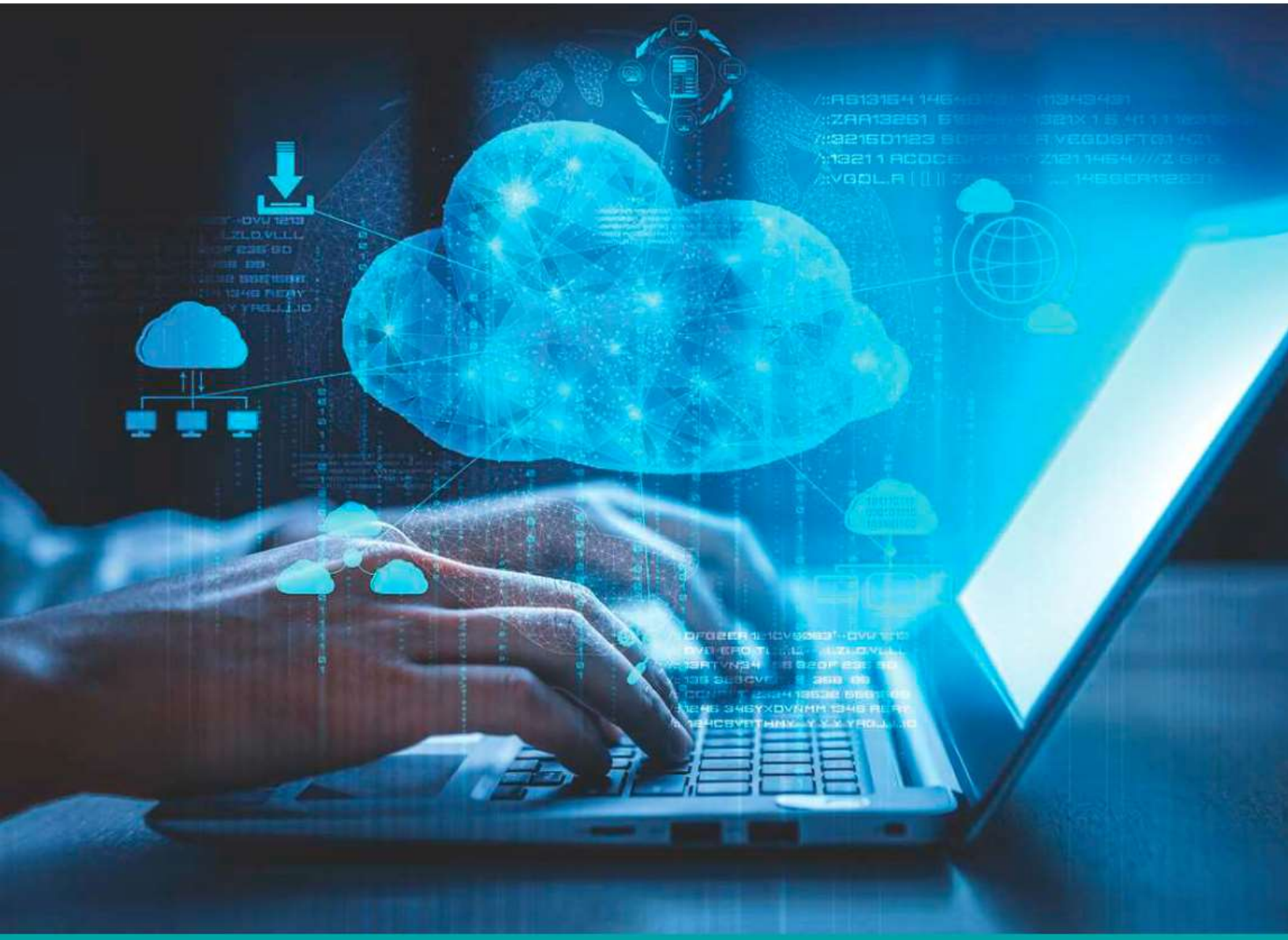
linford&co llp
cpa firm

afi.ai



SOC 3

REPORT ON CONTROLS RELEVANT TO SECURITY AND AVAILABILITY

MARCH 16, 2022 TO MARCH 15, 2023

Afi Technologies, Inc.

Report on Afi Technologies, Inc.'s Description of Its Afi Platform and on Its Controls Relevant to Security and Availability

Table of Contents

linford&co llp
cpa firm

linford&co llp
1550 wewatta st, 2nd floor
denver, co 80202

tel: +1 (720) 330 7201
email: info@linfordco.com
www.linfordco.com

Section I – Independent Service Auditor's Report

To the Executive Management of Afi Technologies, Inc.:

Scope

We have examined Afi Technologies, Inc.'s (Afi or the Company) accompanying assertion titled "Assertion of Afi's Management" (assertion) that the controls within Afi's Afi platform were effective throughout the period March 16, 2022 to March 15, 2023, to provide reasonable assurance that Afi's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability 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

Afi 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 Afi's service commitments and system requirements were achieved. Afi has also provided the accompanying assertion about the effectiveness of controls supporting its Afi platform. When preparing its assertion, Afi is responsible for selecting, and identifying in its assertion, the applicable trust services 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 service organization's service commitments and system requirements.
- ✓ Assessing the risks that controls were not effective to achieve Afi'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 Afi'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 supporting Afi's Afi platform were effective throughout the period March 16, 2022 to March 15, 2023 to provide reasonable assurance that Afi's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

linford&co llp

April 4, 2022
Denver, Colorado

Afi Technologies, Inc.
210 N University Dr, STE 303
Coral Springs, FL 33071

Section II – Assertion of Afi's Management

April 4, 2023

We are responsible for designing, implementing, operating, and maintaining effective controls within Afi Technologies, Inc.'s (Afi or the Company) Afi platform throughout the period March 16, 2022 to March 15, 2023, to provide reasonable assurance that Afi's service commitments and system requirements relevant to security and availability were achieved. Our description of the boundaries of the system and services is presented in Section III and identifies the aspects of the system and services covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period March 16, 2022 to March 15, 2023 to provide reasonable assurance that Afi's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Afi'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 Section III.

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 March 16, 2022 to March 15, 2023, to provide reasonable assurance that Afi's service commitments and system requirements were achieved based on the applicable trust services criteria.

Daniel Pomar
Director

Section III – Afi's Description of Its Afi Platform

Overview of Operations and System Boundaries

Overview of the Organization

Headquartered in Coral Springs, Florida, with engineering offices in the USA, Poland, Cyprus, and Romania, Afi provides a cloud-native backup solution that is built to support cloud applications such as Google Workspace (formerly G Suite), Microsoft 365 (formerly Office 365), Kubernetes, as well as the Google Cloud Platform, Amazon Web Services, Microsoft Azure.

Leveraging the capabilities of artificial intelligence (AI), Afi provides highly resilient data management platform while maintaining a simple and secure solution. Using AI, Afi helps organizations maintain their compliance with data regulations by monitoring for orphaned data and user accounts. Afi's security-enabled backup solution protects organization's data, including metadata. All back data is stored in high-endurance, high-available storage, which is encrypted with a unique encryption key for each client and is protected against tampering. The Afi product enables fast data recovery in the event of data loss, a ransomware attack, or human error. Granular access controls, detailed audit logs, SSO via Microsoft, Google and Okta, and customer managed encryption options also provide critical security functions.

Principal Service Commitments and System Requirements: Afi designs its processes and procedures to meet objectives for its Afi platform. Those objectives are based on the service commitments that Afi makes to user entities and the compliance requirements that Afi has established for its services.

Security commitments to user entities are documented and communicated in its customer agreements. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental design of the Afi platform are implemented to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Controlled access to the production application and the supporting infrastructure.
- Segregation of client data.
- Data backups.
- Monitoring of system performance metrics and critical application services.

Afi establishes operational requirements that support the achievement of security commitments and other system requirements. Such requirements are communicated in Afi'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 networks are managed, and how employees are hired and trained.

Components of the System Used to Provide the Services

Infrastructure

Afi uses a subservice organization to provide its services to its clients in order to achieve operating efficiency and to obtain specific expertise. The following is the principal subservice organization used by Afi:

- ✓ **GCP**—GCP hosts Afi's production IT environment. GCP undergoes a Type II SOC 2 examination annually, and the report may be obtained directly from them. Afi obtains and reviews the SOC 2 report provided by GCP related to its hosting operations to determine whether controls are designed and operating effectively. Additionally, any listed complementary user entity controls in the GCP SOC report are reviewed and addressed by Afi.

Software

The Afi platform is a cloud-native backup solution that leverages AI and has deep support of cloud data sources. It is developed and maintained by Afi's in-house engineering team. The software engineering team enhances and maintains the Afi platform to provide services to its user entities. The Afi platform is a multi-user, web-based, software-as-a-service (SaaS) application. Role-based access controls (RBAC) govern the capabilities employees and users can execute within the platform.

People

Afi has a small staff organized into functional areas so personnel understand their responsibilities within the organization.

Data

Client data is stored within the Afi platform production database instance and GCP storage buckets. Afi has implemented security controls to protect the confidentiality of the data. Access controls have been implemented to control access to client data within the Afi platform database and storage buckets. Additionally, all data transfers between users and the Afi platform are secured using Transport Layer Security (TLS) and industry standard encryption.

Processes and Procedures

Afi has established and maintains security policies and procedures over the Afi Platform covering the following areas:

- Information Security
- Data Retention and Disposal
- Removable Media
- Acceptable Use
- Application Security
- Availability
- Chang Management
- Confidentiality
- Software Development Lifecycle
- Business Continuity

- Encryption
- Incident Response
- Log Management and Audit
- Passwords
- Remote Access
- Data Retention and Disposal
- Risk Assessment
- Vendor Management
- Workstation Security

Afi makes these internal policies and procedures, including security policies, available to its personnel on their shared document repository site to provide direction regarding their responsibilities related to the functioning of internal control.

Afi also provides information to clients and employees on how to report failures, incidents, concerns, or complaints related to the services or systems provided by Afi in the event there are problems and takes actions as appropriate when issues are raised.

Logical access controls are employed throughout the environment which support delivery of the Afi platform. For new employees, requests for initial IT access and asset provisioning are originated by management. All initial access requests are documented in a new hire checklist. In addition, there is a process to determine access is removed when an employee is terminated. For terminated employees, management completes a termination checklist which includes tasks to remove logical access. Employee terminations are treated as a high priority, and access is disabled from all applicable systems on the day of termination. Terminated employee's logical access to the Afi application, associated infrastructure, and data is removed in a timely manner.

System administrator-level access privileges to the GCP environment are restricted to only those individuals who require such access to perform their respective job functions. Access is limited to certain individuals within management who require administrator access and the ability to manage users. In the default configuration, no one can log in to the operating system of the hosts in the production environment as the OS Login functionality is disabled. The Google Kubernetes Engine (GKE) provides the mechanism to interact with the Afi Kubernetes cluster. Administration of the cluster environment occurs through command line tools with infrastructure-as-code tools for infrastructure provisioning and management. Access to the production Kubernetes cluster environment is restricted to only those individuals who require such access to perform their respective job functions. Changes to the production infrastructure are made through the change management process as the infrastructure is managed as code.

Infrastructure password parameters have been configured to be compliant with Afi policies and industry best practices. Password parameters for access to the GCP administration console require a certain level of complexity to minimize the risk of unauthorized access through password guessing. MFA is implemented for access to the GCP administration console. Afi does not manage client passwords for access to the Afi platform. Access is based on clients' Microsoft 365 or Google Workspace accounts. By default, only client Microsoft 365 or Google Workspace administrators have access to the Afi platform. These administrators then grant access to members of their organization. Client access to the Afi platform is granted through single sign on via Microsoft 365 or Google Workspace .

Afi's security policies require workstations to have appropriate end-point protection. Workstations are required to employ antimalware software and be up to date for their operating system. Afi uses a signature-based capability to detect and eradicate malware in its environment. Afi also applies security patches to user workstations that access the production environment at least monthly in accordance with its patch policy, and production Kubernetes clusters are updated to run on recent versions in the stable release channel. To minimize the risk that data is compromised if hardware or data is lost or stolen, Afi requires all employee laptops to be encrypted.

Afi understands the sensitivity of its clients' data and has, therefore, implemented security controls to protect the confidentiality of the data. Client data within the Afi production environment is encrypted at rest.

Afi also maintains backups and monitors the performance of the environment supporting its Afi platform. To protect client data from loss in the event of a system failure, backups are captured daily, stored for seven days, and are replicated across availability zones. Procedures have been developed that outline how to restore the Afi database to an operational state from a backup should the need arise, and the procedures are executed regularly so that restore operations are executed smoothly when needed. A backup of the Afi database is restored periodically so that restore operations are executed smoothly if needed.

To maintain the stability and availability of the infrastructure environment, Afi monitors key performance parameters such as CPU and memory utilization on the production system and is notified when such parameters exceed configured thresholds. Service availability, services stability, abnormal backup/recovery/export failures, services scalability and production load, and DB performance utilization are also monitored. This allows for a proactive response immediately to any potential issues with infrastructure resources. Alerts are generated from monitoring tools, sent to Company staff, and are addressed immediately.