CONSILIUM LABS
Cybersecurity is for Everyone

SOCi Inc.

SOC 3 Examination

November 21, 2025

Versions

Author	Role	Date	Comments
Jorge Sandoval	Auditor	24-OCT-2025	Draft
Joe Weindorfer	Auditor	19-NOV-2025	Technical Review
Thomas Craft	Technical Writer	21-NOV-2025	VQA

Notice! This publication is nonauthoritative and is provided for informational purposes only.

In the following illustrative management assertion and service auditor's report, SOCi Service Organization has engaged the service auditor to (a) examine the controls within the system relevant to security, availability, and confidentiality and (b) issue a SOC 3® report that can be posted on its website to encourage prospective customers to contract the service organization's services.

CONSILIUM LABS
Cybersecurity is for Everyone

Table of Contents

CONSILIUM LABS
Cybersecurity is for Everyone

1 Illustrative Assertion by Service Organization Management

1.1 Assertion of SOCi Service Organization Management

We are responsible for designing, implementing, operating, and maintaining effective controls within SOCi Service Organization's (SOCi's) Chatbot System (system) for the period between October 1, 2024 – September 30, 2025, to provide reasonable assurance that SOCi's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality and processing integrity (applicable trust services criteria[1]) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in *AICPA Trust Services Criteria*. Our description of the boundaries of the system is presented in attachment A 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 for the period between October 1, 2024 – September 30, 2025, to provide reasonable assurance that SOCi's service commitments and system requirements were achieved based on the applicable trust services criteria. SOCi'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 attachment B.

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 for the period between October 1, 2024 – September 30, 2025, to provide reasonable assurance that SOCi's service commitments and system requirements were achieved based on the applicable trust services criteria.

The 2017 trust services criteria are codified in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)*. Because points of focus may be updated without changes to criteria, service organization management and the service auditor should review the most current version of TSP section 100 for the most up-to-date guidance.

[1] The 2017 trust services criteria are codified in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022). Because points of focus may be updated without changes to criteria, service organization management and the service auditor should review the most current version of TSP section 100 for the most up-to-date guidance.

2 Attachment A: SOCi Service Organization's Description of the Boundaries of SOCi's System

2.1 System Overview and Background

SOCi offers a software-as-a-service (SaaS) platform designed specifically to support marketing activities for multi-location businesses. This platform provides these businesses with an effective way to manage their social media presence and engage with online interactions. SOCi's background and system design include the following:

- Regulatory and Contractual Commitments: SOCi's system is built with its main focus on meeting security standards and contractual obligations. This includes aspects such as data protection, availability, and confidentiality.
- Infrastructure: SOCi relies on cloud infrastructure from Amazon Web Services (AWS) and Google Cloud Platform (GCP). These cloud providers offer scalability and reliability for SOCi's platform. They also utilize security measures such as firewalls and intrusion detection systems. For deploying their applications in a consistent and manageable manner, they use Kubernetes, a technology for containerization.
- Software: SOCi maintains a record of all material software that is critical for running its services. They track which parts of the business use each software and how important each software is to their operations. They also work with a third-party company to manage their software licenses.
- Data: SOCi has strict procedures for classifying and managing data based on sensitivity (public, operational, and confidential) and has procedures for securely deleting data when it is no longer needed.
- Processes and procedures: SOCi has documented procedures for important security-related activities. This includes classifying data, managing who has access, implementing and monitoring security controls, and responding to security incidents. These procedures are reviewed on an annual basis and require management approval for any changes.

2.2 Types of Services Provided

SOCi, Inc.'s (SOCi's) product is a software-as-a-service (SaaS) solution that allows companies with multiple locations to manage social media presences and respond to posted complaints or social media posts about certain locations. SOCi is generally used by enterprise clients in addition to small and medium-sized businesses.

SOCi enables clients to coordinate social media marketing activities between social media platforms via a SaaS platform and application programming interfaces (API). This tool also provides information to those platforms regarding sales or communications pushes. SOCi also connects to analytics tools and uses content data to allow customers to learn about social media metrics. Users can pull and graph all conversation metrics for the platform and learn about and respond to comments within 24 hours. Additionally, SOCi enables clients to schedule posts for the most effective times.

SOCi users are also able to upload images, add URLs, establish and present the rules and prize, and then schedule it to be posted.

The support center or SOCi University contains a knowledge base and allows the user to submit a ticket. The client can also use the customer success portal. Email or call SOCi for immediate assistance if needed.

2.3 Service Delivery

SOCi uses multiple touchpoints, such as outbound marketing lead generation, referrals from other customers, or industry or customer events, to identify new sales opportunities. Once a sale is made and a contract is signed, SOCi begins collecting the client's information.

Customer onboarding involves scope discussions and a welcome call with the Customer Success Team. This call includes introductions, determining the implementation process, establishing roles and responsibilities, and establishing customer responsibilities. The organization also maintains additional communications with the client to check on the use cases and goals, ensure the platform is properly configured, and set up groups as needed. To this end, the organization maintains weekly calls with the customers and offers training on the platform. Once the client's platform is established and training has ended, a Customer Support Manager handles the relationship with the client.

Clients are provided with information to contact technical support and Customer Support Managers for issues.

Once a client's contract is terminated, the customer's social media connections are unlinked by removing access and data.

2.4 System Design

SOCi designs its social media marketing and management services system to meet its regulatory and contractual commitments, as well as align with best practices. These commitments are based on the services that SOCi provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that SOCi has established for its services. SOCi establishes operational requirements in its system design that support the achievement of its regulatory and contractual obligations. These requirements are communicated in SOCi's system policies and procedures, system design documentation, and contracts with clients.

2.5 Infrastructure

The organization maintains industry-standard security infrastructure, such as firewalls, to ensure ingress and egress filtering. Additionally, network hardware provides limited management access, time synchronization, and the disabling of unused services and ports. Network server configurations ensure the removal of unnecessary services and ports, firewalls or access list restrictions, standard installations, and clock synchronization.

The organization also uses CloudTrail and GuardDuty for intrusion detection and prevention systems (IDS & IPS). AWS and Google buckets are primarily private.

Production containers and load balancers are built with Kubernetes to ensure consistent configuration and proper change management. Interlaced is responsible for building out end-user systems.

The following network diagrams depict the AWS and GCP networks and the corresponding blue and green production environments.

2.6 Diagrams

The user interacts with the system via **Route 53 DNS (for AWS and GCP)**, which directs traffic to Load Balancers and CDNs (Cloudflare/CloudFront)**.** The load balancers & CDNs route traffic to various Kubernetes services/deployments running on **Amazon EKS.**

SOCi utilizes private subnets for our workloads and databases and is only accessible via internal IP addresses, while public subnets are reserved for the load balancers and NAT gateway.

For GCP, all traffic is protected via Cloudflare, while on AWS, this is enabled per customer by request.

The core services within the Kubernetes clusters are:

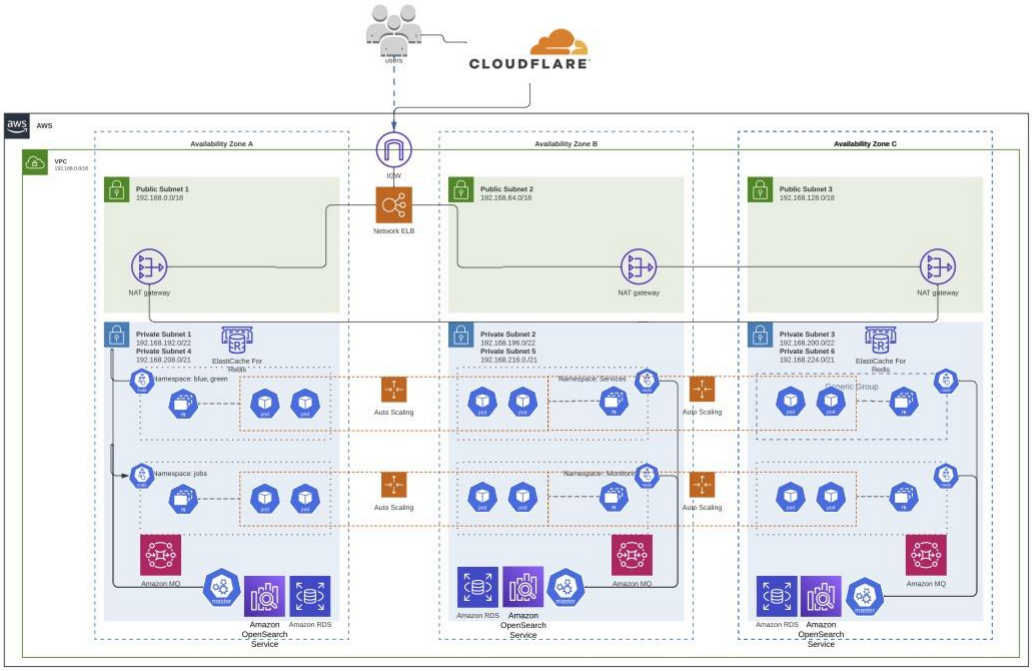
- "soci monolith" (the primary frontend application)
- Landlord (single tenancy management/customer data segregation)
- Auth service
- Product-specific services

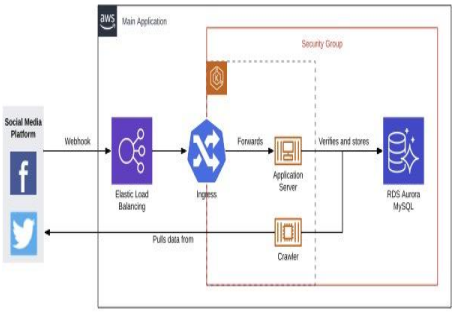
All services in the Kubernetes cluster have access to a **MySQL or PostgreSQL** instance for persistent data storage. The database instances are within the VPC and are **not directly accessible from the outside**. The container images for these services are stored in **Amazon ECR (Elastic Container Registry) and Google Artifact Registry**.

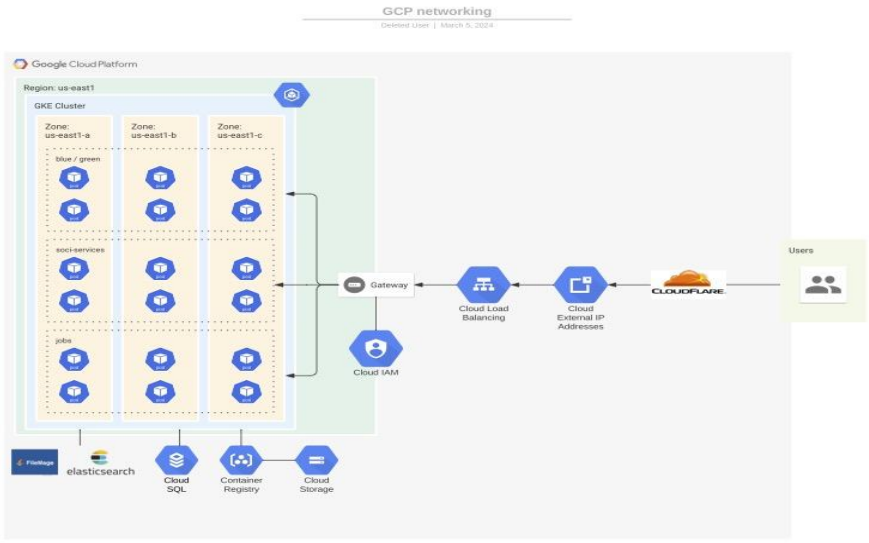
Tech Leads have access to the environment via an **EC2 Jump Box (our server called "Hermes")**, which is used for maintenance tasks. Access to Hermes is restricted to TechLeads and requires a VPN (Cloudflare WARP).

For GCP, Filemage is an SFTP gateway (upload.meetsoci.com) backed by Google Cloud Storage. This is mainly utilized for customers to provide us with their data, which is mainly handled by our ETL service (Data Ingestion Service, aka DIS), although there are some custom jobs and services that use this FTP as well.

Monitoring and security alerting are handled using **CloudWatch, GuardDuty**, **SNS,** Prometheus, and Gatus. CloudWatch gathers logs and metrics for monitoring, while GuardDuty handles threat detection and security event monitoring. Alerts generated by these services are delivered via **SNS** to **Slack** notifications.


CLOUDFLARE
AWS
Availability Zone A
Availability Zone B
Availability Zone C
VPC
IGW
Network ELB
Public Subnet 1
192.168.0.0/18
Public Subnet 2
192.168.64.0/18
Public Subnet 3
192.168.128.0/18
NAT gateway
NAT gateway
NAT gateway
Private Subnet 1
192.168.192.0/22
Private Subnet 4
192.168.208.0/21
Private Subnet 2
192.168.196.0/22
Private Subnet 5
192.168.216.0/21
Private Subnet 3
192.168.200.0/22
Private Subnet 6
192.168.224.0/21
ElastiCache For Redis
Namespace: blue, green
Namespace: jobs
Namespace: Services
Namespace: Monitoring
Security Group
Auto Scaling
Amazon MQ
Amazon RDS
Amazon OpenSearch Service


Main Application
Security Group
Social Media Platform
Webhook
Elastic Load Balancing
Ingress
Forwards
Application Server
Verifies and stores
RDS Aurora MySQL
Pulls data from
Crawler



AWS Resources	GCP Resources	Purpose
AWS Elastic Compute Cloud (EC2)	Google Compute Engine (GCE)	Cloud computing
Elastic Load Balancers	Google Load Balancing	Load balance internal and external traffic
Virtual Private Cloud	Virtual Private Cloud	Protects the network perimeter and restricts inbound and outbound access
S3 Buckets	Cloud Storage (GCS)	Storage, upload, and download

AWS Elastic Kubernetes Service (EKS)	Google Kubernetes Engine (GKE)	Main application
AWS Elastic Container Registry (ECR)	Google Container Registry (GCR) and Artifact Registry	Stores images for Kubernetes workloads
ElasticSearch	ElasticCloud (from Google Marketplace)	Storage of analytics and data needed for customer sites (Locators and Local Pages (LLPs))
RDS (Aurora MySQL & Postgres)	CloudSQL	MySQL is the main application database; Postgres is used sparingly for specific services.
Redis	MemoryStore	Session management and job queues
Redshift	BigQuery	Storage of dimension tables (from MySQL) and analytics
Memcache	Internally managed via k8s	API response caching
CloudFront	Cloud CDN	CDN
Cloudflare	Cloudflare	CDN; custom hostnames; ZeroTrust (w/ WARP)
Lambda functions	CloudRun Jobs and Functions	Small ad hoc jobs (e.g. file transfers); our ETL system Data Ingestion service (DIS (GCP Only)) runs on CloudRun
SQS	Pub/sub	Pub/sub
SES	N/A	Sending emails from applications (We also use Sendgrid)
SNS	N/A	Push Notifications
Amazon MQ (managed RabbitMQ)	Self-managed Rabbit MQ	Message queuing
Secrets Manager	Secrets Manager	Securely store secrets and limit access

2.7 Software

SOCi's IT Department maintains a detailed inventory to track all software deemed critical to the development and implementation of the organization's services. This inventory also tracks the business channel that uses the software and the criticality of the software to the organization.

A third party manages SOCi's software licensing.

Production Application	Business Function
New Relic / Grafana / Prometheus/ Gatus / OpsGenie / (AWS) CloudWatch / Cloud Logging (formerly Stackdriver – GCP)	Application monitoring for load and uptime performance.
New Relic (Logging) DataDog (WIP)	SIEM/Logging system that provides log management and analytics that leverage machine-generated data to deliver real-time IT insights.
Jenkins / ArgoCD / GitHub Actions	Manage and deploy code changes for our applications.
(manual)	Patch management
Symantec Workload Protection	File integrity monitoring platform used to deliver security, monitoring, forensics, and collection of metrics about the environment.
JIRA / AirTable	Software applications used for issue tracking and project management.
GitHub	Version control and DevOps tool used for source code management to track changes in the source code.
GuardDuty (AWS) Cloud Armor / Cloud IDS (GCP) Cloudflare (DDoS Protection)	An intrusion detection system is used to provide visibility into endpoint vulnerabilities by gathering data needed to identify, understand, and respond to attacks.

2.8 People

SOCi's board of directors has five members, consisting of the CEO, the lead investor, and representatives of the investment firms. The board meets quarterly and provides guidance and feedback to the Executive Team.

The Chief Technology Officer (CTO) and the Management Committee update the board of directors, when necessary, on relevant information and meaningful changes.

The organization consists of a hierarchical structure that is led by the CEO and the C-suite; the directors and the vice presidents report to the C-suite and the CEO. The CTO is a co-founder and reports to the CEO, while the Vice President of Security and Compliance reports to the CTO.

2.9 Data

The following data classifications are used by the organization to determine data storage, transmission, and destruction requirements:

- Public
- Operational
- Confidential

Per the Information Security Policy, the organization requires data to be destroyed, ultimately making the recovery process impossible. Furthermore, the organization requires the following methods for data destruction:

- Paper is crosscut shredded
- Asset tags are removed
- Configuration information is removed or reset to default configurations
- Data wiping methods are followed
- Virtual hardware is disposed of in a manner consistent with cloud providers.
- Storage media requires physical destruction

The organization also requires data to be destroyed upon the expiration of data retention requirements.

Encryption is also used for confidential data in transit, and confidential data at rest is managed with strict key management processes. The following is required for encryption keys:

- To be available when needed for decryption
- To be backed up
- To be stored securely
- To never be transmitted in clear text

- To be treated as confidential data
- To never be shared

Additionally, in the AWS platform, AWS-managed key services (KMS) are used to manage encryption keys for Relational Database Service (RDS), SNS, Secrets Manager, Amazon Certificate Manager, VPN, and Cloud Workload Protection. The database contents are also encrypted.

For the Google Cloud environment, the Google Secrets Manager and Kubernetes secrets are used; the database contents are encrypted.

The organization also generally uses accepted, non-proprietary encryption algorithms. All sensitive data in transit occurs over HTTPS or SSH-encrypted protocols.

Passwords stored in the production system are hashed with bcrypt and salted with 10 rounds.

2.10 Processes and Procedures

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

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

2.11 Physical Security

Cloud providers are responsible for protecting environments

2.12 Logical Security

The organization has a detailed description of SOCi's approach to logical security as a part of its broader system of internal controls. The following includes areas and controls related to logical security implemented by SOCi:

- **Least Privilege:** SOCi employs a least-privilege access control model, granting access to systems and data based on specific roles and responsibilities of employees and contractors.
- **Segregation of Duties:** The principle of segregation of duties is considered in granting access rights, preventing any single individual from having excessive control over critical functions. This helps mitigate the risk of fraud and errors.
- **Restricted Administrator Access:** SOCi limits administrator access to systems and data to only authorized personnel. This restriction helps protect against unauthorized changes to critical configurations and settings.
- **Password Security:** Strong password policies are enforced, requiring complex passwords with a minimum length and regular changes. Passwords cannot be reused, and passkeys are permitted as an alternative to meet complexity requirements. Additionally, workstations automatically lock after a period of inactivity, requiring a password to unlock. These measures help prevent unauthorized access through weak or compromised passwords.
- **Multi-Factor Authentication (MFA):** MFA is mandatory for access to critical systems, including AWS and Google Cloud Environments. OneLogin is used as the primary IAM provider for MFA. This additional layer of security helps protect against unauthorized access if passwords are compromised.
- **Account Review and Termination:** Regular account reviews are conducted to ensure the accuracy of user access and to identify inactive accounts. Upon termination, access is immediately revoked, and accounts are disabled. This helps prevent former employees or unauthorized individuals from accessing sensitive information.

2.13 Security Architecture

SOCi's security architecture aims to protect the confidentiality, integrity, and availability of SOCi's systems and client data. The key elements and principles include the following:

- Cloud-Based Foundation with Security Emphasis
    - SOCi relies on the cloud infrastructure provided by Amazon Web Services (AWS) and Google Cloud Platform (GCP). These providers are industry leaders in cloud security, offering robust physical security for their data centers, network security features such as firewalls and intrusion detection systems, and tools for managing access and permissions.
    - SOCi leverages the security features of these platforms and complements them with its own security configurations and controls. For example, they configure firewalls for ingress and

egress filtering, use tools such as CloudTrail and GuardDuty for enhanced security monitoring in AWS, and ensure that their cloud storage buckets are primarily private.

- Network Segmentation for Enhanced Protection
    - SOCi separates its production environment into "blue" and "green" instances, a common practice for enhancing availability and resilience. Meaning, they have two parallel environments running, allowing them to switch over in case of issues with one environment.
    - This segmentation also enhances security by limiting the potential impact of a security incident. If one environment is compromised, the other can continue operating, minimizing downtime and data loss.
- Strong Logical Access Controls
    - SOCi has implemented a range of measures who can access their systems and data:
        - **Least Privilege:** Access is granted based on the principle of least privilege, meaning users only get the access they need to do their jobs.
        - **Role-Based Access Control (RBAC):** Access is determined by a user's role within the company, using a defined access matrix.
        - **Strong Password Policy:** Passwords are required to be complex, changed regularly, and cannot be reused.
        - **Multi-Factor Authentication (MFA):** MFA is required for critical systems, adding an extra layer of security by requiring users to provide multiple forms of identification.
        - **Identity and Access Management (IAM) Solution:** Wherever possible, SOCi uses an IAM solution to manage access to systems containing sensitive data, providing a centralized and more secure way to manage identities and permissions.
- Incident Response Program
    - SOCi has a well-defined Incident Response Policy and Plan that outlines the steps they take to handle security incidents. This plan includes procedures for the following:
        - Preparing for incidents through training and awareness
        - Detecting incidents through monitoring and analysis
        - Responding to and containing incidents to minimize damage
        - Recovering from incidents to restore normal operations
        - Conducting post-incident activities to learn and improve

- Third-Party Security Management
    - SOCi recognizes that its security relies not only on its controls but also on the security practices of its vendors and partners.
    - SOCi has a Vendor Management Policy that outlines procedures for evaluating, selecting, and managing vendors, with a focus on security considerations.
    - They require critical vendors to undergo security reviews before being granted any form of access to SOCi systems and/or data.
    - Critical vendors are also required to be reviewed for information security issues and risks at least annually.

2.14 User Identification and Authentication

SOCi employs a robust system for user identification and authentication, incorporating a multi-layered approach to secure its systems and protect sensitive information and data. These several key components include:

- Strong Password Policy
    - SOCi mandates a strong password policy that requires passwords to be at least eight characters long, including a mix of upper and lowercase letters, numbers, and special characters. Passwords cannot be dictionary words or obvious keyboard sequences.
    - As an alternative to complex passwords, SOCi permits passphrases longer than 20 characters.
    - Passwords are considered confidential data and must be treated with the same level of discretion as other proprietary.
    - Passwords must be changed regularly, and users cannot reuse any of their previous six passwords.
- Multi-Factor Authentication (MFA)
    - SOCi requires MFA for all users on critical systems that support it. This adds an extra layer of security by requiring users to provide more than one form of authentication.
    - OneLogin is used as the primary MFA provider. Single sign-on (SSO) is also employed where possible, allowing users to access multiple systems with their OneLogin credentials.
- Account Management and Access Control
    - SOCi adheres to the principle of least privilege, granting users only the minimum access required for their job functions, wherever feasible.
    - A user access matrix defines appropriate access levels based on roles. Requests for access outside the standard matrix require approval before being granted.

  - Account sharing and group accounts are not allowed. Accounts are assigned to individuals only.
  - Administrator or "root" access is restricted to users who require it for their job functions. Elevated access requires explicit approval from management and should not be used for tasks that don't necessitate it.
  - User access accounts are promptly revoked upon termination of employment. Quarterly account reviews are conducted to verify the accuracy of user access and remove any inactive or terminated accounts.
  - All new employees and contractors must sign and acknowledge agreeing to comply with various security policies, including the Acceptable Use Policy, Mobile Device Policy, Confidential Data Policy, Email Policy, and Non-Disclosure Agreement.
- Workstation Security
  - Workstations are required to lock after 15 minutes of inactivity, requiring users to re-enter their passwords and regain access.
- User Access Reviews
  - The IT Team conducts quarterly user access reviews to ensure appropriateness and coordinates with department managers to determine correct system access.
  - OneLogin, the IAM provider, is also subject to quarterly reviews. These reviews aim to ensure prompt revocation of access for inactive users and those no longer with the company.

In summary, SOCi combines strong password policies, MFA, a strong IAM system, least privilege access controls, and regular account reviews to create a comprehensive system for user identification and authentication. This multi-layered approach aims to mitigate the risk of unauthorized access and protect sensitive information and data throughout the organization.

2.15 Access Provisioning/De-Provisioning

SOCi's robust processes for managing access to its systems and data encompass both the provisioning of access to new users and the de-provisioning of access for those who no longer require it. Access provisioning includes the following:

- Role-Based Access Control: SOCi implements a role-based access control model, meaning that access to systems and data is determined by a user's role within the organization. This approach ensures that users are only granted the information and resources necessary for their specific job functions, adhering to the principle of least privilege.
- User Matrix: A user matrix is used to define the specific access rights associated with each role. When a new user is onboarded, their role is determined, and the corresponding access rights are provisioned based on the predefined rules outlined in the matrix.

- Access Request and Approval: SOCi leverages a formal access request and approval process. Users can request access to systems and equipment through a ticketing system, and these requests are then reviewed and approved based on the user's role and the established access rights.
- Third-Party Management: SOCi utilizes interlaced.io to manage access and Typeform for access requests. This indicates a level of automation and centralization in the access provisioning process, potentially streamlining the workflow and ensuring consistent application of access control policies.

De-Provisioning processes include the following:

- Immediate Access Revocation Upon Termination: Upon termination of an employee or contractor, their access to all systems and data is immediately revoked.
- Account Reviews: SOCi conducts quarterly account reviews to identify and disable inactive accounts.

2.16 Complementary User Entity Controls

Client Responsibility: The client organizations are expected to implement their own access management practices to complement SOCi's security controls. This includes practices such as:

- Removing user accounts for terminated employees who were previously involved with SOCi's services
- Ensuring appropriate authorization for transactions related to SOCi's services
- Protecting data sent to SOCi with appropriate security measures
- Notifying SOCi of any significant changes in the client's control environment or personnel involved with SOCi's services
- Enabling appropriate security measures (such as multifactor authentication) for any shared systems jointly leveraged by SOCi and the client organization.

Overall, SOCi demonstrates a strong commitment to secure access management through a structured and multi-layered approach that incorporates role-based access control, formal request and approval processes, immediate de-provisioning upon termination, and continuous monitoring.

2.17 Encryption of Communication Outside the Boundaries

Encryption for Data in Transit:

- SOCi encrypts confidential data in transit using generally accepted, non-proprietary encryption algorithms. Additionally, all sensitive data in transit occurs over HTTPS or SSH-encrypted protocols.

Client Responsibility:

- SOCi also prioritizes the importance of the implementation of complementary user entity controls, implying that client organizations are also expected to implement their security measures to protect data transmissions to and from SOCi.

2.18 Outside of Scope

- Other divisions, services
- Other Complementary User Entity Controls

2.19 Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication Systems, and Monitoring

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

SOCi Service Organization's internal control components include controls that may have a pervasive effect on the organization or may affect specific processes or applications, or both. Some of the components of internal control include controls that have more of an effect at the entity level, while other components include controls that are primarily related to specific processes or applications. When evaluating internal control, we consider the interrelationships among the components.

2.20 Control Environment

The objectives of internal control as it relates to the SOCi Service System are to provide reasonable, but not absolute, assurance that controls are suitably designed and operating effectively to meet the relevant controls, that assets are protected from unauthorized use or disposition, and that transactions are executed in accordance with management's authorization and SOCi instructions. Management has established and maintains controls designed to monitor compliance with established policies and procedures. The remainder of this subsection discusses the tone at the top as set by management, the integrity, ethical values, and competence of Service Organization employees, the policies and procedures, the risk management (RM) process and monitoring, and the roles of significant control groups. The internal control structure is established and refreshed based on the SOCi Service Organization's assessment of the risk facing the organization.

2.21 Integrity and Ethical Values

Integrity and ethical values are essential elements of the control environment, affecting the design, administration, and monitoring of key processes. Integrity and ethical behavior are the products of the Service Organization's ethical and behavioral standards, how they are communicated, and how they are monitored and enforced in its business activities. They include management's actions to remove or reduce incentives/pressures, and opportunities that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of the entity's values and behavioral standards to personnel through policy statements and codes of conduct, and by the examples the executives set. The SOCi Service Organization Board of Directors (the Board) and management recognize their responsibility to foster a strong ethical environment within SOCi Service Organization to determine that its business affairs are conducted with integrity and in accordance with high standards of personal and corporate conduct. This responsibility is characterized and reflected in the SOCi Service Organization Code of Business Conduct and Ethics (the Code of Conduct), which is distributed to all employees of the organization. Specifically, employees and their immediate families are prohibited from using their positions with SOCi Service Organization for personal or private gain, disclosing confidential information regarding clients, or taking any action that is not in the best interest of clients. Employees' personal securities transactions are governed by corporate policy, and employee account trades are reviewed to monitor adherence to SOCi Service Organization policy. All employees are required to maintain ongoing compliance with all statements of policies, procedures, and standards of the Code of Conduct and with lawful and ethical business practices, whether or not they are specifically mentioned in the Code of Conduct. Each employee is required to affirm annually that he or she received, read, understood, and complied with the requirements set forth in the Code of Conduct and the Employee Handbook. Employee recertification status is monitored periodically for compliance.

2.22 Governance and Oversight

SOCi has established a comprehensive governance and oversight framework to manage its information security and privacy risks. This framework comprises several key elements, working together to ensure the confidentiality, integrity, and availability of SOCi's systems and data.

The Information Security and Privacy Management Committee (ISPMC) is responsible for overseeing the Information Security and Privacy Management System (ISPMS). The ISPMC is composed of key executives and department heads who play a crucial role in setting information security and privacy standards, reviewing policies, monitoring risk assessments, and ensuring compliance with relevant standards and regulations. The committee's charter outlines its responsibilities, including the ISPMS, coordinating the security framework, reviewing and approving policies, and ensuring communication of security-related information throughout the organization. The ISPMC's active involvement in the risk assessment process, policy review, and incident response planning showcases its commitment to maintaining a strong security posture. This ISPMC meets at least quarterly.

SOCi's executive management team demonstrates strong leadership and support for information security and privacy initiatives. The CTO's role in approving policies, the CEO's engagement with the board of directors on

security matters, and overall leadership commitment to fostering a culture of security within the organization. The commitment from top leadership plays a crucial role in driving a successful information security program, as it sets the tone and demonstrates the importance of security throughout the organization.

In conclusion, SOCi's governance and oversight framework demonstrates a protective approach to managing information security and privacy risks. The strong leadership commitment, clear roles and responsibilities, comprehensive policies, regular audits, risk assessments, and monitoring processes contribute to a well-structured and effective security program. By continually improving systems and processes, SOCi aims to maintain a secure and compliant environment for its operations and client data.

2.23 Organizational Structure and Assignment of Authority and Responsibility

SOCi Service Organization's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. SOCi Service Organization has established an organizational structure that includes consideration of key areas of authority and responsibility, as well as appropriate lines of reporting. SOCi Service Organization has an established organizational structure with defined roles and responsibilities.

2.24 Commitment to Competence

SOCi demonstrates a strong commitment to building a competent workforce, recognizing that skilled and knowledgeable employees are crucial for maintaining a robust security posture.

SOCi performs thorough background checks on all employees and contractors prior to hiring. This practice helps ensure SOCi is bringing in individuals with a clean record and suitable for positions handling sensitive information and data. Background checks include federal and state criminal searches, county criminal searches, sex offender registry checks, global watchlists, and SNN traces. The thoroughness of these checks underscores SOCi's commitment to hiring trustworthy and reliable individuals.

SOCi has a comprehensive onboarding program. This well-defined onboarding process for new employees includes mandatory security awareness training. This training covers critical areas such as data protection, password security, phishing awareness, and secure communication practices. New hires are also required to acknowledge key policies, including the Information Security Policy, Acceptable Use Policy, Mobile Device Policy, Confidential Data Policy, Email Policy, Non-Disclosure Agreement, and the Employee Handbook. These measures ensure that new employees are well-versed in SOCi's security and privacy expectations from the outset.

SOCi has developed this and defined clear roles and responsibilities for information security and privacy across the organization. The clarity ensures accountability and facilitates efficient decision-making and task execution, contributing to the overall competence of the workforce in managing security risks.

SOCi conducts regular internal and external audits to assess the effectiveness of its ISPMS, including the competence of its workforce. Annual performance evaluations also provide an opportunity to identify areas for

individual development and training. These ongoing assessment and evaluation mechanisms contribute to a culture of continuous improvement and ensure employees' skills and knowledge remain up to date.

By focusing on these key areas, SOCi demonstrates a commitment to building a workforce that is knowledgeable, skilled, and well-equipped to manage information security and privacy risks. Their comprehensive approach to recruitment, training, role definition, performance evaluation, and continuous improvement contributes to a security-conscious culture and a competent workforce capable of protecting the organization's systems and data.

2.25 Accountability

Human resource (HR) policies and practices related to hiring, orienting, training, evaluating, counseling, promoting, and compensating personnel. The competence and integrity of the Service Organization's personnel are essential elements of its control environment.

The foundation of accountability lies within the Information Security and Privacy Management System (ISPMS), a comprehensive framework designed to manage information security and privacy risks. SOCi emphasizes employee awareness and acceptance of its security policies. All employees must sign and acknowledge a suite of crucial security and privacy policies before gaining access to sensitive information. This mandatory acknowledgment process ensures employees understand their responsibilities and the consequences of policy violations.

When it comes to reporting violations, SOCi provides clear channels for reporting policy violations and security incidents. Employees are responsible for reporting any violations to designated individuals, including the CTO, VP of Information Security, or general counsel. A dedicated email address (security@meetsoci.com) is available for reporting security concerns. The reporting mechanism facilitates the timely identification and resolution of security issues and reinforces the culture of accountability.

SOCi's management team plays a critical role in enforcing policies and procedures. All members of management are accountable for ensuring adherence to security policies within their respective departments. This distributed accountability model ensures security is integrated into daily operations.

SOCi conducts annual performance evaluations for employees, which include assessments of their adherence to security policies. The organization's policies state that violations may result in disciplinary actions, ranging from warnings to termination of employment. For serious violations, such as illegal activities or their company's property, SOCi may report the incidents to law enforcement.

In conclusion, SOCi's accountability process is embedded within a comprehensive framework that emphasizes policy awareness, clear reporting channels, management responsibility, robust audits, and effective monitoring. SOCi has established a culture of accountability, ensuring individuals are responsible for their actions and the organization as a whole prioritizes information security and privacy.

2.26 Risk Assessment

The process of identifying, assessing, and managing risks is a critical component of a Service Organization's internal control system. The purpose of the Service Organization's risk assessment process is to identify, assess, and manage risks that affect the organization's ability to achieve its objectives. The Management Service Organization also monitors controls to consider whether they are operating as intended and whether they are modified as appropriate for changes in conditions or risks facing the organization.

SOCi bases its annual risk assessments on ISO 27701 and 27001 and uses stranded methodologies to be consistent with NIST. The risk assessment identifies critical assets and corresponding risks, in addition to risks outside of the organization's risk appetite, which are tracked and either remediated, accepted, or managed.

The organization has had two risk assessments performed, one by a reputable information security consulting firm (Pivot Point) and one by the Chief Information Security Officer. The Pivot Point risk assessment is a control maturity assessment where the controls are based on the framework and are used to determine how the controls are based on the framework and are used to determine how the controls have been implemented. Pivot Point performs this risk assessment with the Automated Risk Management (ARM) tool to process the output. The ARM tool also processes asset types with pre-selected data regarding threats and vulnerabilities to produce the risk assessment, determine the residual risk according to quantitative scoring, and create a remediation plan with recommendations.

The second risk assessment is based on the 32 domains of the Secure Controls Framework, which is used to associate controls with the domain. This process involves interviewing staff and determining the current maturity levels of each of the domains. The risk assessment drives the strategic directives for the company; management uses the risk assessment's output to determine the quarterly objectives.

2.27 Integration with Risk Assessment

Along with assessing risks, management has identified and put into effect actions needed to address those risks. To address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of the security and availability categories.

2.28 Selection and Development of Control Activities

The description of the service auditor's tests of operating effectiveness and the results of those tests is also presented in Section 4, the Testing Matrices, adjacent to the service organization's description of controls. The description of the tests of operating effectiveness and the results of those tests is the responsibility of the service auditor and should be considered information provided by the service auditor.

2.29 Information and Communication Systems

Information and communication are an integral component of the Service Organization's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology.

SOCi prioritizes secure internal communications by mandating the use of Slack for all internal communications. This approach aims to reduce the risk of data leaks and unauthorized access to sensitive information. The use of a dedicated platform like Slack allows SOCi to implement security controls and monitoring specific to internal communications. It also facilitates a centralized approach to communication, potentially making it easier to manage and audit.

SOCi has implemented a data classification scheme to categorize different types of data based on their sensitivity and confidentiality. This classification guides their data protection measures, ensuring appropriate levels of security are applied to different data types. For example, sensitive data in transit is encrypted using HTTPS or SSH protocols. The data classification scheme also informs data retention requirements, ensuring data is stored only for as long as necessary.

SOCi conducts security awareness training for all employees to reinforce security policies, promote responsible data handling, and raise awareness of potential security threats. The training covers various topics such as data protection, password security, phishing awareness, and secure communication practices.

Overall, SOCi's approach to information and communication systems prioritizes security, data protection, and responsible data handling. They utilize a combination of technical safeguards, administrative controls, and a commitment to security best practices to achieve these goals. This dedication to security is evident in their compliance with industry standards, implementation of a robust ISPMS, and comprehensive security training programs.

2.30 Monitoring

SOCi implements a multi-layered monitoring process that encompasses various aspects of its IT infrastructure, applications, and user activity. SOCi leverages multiple tools and technologies to monitor its network infrastructure. Intrusion Detection/Prevention System (IDS/IPS). SOCi utilizes Amazon CloudTrail and GuardDuty for intrusion detection and prevention on critical or high-risk network segments. These systems actively monitor traffic for suspicious patterns and attempt to block malicious traffic. SOCi's Network Security Policy outlines the guidelines and controls for maintaining a secure network infrastructure. SOCi also conducts regular vulnerability assessments, security audits, and penetration testing to identify and remediate network vulnerabilities. This proactive approach to security testing helps detect potential weaknesses and strengthen the overall security posture.

SOCi also conducts a multifaceted monitoring process encompassing network security, system performance, user activity, and security events. This comprehensive approach helps proactively detect and respond to potential threats, ensure the availability of critical systems, and safeguard sensitive information.

In summary, SOCi employs a multifaceted monitoring process encompassing network security, system performance, user activity, and security events.

2.30.1 Vulnerability Scanning and Monitoring

SOCi employs a multifaceted strategy that incorporates regular vulnerability scanning, penetration testing, prompt remediation, and continuous monitoring.

Weekly Vulnerability Scans:

- SOCi conducts weekly vulnerability scans, SOCi also performs configuration scans in its AWS environment using tools like Trusted Advisor and Prowler. These scans help ensure that the cloud infrastructure is configured according to security best practices and that any misconfigurations that could introduce vulnerabilities are identified and addressed.

Container Image Scanning:

- GRC.IO is used to scan container images deployed to the Google Cloud environment for OS-level vulnerabilities. This ensures that the underlying operating systems used for running applications are secure and free from known vulnerabilities.

Scanning Timelines:

- SOCi adheres to specific timelines for remediating vulnerabilities based on their severity level. Critical vulnerabilities are addressed within a 30-day time frame, high-critical vulnerabilities within a 30-day time frame, and medium or low-risk vulnerabilities are evaluated on a case-by-case basis

2.31 Assessments

Penetration Testing:

- Penetration testing is conducted to measure the security posture of a target system or environment. SOCi engages in annual penetration testing of its applications, as evidenced by the Application Security Verification Standard Level 2 Assessment. This assessment involves a penetration test to simulate real-world attacks and identify vulnerabilities that could be exploited by malicious actors.

Internal and External Testing:

- SOCi's vulnerability management program encompasses both internal and external testing. This dual approach helps provide a comprehensive view of potential vulnerabilities and ensures that both internal and external perspectives are considered.

2.32 Availability Monitoring

SOCi's approach to availability monitoring includes various tools and processes that are employed to ensure the continuous operation of its social media marketing management services system. Real-time monitoring and alerting include the following:

- Monitoring Tools: SOCi uses a diverse set of tools to monitor its systems in real-time, tracking key performance indicators that reflect the health and availability of the platform:

Alerting Mechanisms: SOCi leverages Slack as a central communication channel for alerting relevant personnel about system issues. This ensures prompt notification and facilitates a smooth response to potential availability issues/disruptions.

2.33 Changes to the System During the Period

There were no significant changes that are likely to affect report users' understanding of how the in-scope system is used to provide the services covered by this examination during the period.

2.34 Complimentary User-Entity Controls

Client Responsibility: The client organizations are expected to implement their own access management practices to complement SOCi's security controls. This includes practices such as:

- Removing user accounts for terminated employees who were previously involved with SOCi's services
- Ensuring appropriate authorization for transactions related to SOCi's services
- Protecting data sent to SOCi with appropriate security measures
- Notifying SOCi of any significant changes in the client's control environment or personnel involved with SOCi's services
- Enabling appropriate security measures (such as multifactor authentication) for any shared systems jointly leveraged by SOCi and the client organization.

Overall, SOCi demonstrates a strong commitment to secure access management through a structured and multi-layered approach that incorporates role-based access control, formal request and approval processes, immediate de-provisioning upon termination, and continuous monitoring.

3 Attachment B

3.1 Principal Service Commitments and System Requirements[2]

SOCi designs its processes and procedures related to the SOCi to meet its objectives for its services. Those objectives are based on the service commitments that SOCi makes to its customers, business partners, and vendors, and the operational and compliance requirements that SOCi has established for the services. Service commitments are declarations made by management to its customers regarding the performance of the SOCi. Service commitments are set forth in standardized contracts, service level agreements, and in the description of the service offering provided online and include the following:

- Commitments regarding the security and availability of the system and confidentiality of information processed by the system in accordance with contractual stipulations.
- Commitments regarding customer interactions as described in the master service agreement, service level agreement, and the system reference document.
- Commitments to support customer compliance with the security-related requirements of the EU General Data Protection Regulation, as set forth in the master services agreement.

SOCi establishes operational requirements that support the achievement of security commitments, relevant operational and compliance requirements, applicable laws and regulations, and other system requirements. These include system requirements (both functional and non-functional) derived from service commitments, published documentation of system functionality, and other descriptions of the system.

Such requirements are communicated in SOCi's system policies and procedures, system design documentation, and contracts with customers.

SOCi has adopted the ISO/IEC 27001:2022 and ISO/IEC 27701:2019 as the basis for its organization-wide information security policies. In addition to these policies, standard operating procedures have been developed and documented on how to carry out specific manual and automated processes required in the operation and development of the SOCi. System requirements based on ISMS & PIMS include the following:

- Data, personnel, devices, systems, and facilities are identified and managed.
- SOCi management understands and manages the cybersecurity risk to organizational operations.
- SOCi's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

[2] Service commitments are commonly reflected in existing documents, such as service level agreements, available to customers and business partners. In most situations, rather than including a reference to the principal service commitments in these existing documents, management would list the individual commitments in the description.

- Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
- Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
- Security policies, processes, and procedures are maintained and used to manage protection of information systems and assets.
- Maintenance and repairs of information system components are performed consistent with policies and procedures.
- Technical security solutions are managed to help ensure the security and resilience of systems and assets.
- Anomalous activity is detected and the potential impact of events is understood.
- The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
- Detection processes and procedures are maintained and tested to help ensure awareness of anomalous events.
- Response processes and procedures are executed and maintained to help ensure response to detected cybersecurity incidents.
- Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.
- Recovery processes and procedures are executed and maintained to help ensure restoration of systems or assets affected by cybersecurity incidents.

4 Illustrative Independent Service Auditor's SOC 3 Report

4.1 Independent Service Auditor's Report on a SOC 3 Examination[3]

To: Management of SOCi Service Organization

4.2 Scope

We have examined SOCi's Service Organization's (SOCi's) accompanying assertion titled "Assertion of SOCi Service Organization Management" (assertion) that the controls within SOCi's (system) were effective throughout the period between October 1, 2024 – September 30, 2025, to provide reasonable assurance that ABC's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria.

4.3 Service Organization's Responsibilities

SOCi Service Organization is responsible for providing the services covered by the description; specifying its service commitments and system requirements; identifying the risks that threaten the achievement of the service organization's service commitments and system requirements and designing, implementing, and operating effective controls within the system to provide reasonable assurance that SOCi service commitments and system requirements and its business objectives, security requirements and compliance obligations were achieved; preparing the description, including stating the related controls in the description and the completeness, accuracy, and method of presentation of the description; and selecting the applicable trust services criteria as the criteria against which the controls were measured. SOCi Service Organization has provided the accompanying assertion, in Section 1, ("assertion") about the description, the suitability of design, and the operating effectiveness of controls. SOCi is also responsible for the completeness, accuracy, and method of presentation of the assertion.

4.4 Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and the suitability of the design and the controls' operating effectiveness stated in the description, based on our examination. Our examination was conducted in accordance with the attestation standards established by the American Institute of Certified Public Accountants. These standards require that we plan and perform our examination to obtain reasonable assurance about

3 The report may also be titled "Report of Independent Service Auditors."

whether, in all material respects, the description is presented in accordance with the description criteria and whether the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria, and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description.

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

4.5 Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs. There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with policies or procedures may deteriorate.

4.6 Description of Tests of Controls

The specific controls we tested, and the nature, timing, and results of those tests, are presented in the test matrices in Section 4 of our report titled "Applicable Trust Service Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests."

4.7 Opinion

In our opinion, in all material respects,

a) The description presents SOCi Service Organization's Infrastructure Services system that was designed and implemented for the period between October 1, 2024 – September 30, 2025, in accordance with the description criteria; and,

b) The controls stated in the description were suitably designed as of for the period between October 1, 2024 – September 30, 2025 to provide reasonable assurance that SOCi Service Organization's service commitments and system requirements would be achieved based on the applicable trust services criteria and its business objectives, security requirements, and compliance obligations would be achieved based on applicable trust services criteria throughout that period.

c) The controls stated in the description operated effectively for the period between October 1, 2024 – September 30, 2025, to provide reasonable assurance that SOCi service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of SOCi controls operated effectively throughout that period.

4.8 Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of SOCi Service Organization; user entities of SOCi Service Organization's Infrastructure Services system for the period between October 1, 2024 – September 30, 2025; business partners of SOCi Service Organization subject to risks arising from interactions with the Infrastructure Services system; practitioners providing services to such user entities and business partners; prospective user entities and business partners; regulators; and sponsoring organizations who have sufficient knowledge and understanding of the following:

- The Nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties;
- Internal control and its limitations;

- Complementary user entity controls and complementary subservice organization controls, and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services;
- The applicable trust services criteria;
- The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Signature: Joseph Weindorfer **Date:** 2025-12-03

Joseph Weindorfer, CPA

CISSP, ITiL, MCSE, M.S

Audit trail

Details

FILE NAME	SOCi Inc Form 051 SOC3 Examination Report.pdf - 12/3/25, 4:24 AM
STATUS	Signed
STATUS TIMESTAMP	2025/12/03 13:23:43 UTC

Activity

SENT	juvie@consilium-labs.com **sent** a signature request to: • Joseph Wiendorfer (joseph@consilium-labs.com)	2025/12/02 20:24:38 UTC
SIGNED	**Signed** by Joseph Wiendorfer (joseph@consilium-labs.com)	2025/12/03 13:23:43 UTC
COMPLETED	This document has been signed by all signers and is **complete**	2025/12/03 13:23:43 UTC

The email address indicated above for each signer may be associated with a Google account, and may either be the primary email address or secondary email address associated with that account.