Alembic

Alembic Technologies, Inc

Report on Controls at a Service
Organization Relevant to
Security, Confidentiality,
Availability

SOC 3^{SM} Report

For the Period May 1, 2020 to July 31, 2020

*SOC 3 is a registered service mark of the American Institute
of Certified Public Accountants (AICPA)*

BARR
ADVISORY

Independent Service Auditor's Report

To the Management of Alembic Technologies, Inc. (Alembic):

Scope

We have examined Alembic's accompanying assertion titled "Assertion of Alembic Management" (assertion) that the controls within the Alembic system (system) were effective throughout the period May 1, 2020 to July 31, 2020, to provide reasonable assurance that Alembic's service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality, and availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria).

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

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

Our examination included:

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

- Assessing the risks that controls were not effective to achieve Alembic's service commitments and system requirements based on the applicable trust services criteria

- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Alembic's service commitments and system requirements based on the applicable trust services criteria

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

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

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

procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within the Alembic system were effective throughout the period May 1, 2020 to July 31, 2020, to provide reasonable assurance that Alembic's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

BARR Advisory, P.A.

Fairway, KS

September 15, 2020

Assertion of Alembic Management

We are responsible for designing, implementing, operating, and maintaining effective controls within the Alembic system (system) throughout the period May 1, 2020 to July 31, 2020, to provide reasonable assurance that Alembic's service commitments and system requirements relevant to security, confidentiality, and availability were achieved. Our attached system description of the Alembic system identified the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period May 1, 2020 to July 31, 2020, to provide reasonable assurance that Alembic's service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality, and availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria). Alembic's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in the attached system description.

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

We assert that the controls within the system were effective throughout the period May 1, 2020 to July 31, 2020, to provide reasonable assurance that Alembic's service commitments and system requirements were achieved based on the applicable trust services criteria.

Alembic Technologies, Inc

September 15, 2020

Overview of Operations

Description of Services Provided

Alembic Technologies, Inc. ("Alembic" or the "company") provides Marketing Automation Software as a Service (SaaS) throughout the United States and Europe. The company was founded in 2018.

Alembic's SaaS offering (the "system") streamlines the complexities of marketing across multiple platforms for enterprise and mid-market users, building a single portal to coordinate and quantify campaigns across multiple channels. Services include:

- Metrics Collection: Automated ingestion of data from multiple sources
- Attribution: Link shortening, callbacks URL, and mix analysis without cookies
- Predictive Analytics: Baseline, future, and demographic
- Channel Execution: Execute on social, email, direct mail, SMS, and API
- Asset Management: Images, video, text, PDFs, and more

Principal Service Commitments and System Requirements

Alembic designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Alembic makes to user entities, the laws and regulations that govern its services, and the financial, operational, and compliance requirements that Alembic has established. The system services are subject to the security, confidentiality, and availability commitments established internally for its services.

Commitments to user entities are documented and communicated in service-level agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online.

Security commitments include, but are not limited to, the following:

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role;
- Regular vulnerability scans over the system and network, and penetration tests over the production environment; and,
- Operational procedures for managing security incidents and breaches, including notification procedures.

Confidentiality commitments include, but are not limited to, the following:

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

Availability commitments include, but are not limited to, the following:

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components;

- Responding to customer requests in a reasonably timely manner;

- Business continuity and disaster recovery plans that include detailed instructions, recovery point objectives (RPOs), recovery time objectives (RTOs), roles, and responsibilities; and,

- Operational procedures supporting the achievement of availability commitments to user entities.

Such requirements are communicated in Alembic's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures are documented on how to carry out specific manual and automated processes required in the operation and development of the system.

Components of the System Used to Provide the Services

The purpose of the system description is to delineate the boundaries of the system, which includes the services and commitments outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Infrastructure

The system is hosted in Amazon Web Services (AWS) in a virtual private cloud (VPC) environment which protects the network from unauthorized external access. The network topology includes segmented VPCs and access control lists (ACLs). User requests to Alembic's web-based systems are encrypted using Transport Layer Security (TLS) using certificates from an established third party certificate authority. System administration access to Alembic web and application servers is possible only through dedicated bastion hosts. The hardware components that make up the aforementioned system include servers hosted, managed, and protected by AWS. AWS maintains production servers with failover capabilities. This infrastructure is hosted in high availability data centers with multiple availability zones.

Software

Alembic is responsible for managing the development and operation of the Alembic platform including infrastructure components such as servers, database and storage systems.

People

Alembic has a staff of approximately 14 employees organized in the following functional areas:

- **Corporate:** Responsible for overseeing company wide activities, establishing and accomplishing goals, and overseeing objectives.

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

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

- **Security:** Responsible for access controls and security of the production environment.
- **People:** Responsible for recruiting and onboarding new personnel, defining roles and positions for new hires, performing background checks, and facilitating the employee termination process.
- **IT:** Responsible for managing laptops, software, and other technology involved in employee productivity and business operations.
- **Customer Success:** Responsible for sales, account management, customer success, and customer support activities.

Data

Data, as defined by Alembic, constitutes the following:

- Input, including the following:
    - Customer provided access tokens for social media and email services
    - Alembic collected data using the aforementioned tokens
    - Lists and CRM data inputted by customers
- Output, including the following:
    - Analytics and derived data based on the collected data
    - Social media posts and emails sent on a scheduled basis by customers
    - Reports based on the previously mentioned inputs

Output reports are available and include data and files systematically generated from the system. The availability of these reports is limited by job function. Reports delivered externally are only sent using a secure method, typically over HTTPS. Alembic does not offer any other form of access at this time.

Information assets are assigned a sensitivity level based on the audience for the information. If the information has been previously classified by regulatory, legal, contractual, or company directive, then that classification will take precedence. The sensitivity level then guides the selection of protective measures to secure the information. All data are to be assigned one of the following sensitivity levels:

- **Restricted**: Highly valuable and sensitive information where the level of protection is dictated externally by legal and/or contractual requirements. Access to restricted information is limited to authorized employees, contractors, and business partners with a specific need.
- **Confidential**: Highly valuable and sensitive information where the level of protection is dictated internally.
- **Internal Use**: Information that originated or is owned internally, or was entrusted to Alembic by others. Internal use information may be shared with authorized employees, contractors, and business partners but not released to the general public.
- **Public**: Information that has been approved for release to the public and is freely shareable both internally and externally.

Type of Data	Example(s) of Data	Public	Internal	Confidential	Restricted
User accounts	• Email address • Password			X	
Hashes of passwords	• User Password			X	
Users' individual identifiers	• Alternative unique identifier • IP address				X
Users' location when interacting with the application	• City • State • Country				X
System-recorded information	• Account creation date • Date of last login • Chat logs with customer service			X	
Company documents	• Policy and process documents • Technical documentation		X		
Company data	• Product roadmap • Change tracking • Calendars		X		
Logos	• Images • Icons • Branding	X			

Processes and Procedures

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

- Information security policy and organization
- Risk management
- Asset management
- Access control
- Communications and network security
- Change management and secure development life cycle
- Vulnerability management

- Incident management and response

- Business continuity and planning

- Compliance

- Endpoint management

- Personnel security

- Data classification (data at rest, in motion, and output)

Complementary User Entity Controls

Alembic controls were designed with the assumption that certain internal controls would be in place at customer organizations. The application of such internal controls by customer organizations is necessary to achieve certain trust services criteria identified in this report. In addition, there may be control activities that are not identified in this report that would be appropriate for processing of transactions for Alembic customers.

For customers to rely on the information processed through the Alembic application, each customer is expected to evaluate its own internal controls to ensure appropriate control activities are in place. The following general procedures and controls should be considered. They should not, however, be regarded as a comprehensive list of all controls that should be implemented by customer organizations.

- User entity is responsible for protecting established user IDs and passwords within their organizations.

- User entity is responsible for reviewing customer access to the Alembic application periodically to validate appropriateness of access levels.

- User entity is responsible for approving and creating new user access to the Alembic application.

- User entity is responsible for removing terminated employee access to the Alembic application.

- User entity is responsible for implementing policies and procedures over the types of data that are allowed to be entered into the Alembic application.

- User entity is responsible for sending data to Alembic via a secure connection and/or the data should be encrypted.

- User entity is responsible for notifying Alembic if they detect or suspect a security incident related to the Alembic system.

- User entity is responsible for reviewing email and other forms of communications from Alembic, related to changes that may affect Alembic customers and users, and their security or availability obligations.

- User entity is responsible for establishing, monitoring, and maintaining controls over the security for system-generated outputs and reports from the system.

- User entity is responsible for endpoint protection of workstations used to access the system.

- User entity is responsible for developing their own business continuity and disaster recovery plan.

Complementary Subservice Organization Controls

Alembic uses subservice organizations in support of its system. Alembic's controls related to the system cover only a portion of overall internal control for user entities. It is not feasible for the trust services criteria over the Alembic system to be achieved solely by Alembic. Therefore, user entity controls must be evaluated in conjunction with Alembic's controls described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Alembic periodically reviews the quality of the outsourced operations by various methods including:

- Review of subservice organizations' SOC reports;
- Regular meetings to discuss performance; and,
- Non-disclosure agreements.

Control Activity Expected to be Implemented by Subservice Organization	Subservice Organization	Applicable Criteria
Logical access to the underlying network and virtualization management software for the cloud architecture is appropriate.	AWS	CC6.1, CC6.2, CC6.3, CC7.2
Physical access to the data center facility is restricted to authorized personnel.	AWS	CC6.4,
Environmental protections, including monitoring and alarming mechanisms, are implemented to address physical security and environmental control requirements.	AWS	CC6.4, A1.2,
Business continuity and disaster recovery procedures are developed, reviewed, and tested periodically.	AWS	A1.3
Policies and procedures to document repairs and modifications to the physical components of a facility including, but not limited to, hardware, walls, doors, locks, and other physical security components.	AWS	A1.2
The Company has a defined Data Classification Standard, which specifies classification levels and control requirements in order to meet the Company's commitments related to confidentiality.	AWS	C1.1
The Company has a defined process to sanitize and destroy hard drives and back up media containing Customer Data prior to leaving Company facilities.	AWS	C1.2