System

All relevant trust services criteria were applicable to Coral’s Platform.

Subservice Organizations

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

The following subservice organization controls should be implemented by GCP to provide additional assurance that the trust services criteria described within this report are met.

Security Category	
Criteria	*Controls expected to be in place*
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity’s objectives.	

Security Category	
Criteria	*Controls expected to be in place*
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	GCP is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where the entity's system resides.
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	

Security Category	
Criteria	*Controls expected to be in place*
CC6.4 - The entity restricts physical access to facilities and protected information assets (e.g., datacenter facilities, backup media storage and other sensitive locations) to authorized personnel to meet the entity's objectives.	GCP is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers where the entity's system resides.

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

- Holding periodic discussions with vendors and subservice organization
- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

Complementary User Entity Controls

Coral's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the SOC 2 Criteria related to Coral's services to be solely achieved by Coral 's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Coral's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the SOC 2 Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Coral.
2. User entities are responsible for notifying Coral of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Coral services by their personnel.

5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Coral services.
6. User entities are responsible for providing Coral with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Coral of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.