Cosmoverse, Inc.

System and Organization Control (SOC 2) Type II Report

Report on Description of Cosmoverse, Inc's ProcIndex Platform and on Suitability of the Design and Operational Effectiveness of Controls Relevant to Security, Availability, and Processing Integrity

For the Audit Period

January 15, 2026, to April 15, 2026

PERCILCHOFE

Audit Performed by: Percilchofe CPA LLC

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations

Table of Contents

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

1.Independent Service Auditor's Report

To the Management of Cosmoverse, Inc

Scope

We have examined the attached description of the system of Cosmoverse, Inc.(the "Service Organization" or "Cosmoverse") related to the ProcIndex Platform for the audit period January 15, 2026 to April 15, 2026 (the "description") based on the criteria for a description of the service organization's system set forth in the description criteria DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report ("description criteria") and the suitability of the design and operating effectiveness of controls included in the description for the audit period January 15, 2026 to April 15, 2026 to provide reasonable assurance that Cosmoverse's service commitments and system requirements would be achieved based on the trust services criteria for Security, Availability, and Processing Integrity ("applicable trust services criteria") set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Privacy, Confidentiality and Processing Integrity.

Cosmoverse uses Railway, Supabase, Cloudflare R2, Resend, Clerk, and GitHub as Subservice Organizations. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Cosmoverse, to achieve Cosmoverse's service commitments and system requirements based on the applicable trust services criteria. The description presents Cosmoverse's system, its controls, and the types of complementary subservice organization controls that the service organization assumes have been suitably designed and implemented at subservice organizations.

The description also indicates that Cosmoverse's controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of Cosmoverse's controls are suitably designed and implemented, along with related controls at the service organization. The description does not disclose the actual controls at the subservice organizations.

Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

Management of Cosmoverse 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 the service commitments and system requirements were achieved. Cosmoverse has provided the accompanying assertion titled, "Management Assertion Provided by Service Organization" (Assertion) about the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria. Cosmoverse is responsible for (1) preparing the description and assertion; (2) the completeness, accuracy, and method of presentation of the description and assertion; (3) providing the services covered by the description; (4) identifying the risks that would threaten the achievement of the service organization's service commitments and system requirements; and (5) designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve its service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description, on the suitability of the design, and on the operating effectiveness of the controls described therein to achieve the service organization's service commitments and system requirements, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the description is presented in accordance with the description criteria, (2) the controls described therein are suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria, and (3) the controls operated effectively 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. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Performing procedures to obtain evidence about whether the controls stated in the description are presented in accordance with the description criteria and operated effectively.
- Evaluating the overall presentation of the description, the suitability of the control objectives, and the suitability of the 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 related to the examination engagement.

Inherent Limitations

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 its own particular needs.

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. Also, the projection to the future of any evaluation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the service organization's service commitments and system requirements, is subject to the risk that the system may change or that controls at a service organization may become ineffective.

Opinion

In our opinion, in all material respects:

- The description presents the ProcIndex Platform system that was designed and implemented for the audit period January 15, 2026, to April 15, 2026, in accordance with the description criteria.

- The controls stated in the description were suitably designed for the audit period January 15, 2026, to April 15, 2026, to provide reasonable assurance that Cosmoverse's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively.

- The controls stated in the description operated effectively for the audit period January 15, 2026, to April 15, 2026, to provide reasonable assurance that Cosmoverse's service commitments and system requirements were achieved based on the applicable trust services criteria.

Restricted Use

This report is intended solely for the information and use of Cosmoverse, user entities of the ProcIndex Platform for the audit period January 15, 2026 to April 15, 2026 and prospective user entities, independent auditors and practitioners providing services to such user entities 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, or other parties, including complementary user entity controls and subservice organization controls assumed in the design of the service organization's controls.
- Internal control and its limitations.
- User entity responsibilities and how they interact with related controls at the service organization.
- 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.

Percilchofe CPA LLC

Digitally signed by Percilchofe CPA LLC
Date: 2026.05.28 11:50:01 +05'30'

Percilchofe CPA LLC
License No.: 1188
Date: May 28, 2026

SECTION 2

MANAGEMENT ASSERTION

2. Management Assertion Letter

Management Assertion Provided by Cosmoverse, Inc.

We have prepared the accompanying description of systems in Section 3 of Cosmoverse, Inc.(the "Service Organization" or "Cosmoverse") for the audit period January 15, 2026 to April 15, 2026 related to the ProcIndex Platform, based on criteria for a description of a service organization's system set forth in the Description Criteria DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report ("Description Criteria"). The description is intended to provide report users with information about our ProcIndex Platform that may be useful when assessing the risks from interactions with the System, particularly information about system controls that Cosmoverse has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria for Security, Availability, and Processing Integrity set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, and Processing Integrity (applicable trust services criteria).

Cosmoverse uses Railway, Supabase, Cloudflare R2, Resend, Clerk, and GitHub as Subservice Organizations. The Description includes only the controls of Cosmoverse and excludes controls of Subservice Organizations. The Description also indicates that certain trust services criteria specified therein can be met only if Subservice Organization's controls assumed in the design of Cosmoverse's controls are suitably designed and operating effectively along with the related controls at the Service Organization. The Description does not extend to controls of Subservice Organizations.

The Description also indicates that certain trust services criteria specified in the Description can be met only if complementary user entity controls assumed in the design of Cosmoverse's controls are suitably designed and operating effectively, along with related controls at the Service Organization. The Description does not extend to controls of user entities.

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

- The Description presents the System that was designed and implemented for the audit period January 15, 2026, to April 15, 2026, in accordance with the Description Criteria.
- The controls stated in the Description were suitably designed and operated effectively to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated as described and if user entities applied the complementary user entity controls and the subservice organization applied the controls assumed in the design of Cosmoverse's controls for the audit period January 15, 2026 to April 15, 2026.

For Cosmoverse, Inc.

Signature: 
Name: Neha Suresh Kumar
Designation: CEO
Date: May 26th, 2026

SECTION 3

DESCRIPTION OF THE SYSTEM

Description of Systems Provided by the Service Organization

3.1 Overview of the Company

3.1.1 Operational Role and Business Model

Cosmoverse, Inc.is a technology company headquartered in San Francisco, CA that develops agentic tools that automate accounting operations and streamline finance workflows. The company's flagship product, ProcIndex, provides an agentic accounting automation platform designed to help finance teams automate critical accounting and finance operations including accounts payable, accounts receivable, cash application, invoice review, collections, and related finance operations workflows.

3.1.2 Strategic Importance and Growth

Cosmoverse serves finance and accounting teams across various industries, enabling them to reduce manual workload, improve processing accuracy, accelerate cash conversion cycles, and scale operations efficiently. The ProcIndex platform leverages agentic automation technology combined with human review workflows to process accounting transactions, manage vendor and customer communications, and integrate with enterprise resource planning (ERP) and accounting systems.

3.2 Scope

This SOC 2 Type II Report covers the ProcIndex platform operated by Cosmoverse, Inc. For the period from January 15, 2026 to April 15, 2026. The scope of this examination includes:

- The ProcIndex web application for finance operations management
- Accounts payable automation, including invoice intake, review, matching, and approval workflows
- Accounts receivable automation, including invoice tracking, collections workflows, reminders, and customer follow-up
- Agentic workflow automation for accounting and finance operations
- Human review queues for exceptions, approvals, disputes, and action-required items
- Customer, vendor, invoice, payment, and workflow data management
- ERP and accounting system integrations
- Email and communication workflows used for AP and AR operations
- User access management, organization/team management, and role-based permissions
- Backend APIs, background jobs, and supporting cloud infrastructure used to operate the ProcIndex platform

3.3 Overview of Services

3.3.1 Core Functions and Operations

ProcIndex is an agentic accounting automation platform that helps finance teams automate accounts payable, accounts receivable, cash application, invoice review, collections, and related finance operations workflows. The platform provides the following core capabilities:

- Automated invoice processing and three-way matching for accounts payable workflows
- Automated collections management and payment tracking for accounts receivable operations
- Agentic workflow automation that processes routine accounting tasks while routing exceptions to human review
- Integration with ERP and accounting systems for data synchronization and transaction posting

- Email-based communication workflows for vendor inquiries and customer collections
- Audit trails and workflow logs supporting compliance and reconciliation requirements

3.3.2 Operational Support for Business Units

The company is organized into functional teams that support the design, delivery, and operation of the ProcIndex platform:

- Engineering: Responsible for design, development, testing, deployment, maintenance, and security of the ProcIndex application, backend services, infrastructure, integrations, and automation workflows. Engineering owns vulnerability remediation, code review, system monitoring, incident response support, and technical controls.
- Product & Sales: Responsible for product strategy, roadmap planning, customer requirements, go-to-market activities, customer communications, and ensuring product commitments are clearly understood and communicated. Supports customer onboarding, feedback collection, and alignment between customer needs and product development.
- Operations: Responsible for business operations, finance and administrative processes, vendor management, policy coordination, compliance support, and ensuring internal procedures are followed. Coordinates security and compliance activities, including evidence collection, vendor reviews, and process documentation.
- IT: Responsible for internal technology administration, employee access provisioning and deprovisioning, device and account management, endpoint security, and support for internal systems used by employees.

3.4 Principal Service Commitments and System Requirements

Cosmoverse is committed to delivering secure, available, and accurately processing services to its customers. To fulfill these service commitments and support the achievement of system objectives, the ProcIndex platform is underpinned by the following system requirements:

Security

- Access to customer accounting and finance data is limited to authorized users and personnel based on business need, role-based permissions, and documented security procedures.
- System features and configuration settings are designed to authorize user access while restricting unauthorized users from accessing information not needed for their role.
- Operational procedures for managing security incidents and breaches, including notification procedures, are established and maintained.

Availability

- System performance and availability monitoring mechanisms help ensure consistent delivery of the system and its components.
- Customer requests are responded to in a reasonably timely manner.
- Operational procedures support the achievement of availability commitments to user entities.
- Database backups are performed daily through Supabase managed database backups.
- Backup restoration and recovery testing is performed periodically to validate integrity and recoverability of backup data.

Processing Integrity

- System processing is complete, valid, accurate, timely, and authorized to meet organizational objectives.
- Input, processing, and output controls ensure data integrity, including validation checks and error handling mechanisms.

- Change management processes ensure that system changes are tested, approved, and implemented without compromising data integrity.
- Automated validation rules and exception handling identify missing, inconsistent, duplicate, or unusual data for review.

3.5 Relevant Aspects of Control Environment, Risk Assessment, and Monitoring

3.5.1 Control Environment

Integrity and Ethical Values

Cosmoverse maintains policies and procedures that define standards for ethical conduct, confidentiality, and data protection. New hires and contractors are required to acknowledge the Company Handbook and accept confidentiality and non-disclosure agreements upon hire. Management establishes a tone emphasizing accountability, integrity, and adherence to security and privacy practices.

Organization Structure

Cosmoverse establishes organizational structure through defined leadership responsibilities, role-based access controls, documented security procedures, assigned ownership for key security functions, and management oversight of security, compliance, and operational risks. The executive team provides strategic direction and approves key policies and procedures governing system operations and security controls.

Human Resources

Personnel security practices support the hiring, onboarding, training, performance management, and offboarding of employees and contractors. All personnel are required to acknowledge confidentiality obligations and complete security awareness training. Access provisioning and deprovisioning procedures are managed by the executive team with a service level agreement of one day for both provisioning and deprovisioning activities.

3.5.2 Risk Assessment

Cosmoverse has established a risk management framework to identify, assess, and respond to risks that could impact service commitments and system requirements. The Risk Assessment and Treatment Policy defines the process for identifying operational, technical, and security risks; evaluating their potential impact and likelihood; and implementing appropriate risk treatment strategies. Risk assessments consider threats to system security, availability, and processing integrity, including risks associated with subservice providers, system changes, and evolving threat landscapes.

3.5.3 Monitoring

Cosmoverse monitors system operations and control effectiveness through a combination of automated monitoring, periodic reviews, and incident management processes. Application logs, deployment logs, and operational metrics are captured through Railway and related platform tooling. System availability and performance are monitored continuously, with alerts configured for critical operational events. Quarterly access reviews are performed to validate that user access remains appropriate based on current roles and responsibilities.

3.5.4 Information and Communication

Cosmoverse communicates system and service commitments to customers through customer agreements, order forms, security and compliance documentation, product documentation, onboarding materials, and direct customer communications. These commitments include the scope of services provided, availability and support expectations, data protection responsibilities, security practices, and applicable service-level or operational commitments. Updates or material changes are communicated through email, in-app notices, documentation updates, or direct account communications.

3.5.5 Communication

Internal communication supports the functioning of controls through documented policies and procedures, team collaboration tools including Email and Slack, and regular operational reviews. Security incidents and operational issues are communicated through defined incident response and escalation procedures documented in the Incident Response Policy.

3.6 Information Security

3.6.1 Logical Access

Logical access to the ProcIndex platform and supporting infrastructure is managed through authentication and authorization controls:

- User authentication is provided through Clerk, a third-party authentication and identity management service.
- Access to production systems and infrastructure is restricted to authorized engineering personnel.
- Role-based access controls are implemented within the application to restrict user access to data and functionality based on assigned roles and permissions.
- Quarterly access reviews are performed to validate that user access remains appropriate.
- Access provisioning and deprovisioning procedures are executed within one day of request approval or employment termination.

3.6.2 Physical Security

Physical security for production systems is the responsibility of subservice organizations. Railway provides application hosting with physical data center security controls. Supabase provides managed database services with physical security controls for database infrastructure. Cosmoverse relies on these subservice providers to maintain appropriate physical security controls for hosted infrastructure and data.

3.6.3 Change Management

Changes to the ProcIndex platform are managed through a defined change management process documented in the Change Management Policy. The process includes:

- Code changes are tracked through GitHub version control with pull request and code review workflows.
- Changes are tested in development environments prior to production deployment.
- Deployment to production is performed through Railway's deployment pipeline with automated build and deployment processes.
- Deployment logs and change records are maintained for audit and troubleshooting purposes.

3.6.4 Incident Management

Security incidents and operational issues are managed through procedures defined in the Incident Response Policy. The process includes incident detection, assessment, containment, investigation, resolution, and post-incident review. Incidents are tracked and documented to support root cause analysis and continuous improvement. Customer notification procedures are established for security incidents that may impact customer data or service availability.

3.6.5 Third Party Service Delivery

Cosmoverse engages subservice providers to support infrastructure, platform services, and operational capabilities. Vendor relationships are managed through procedures defined in the Vendor Management Policy. Key subservice providers include:

- Railway: Application hosting and deployment services
- Supabase: Managed production database services and database backup services

- Cloudflare R2: Object storage services for invoice attachments and supporting documents
- Resend: Email sending and inbound email processing services
- Clerk: Authentication and identity management services
- GitHub: Source code repository and version control
- Vendor reviews include evaluation of security posture, compliance attestations where available, and contractual commitments to data protection and service availability.

3.6.6 Business Continuity Management

Cosmoverse maintains business continuity procedures to support system availability and data recovery. Database backups are performed daily through Supabase managed backup services. Based on this backup frequency, Cosmoverse defines a Recovery Point Objective (RPO) of up to 24 hours for database data. The target Recovery Time Objective (RTO) is 24 hours for restoration of core services, depending on incident scope, database restore time, and application redeployment requirements. Backup and recovery procedures are reviewed and tested at least quarterly or after material infrastructure changes.

3.7 Complementary User Entity Controls (CUECs)

Cosmoverse's controls are designed with the assumption that certain complementary controls are implemented and operating effectively at user entities. The effectiveness of Cosmoverse's controls is dependent, in part, on user entities implementing and maintaining these complementary controls. User entities are responsible for:

- Implementing appropriate access controls to restrict user access to the ProcIndex application based on job responsibilities and business need.
- Promptly notifying Cosmoverse of employee terminations, role changes, or other events requiring access modification or revocation.
- Reviewing and validating the accuracy and completeness of data provided to and received from the ProcIndex platform.
- Maintaining appropriate controls over integrations with ERP and accounting systems, including credential management and access logging.
- Establishing and maintaining procedures for reviewing and approving workflow outputs, exception items, and agent recommendations before final acceptance or execution.
- Implementing appropriate network security controls and endpoint protection for devices used to access the ProcIndex platform.

3.8 Complementary Sub-Service Organization Controls (CSOCs)

Cosmoverse uses subservice organizations to support infrastructure, platform services, and system operations. The effectiveness of Cosmoverse's controls relies, in part, on controls implemented and operating effectively at these subservice organizations. Subservice organizations are responsible for:

Sub-Service Organization	Complementary Sub-Service Organization Control
Railway	Physical security of data centres, infrastructure availability and performance monitoring, network security controls, and infrastructure backup and disaster recovery procedures.
Supabase	Physical security of database infrastructure, database platform security controls, encryption of data at rest, database backup execution and retention, and database availability monitoring.
Cloudflare R2	Physical security of storage infrastructure, object storage platform security, encryption of data at rest, and object storage availability.
Resend	Email delivery infrastructure security, email sending and receiving platform controls, and email service availability.

Sub-Service Organization	Complementary Sub-Service Organization Control
Clerk	Authentication infrastructure security, identity and access management platform controls, secure credential storage, and authentication service availability.
GitHub	Source code repository security, access controls for repositories, version control integrity, and repository availability.

Cosmoverse obtains and reviews available SOC 2 or equivalent attestation reports from subservice providers on at least an annual basis to evaluate the design and operating effectiveness of controls at subservice organizations. Any identified complementary subservice organization controls are assessed for applicability and incorporated into Cosmoverse's control framework where relevant.

SECTION 4

INFORMATION PROVIDED BY THE SERVICE AUDITOR

4.Trust Services Criteria, Description of Related Controls, Tests of Controls and Results of Tests

4.1 SOC 2 Overview

This Report on Controls at a Service Organization Relevant to Trust Services Criteria for Security, Availability, and Processing Integrity and the Suitability of the Design and Operating Effectiveness of Controls is intended to provide interested parties with information sufficient to understand the basic structure of controls within Cosmoverse. This report, when coupled with an understanding of controls in place at user locations, is intended to permit evaluation of the total system of internal control surrounding transactions processed through the reviewed systems.
Our examination was restricted to selected services and applicable trust services criteria provided to system users by Cosmoverse and, accordingly, did not extend to controls in effect at user's other locations. It is each interested party's responsibility to evaluate this information in relation to controls in place at each user location in order to assess the total system of internal control. The user and the Cosmoverse portions of the system must be evaluated together. If effective user controls are not in place, the Cosmoverse controls may not compensate for such weakness.

4.2 Objectives of this Examination

Our examination included interviews with key personnel, review of available documentation and security, availability, and processing integrity procedures as appropriate, and observation and inspection of sample controls surrounding services provided by the Cosmoverse systems. Our examinations were designed to clarify understanding of the information contained in the system description.

Cosmoverse relevant Trust Services Criteria for Security, Availability, and Processing Integrity, their related controls and test of controls and results thereof, are presented in the following table. The objectives of trust services controls are to provide reasonable, but not absolute, assurance about such things as:

- Security – the system is protected against unauthorized access (both physical and logical).
- Availability – the system is available for operation and use as committed or agreed.
- Processing Integrity – system processing is complete, valid, accurate, timely, and authorized to meet organizational objectives.

4.3 Control Environment Elements

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for other components of internal control, providing discipline and structure. In addition to the tests of design and operating effectiveness of controls identified by Cosmoverse, our procedures include test of the following relevant elements of Cosmoverse's control environment:

4.3.1 Risk Assessment and Risk Management

Cosmoverse designed and implemented controls to identify, assess, and manage risks that could impact its ability to meet its service commitments and system requirements. These controls include a formally defined risk management framework covering operational, technical, and security risks. Cosmoverse has established processes to define risk tolerances, perform risk assessments, and assign risk ratings based on identified threats. Risk response strategies are developed, assigned to responsible owners, and tracked through to closure, with oversight by management.

4.3.2 Human Resources and Personnel Controls

Cosmoverse designed and implemented controls related to personnel security, including policies for hiring, onboarding, training, and termination. Personnel are required to acknowledge confidentiality and security policies upon hire.

Security awareness training is provided to personnel. Access provisioning and deprovisioning procedures are executed within defined service level agreements. Quarterly access reviews validate that access remains appropriate based on current roles and responsibilities.

4.3.3 Vendor and Third-Party Management

Cosmoverse designed and implemented controls to manage relationships with subservice providers and other third parties. Vendor management procedures include evaluation of security posture, review of compliance attestations where available, and establishment of contractual commitments to data protection and service availability. Annual vendor reviews are performed for key subservice providers.

4.3.4 Change Management

Cosmoverse designed and implemented controls to manage changes to the ProcIndex platform. Changes are tracked through version control, tested prior to production deployment, and deployed through automated deployment pipelines. Change records and deployment logs are maintained to support auditability and troubleshooting.

4.3.5 Incident Management and Monitoring

Cosmoverse designed and implemented controls for incident management and system monitoring. Security incidents and operational issues are managed through defined incident response procedures including detection, assessment, containment, investigation, resolution, and post-incident review. System monitoring captures operational metrics, error logs, and security-relevant events to support anomaly detection and incident investigation.

4.3.6 Logical and Physical Access Controls

Cosmoverse designed and implemented logical access controls including authentication through Clerk, role-based access controls within the application, and restricted access to production infrastructure. Access provisioning and deprovisioning procedures are executed within defined service level agreements. Quarterly access reviews validate appropriateness of user access. Physical security for production systems is provided by subservice organizations including Railway and Supabase.

4.3.7 System Operations and Data Processing Controls

Cosmoverse designed and implemented controls for system operations and data processing including input validation, processing controls, output validation, data storage integrity, and exception handling. Automated validation rules identify incomplete, inconsistent, or unusual data for human review. Audit logs capture processing decisions, status changes, and user actions to support traceability and investigation.

4.3.8 Data Protection and Encryption

Cosmoverse designed and implemented controls for data protection including encryption of data in transit using industry-standard TLS encryption. Data at rest encryption is provided by subservice organizations. Secure communication protocols are used for API integrations and email communications.

4.4 Trust Services Criteria Security, Availability, and Processing Integrity Related Controls and Tests of Results

The following table presents the Trust Services Criteria applicable to the ProcIndex platform, the related control descriptions, tests of controls performed, and results of tests:

Control ID	Trust Services Criteria	Control Description	Tests of Controls	Test Results
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Cosmoverse maintains documented policies and procedures including the Company Handbook, Information Security Policy, Acceptable Use Policy, and Personnel Security Policy. New employees and contractors are required to acknowledge these policies upon onboarding.	We obtained the Company Handbook, Information Security Policy, Acceptable Use Policy, and Personnel Security Policy and confirmed that these documents were maintained and available to personnel. We inspected onboarding documentation for a sample of employees hired and verified that policy acknowledgment forms were completed.	No Exceptions Noted
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Cosmoverse has established organizational structure with defined roles and responsibilities. The Board of Directors Charter and Risk and Governance Executive Committee Charter define governance oversight responsibilities.	We obtained and inspected the Management Review Meeting MoM and Risk and Governance Executive Committee Charter and confirmed that governance oversight responsibilities were defined. We inspected organizational structure documentation confirming defined reporting lines and responsibilities.	No Exceptions Noted
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Cosmoverse defines organizational structure through functional teams (Engineering, Product & Sales, Operations, IT) with assigned responsibilities. The executive team provides strategic direction and approves key policies.	We obtained organizational structure documentation and inspected defined functional team responsibilities. We confirmed that the executive team provides oversight and approves policies governing system operations.	No Exceptions Noted
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Cosmoverse's Personnel Security Policy defines requirements for hiring, onboarding, training, and performance management. All personnel complete security awareness training.	We obtained the Personnel Security Policy and confirmed it defines personnel security requirements. We inspected training records for a sample of personnel and verified completion of required security awareness training.	No Exceptions Noted

Control ID	Trust Services Criteria	Control Description	Tests of Controls	Test Results
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Cosmoverse assigns ownership for key security functions and holds personnel accountable through defined roles, responsibilities, and performance expectations documented in policies and job responsibilities.	We obtained documentation defining assigned ownership for key security and operational functions. We inspected evidence of management oversight and accountability for control responsibilities.	No Exceptions Noted
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Cosmoverse maintains documented standard operating procedures and policies covering key operational and security domains including Information Security, Access Control, Change Management, Incident Response, Business Continuity, Risk Assessment, and Vendor Management.	We obtained and inspected documented policies including Information Security Policy, Access Control and Termination Policy, Change Management Policy, Incident Response Policy, Business Continuity and Disaster Recovery Policy, Risk Assessment and Treatment Policy, and Vendor Management Policy.	No Exceptions Noted
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Cosmoverse communicates service commitments and system requirements to customers through customer agreements, product documentation, and security documentation. Internal communication occurs through collaboration tools including Email and Slack.	We obtained sample customer agreements and confirmed that service commitments were communicated to customers. We inspected internal communication channels and confirmed that operational information and security updates were communicated to personnel.	No Exceptions Noted
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Cosmoverse communicates with customers regarding system commitments, changes, and incidents through established communication channels. Subservice provider relationships are defined through vendor agreements specifying security and operational requirements.	We obtained and inspected the Change Management Policy and confirmed that procedures for communicating material changes to customers were documented. We obtained the Vendor Management Policy and confirmed that vendor assessment procedures were documented	No Exceptions Noted
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Cosmoverse has established a risk management framework documented in the Risk Assessment and Treatment Policy. The framework covers operational, technical, and security risks related to service commitments and system requirements.	We obtained and inspected the Risk Assessment and Treatment Policy and confirmed that the risk management framework was documented and covered operational, technical, and security risks.	No Exceptions Noted
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its	Cosmoverse performs risk assessments to identify and evaluate risks that could impact service commitments and system requirements. Risk	We obtained risk assessment documentation and confirmed that risks were identified, evaluated,	No Exceptions Noted

Control ID	Trust Services Criteria	Control Description	Tests of Controls	Test Results
	objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	assessment results are documented and reviewed by management.	and documented. We inspected evidence of management review of risk assessment results.	
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Risk assessment procedures consider potential fraud risks including unauthorized access, data manipulation, and misuse of system privileges. Risk treatment strategies are developed for identified fraud risks.	We inspected risk assessment documentation and confirmed that potential fraud risks were considered.	No Exceptions Noted
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Cosmoverse's risk assessment process includes evaluation of changes that could impact the system of internal control, including system changes, infrastructure changes, and organizational changes.	We obtained and inspected risk assessment documentation covering the audit period and confirmed that significant changes impacting internal controls were identified and assessed	No Exceptions Noted
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Cosmoverse performs vulnerability scanning and security assessments to evaluate security controls. Quarterly access reviews are performed to validate appropriateness of user access.	We obtained vulnerability scan reports and confirmed that vulnerability scanning was performed. We inspected quarterly access review documentation and confirmed that access reviews were completed.	No Exceptions Noted
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Control deficiencies and security findings are communicated to management through incident reports, vulnerability reports, and assessment findings. Corrective actions are tracked to resolution.	We inspected incident reports and vulnerability reports and confirmed that findings were communicated to management. We reviewed documentation of corrective actions for identified deficiencies.	No Exceptions Noted
CC5.1	COSO Principle 11: The entity also selects and develops general control activities over technology to	Cosmoverse implements technology controls including access controls, change management procedures, infrastructure monitoring, and backup procedures to support system objectives.	We obtained and inspected documentation of technology controls including access control configurations, change management procedures,	No Exceptions Noted

Control ID	Trust Services Criteria	Control Description	Tests of Controls	Test Results
	support the achievement of objectives.		monitoring configurations, and backup procedures.	
CC5.2	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and procedures that put policies into action.	Control activities are documented in policies and procedures including Access Control and Termination Policy, Change Management Policy, Incident Response Policy, and operational procedures.	We obtained policies and procedures documenting control activities and confirmed that policies establish expectations and procedures define implementation steps.	No Exceptions Noted
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.	Logical access to the ProcIndex platform is controlled through Clerk authentication services. Access to production infrastructure is restricted to authorized engineering personnel. Role-based access controls are implemented within the application.	We obtained and inspected documentation regarding access control configurations for the ProcIndex application and production infrastructure. We confirmed that authentication is provided through Clerk and role-based access controls are implemented. We inspected access listings and confirmed access was restricted to authorized personnel.	No Exceptions Noted
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Access provisioning and deprovisioning procedures are managed by the executive team. New user access is provisioned within one day of approval. Terminated user access is deprovisioned within one day of termination notification.	We obtained the Access Control and Termination Policy and confirmed that access provisioning and deprovisioning procedures were documented with one-day service level agreements. We inspected a sample of access provisioning and deprovisioning events and confirmed timely execution.	No Exceptions Noted
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the	Role-based access controls are implemented within the ProcIndex application to restrict access based on assigned roles. Quarterly access reviews are performed to validate that access remains appropriate based on current roles and responsibilities.	We obtained documentation role-based access control configurations and confirmed that access was restricted based on assigned roles. We inspected quarterly access review documentation for the audit period	No Exceptions Noted

Control ID	Trust Services Criteria	Control Description	Tests of Controls	Test Results
	concepts of least privilege and segregation of duties, 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.	Network security controls are implemented through Railway infrastructure and Cloudflare services. The Network Security Policy defines requirements for network protection including firewall configurations and secure communications.	We obtained the Network Security Policy and confirmed network security requirements were documented. We inspected network security configurations provided by Railway and Cloudflare and confirmed security measures were implemented to protect against external threats.	No Exceptions Noted
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Data in transit is encrypted using industry-standard TLS encryption for web communications. API communications with integrated systems use secure protocols. Email communications are transmitted through Resend using secure email protocols.	We inspected application configurations and confirmed that TLS encryption was implemented for web communications. We reviewed API integration configurations and verified use of secure protocols. We confirmed that email communications were transmitted through Resend using secure protocols.	No Exceptions Noted
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Endpoint security controls are implemented on employee devices used to access production systems and customer data. The Baseline Hardening Policy defines requirements for system hardening and malware protection.	We obtained the Baseline Hardening Policy and confirmed that requirements for endpoint security and malware protection were documented. We inspected endpoint security configurations on a sample of employee devices and verified that malware protection was implemented.	No Exceptions Noted
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Cosmoverse performs vulnerability scanning on a periodic basis to identify security weaknesses. An external security provider is engaged to perform annual Web Application Penetration Testing (WAPT). Identified vulnerabilities are reviewed, prioritized, and tracked through remediation.	We obtained vulnerability scan reports covering the audit period and confirmed that vulnerability scanning was performed. We inspected the annual penetration test report and verified that testing was conducted by an external security provider. We reviewed vulnerability remediation tracking and confirmed that identified vulnerabilities were prioritized and tracked to resolution.	No Exceptions Noted
CC7.2	The entity monitors system components and the	System monitoring is implemented through Railway platform monitoring and application	We obtained monitoring configurations and confirmed that system monitoring was	No Exceptions Noted

Control ID	Trust Services Criteria	Control Description	Tests of Controls	Test Results
	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.	logging. Operational metrics and error logs are reviewed for anomalies. Security-relevant events are captured in application logs for investigation.	implemented through Railway. We inspected application logs and operational metrics and verified that anomalies were captured and available for review. We confirmed security-relevant events were logged.	
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Security incidents are managed through procedures defined in the Incident Response Policy. The process includes incident detection, assessment, containment, investigation, resolution, and post-incident review.	We obtained the Incident Response Policy and confirmed that incident management procedures were documented. No incidents reported during the review period.	No Exceptions Noted
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The Incident Response Policy defines procedures for incident response including containment, investigation, remediation, and communication. Customer notification procedures are established for incidents impacting customer data or service availability.	We obtained the Incident Response Policy and confirmed incident response procedures were documented including customer notification requirements. We inspected incident response activities for the audit period and verified execution of incident response procedures.	No Exceptions Noted
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Incident response procedures include recovery activities to restore normal operations following security incidents. Post-incident reviews are conducted to identify lessons learned and implement improvements.	We obtained the Incident Response Policy and confirmed it was documented and acknowledged by Akash Thakur on January 13, 2026. We inquired of management and confirmed that no security or privacy incidents occurred during the period.	No Exceptions Noted
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data,	Changes to the ProcIndex platform are managed through procedures documented in the Change Management Policy. Code changes are tracked through GitHub. Changes are tested prior to production deployment. Deployments are performed through Railway's deployment pipeline.	We obtained the Change Management Policy and confirmed change management procedures were documented. We inspected a sample of changes deployed during the audit period and verified that changes were tracked in GitHub, tested, and deployed through Railway. We reviewed	No Exceptions Noted

Control ID	Trust Services Criteria	Control Description	Tests of Controls	Test Results
	software, and procedures to meet its objectives.		deployment logs confirming change implementation.	
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Cosmoverse maintains business continuity procedures documented in the Business Continuity and Disaster Recovery Policy. Daily database backups are performed through Supabase. Recovery objectives are defined and backup restoration testing is performed.	We obtained the Business Continuity and Disaster Recovery Policy and confirmed business continuity procedures were documented. We inspected backup logs and verified daily database backups were performed through Supabase. We reviewed backup restoration test documentation confirming testing was conducted.	No Exceptions Noted
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Vendor relationships are managed through procedures defined in the Vendor Management Policy. Vendor reviews include evaluation of security posture and compliance attestations. Key subservice providers are reviewed annually.	We obtained the Vendor Management Policy and confirmed vendor management procedures were documented. We inspected vendor assessment documentation for key subservice providers and verified that security posture and compliance were evaluated. We confirmed annual vendor reviews were performed.	No Exceptions Noted
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	System performance and capacity are monitored through Railway platform monitoring. Resource utilization metrics are reviewed to support capacity planning and scaling decisions.	We obtained monitoring configurations and confirmed system performance and capacity monitoring was implemented. We inspected capacity monitoring reports and verified resource utilization was tracked to support capacity planning.	No Exceptions Noted
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	Daily database backups are performed through Supabase managed backup services. Backup execution is monitored and backup failures are investigated. Recovery procedures are tested periodically.	We obtained backup configuration documentation and confirmed daily database backups were configured through Supabase. We inspected backup logs for the audit period and verified daily backups were executed. We reviewed backup restoration test documentation and confirmed periodic testing was performed.	No Exceptions Noted

Control ID	Trust Services Criteria	Control Description	Tests of Controls	Test Results
A1.3	The entity provides for the recovery and continuity of operations in the event of a disruption.	Business continuity procedures define recovery objectives and recovery processes. A Recovery Point Objective (RPO) of 24 hours and Recovery Time Objective (RTO) of 24 hours are established. Backup restoration testing validates recovery capability.	We obtained the Business Continuity and Disaster Recovery Policy and confirmed recovery objectives were documented. We inspected backup restoration test documentation and verified that recovery procedures were tested and recovery objectives were validated.	No Exceptions Noted
PI1.1	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.	Data types processed by the ProcIndex platform are documented in the system description. Product documentation and onboarding materials communicate processing capabilities and data handling practices to customers.	We obtained system description documentation and confirmed data types processed by the platform were documented.	No Exceptions Noted
PI1.2	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 validation controls ensure data completeness and accuracy. Automated validation rules identify missing, inconsistent, duplicate, or unusual data. Exception items are routed to human review queues for verification.	We obtained documentation of input validation controls and confirmed validation rules were implemented. We inspected application code and configurations and verified validation checks for completeness and accuracy. We reviewed exception handling procedures and confirmed items requiring review were routed to human review queues.	No Exceptions Noted
PI1.3	The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives to ensure completeness, accuracy, and timeliness of processing.	Processing controls ensure workflow completeness, accuracy, and timeliness. Workflow state is tracked and audit logs record processing decisions, status changes, and user actions. Exception handling procedures ensure incomplete or unusual items are identified for review.	We obtained documentation of processing controls and confirmed workflow tracking and audit logging were implemented	No Exceptions Noted
PI1.4	The entity implements policies and procedures to make available or deliver output completely,	Output controls ensure processed results are complete and accurate prior to delivery. Human review and approval procedures validate workflow outputs before final acceptance. Integration with	We obtained system documentation and confirmed that output validation procedures were implemented. We confirmed that human review and approval workflows were established for	No Exceptions Noted

Control ID	Trust Services Criteria	Control Description	Tests of Controls	Test Results
	accurately, and timely in accordance with specifications to meet the entity's objectives.	ERP systems includes validation of data completeness and accuracy.	critical processing functions, including exception handling and validation of items requiring additional judgment	
PI1.5	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.	Data storage controls ensure inputs, processing data, and outputs are stored securely and accurately. Database schema constraints enforce data integrity. Backup procedures protect stored data from loss.	We obtained database schema documentation and confirmed integrity constraints were implemented. We inspected backup procedures and verified data storage was protected through daily backups. We reviewed data storage controls and confirmed inputs, processing data, and outputs were stored in accordance with specifications.	No Exceptions Noted

SECTION 5

ADDITIONAL INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

5. Additional Information Provided by the Service Organization

Cosmoverse, Inc. engages Railway, Supabase, Cloudflare R2, Resend, Clerk, and GitHub as subservice organizations to support infrastructure, platform services, and system operations. These services are integral to ensuring the Security, Availability, and Processing integrity of the ProcIndex platform.

Railway provides application hosting and deployment services, including physical security of data centers, infrastructure availability and performance monitoring, network security controls, and infrastructure backup and disaster recovery procedures.

Supabase provides managed production database services and database backup services, including physical security of database infrastructure, database platform security controls, encryption of data at rest, database backup execution and retention, and database availability monitoring.

Cloudflare R2 provides object storage services for invoice attachments and supporting documents, including physical security of storage infrastructure, object storage platform security, encryption of data at rest, and object storage availability.

Resend provides email sending and inbound email processing services, including email delivery infrastructure security, email sending and receiving platform controls, and email service availability.

Clerk provides authentication and identity management services, including authentication infrastructure security, identity and access management platform controls, secure credential storage, and authentication service availability.

GitHub provides source code repository and version control services, including source code repository security, access controls for repositories, version control integrity, and repository availability.

As part of Cosmoverse's vendor management and risk governance processes, management obtains and reviews available SOC 2 or equivalent attestation reports from subservice providers on at least an annual basis to evaluate the design and operating effectiveness of controls at the subservice organizations. Any complementary subservice organization controls (CSOCs) identified within subservice provider reports are assessed for applicability and are incorporated into Cosmoverse's internal control framework, where relevant. This approach supports Cosmoverse's overall control environment and provides reasonable assurance over the services performed by the subservice organizations.

Our examination was conducted for the purpose of expressing an opinion on Cosmoverse's system description and the suitability of the design and operating effectiveness of controls relevant to the applicable trust services criteria during the specified period. Accordingly, we did not perform any procedures with respect to this other information, and, therefore, we do not express an opinion or provide any assurance on it.

Users of this report are advised to consider this information in conjunction with, but not as part of, the system description and related controls included within the scope of this report.

***** End of Report *****