ISPARTNERS

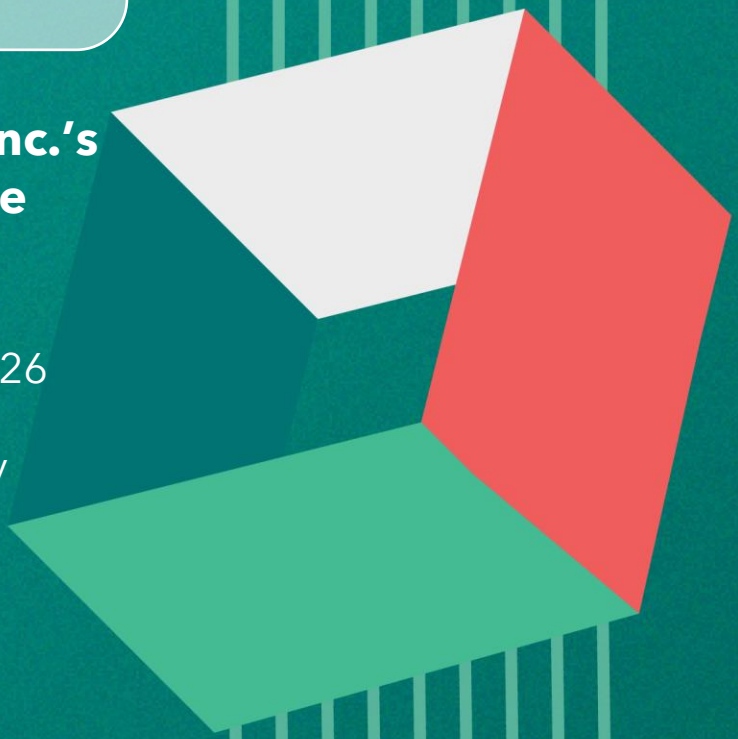
afi.ai

Report on Afi Technologies, Inc.'s Management Assertion for the Afi Platform

April 1, 2025 through March 31, 2026

Relevant to Security and Availability

SOC 3®



I. INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of Afi Technologies, Inc.:

Scope

We have examined Afi Technologies, Inc.'s ("Afi" or the "Company") accompanying assertion titled "Management Assertion of Afi Technologies, Inc." ("assertion") that the controls within the Afi Platform ("system") were effective throughout the period April 1, 2025 through March 31, 2026, 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 ("applicable trust services criteria") set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (with Revised Points of Focus–2022)* (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 within the system. When preparing its assertion, Afi 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 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.

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

Inherent limitations

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

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

Opinion

In our opinion, management's assertion that the controls within the Afi Platform were effective throughout the period April 1, 2025 through March 31, 2026, 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.

IS Partners, LLC

IS Partners, LLC
Dresher, Pennsylvania
May 11, 2026

II. MANAGEMENT ASSERTION OF AFI TECHNOLOGIES, INC.

We are responsible for designing, implementing, operating, and maintaining effective controls within Afi Technologies, Inc.'s Afi Platform ("system") throughout the period April 1, 2025 through March 31, 2026, 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 is presented in this report and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2025 through March 31, 2026, 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 ("applicable trust services criteria") set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (with Revised Points of Focus—2022)* (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.

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 April 1, 2025 through March 31, 2026, to provide reasonable assurance that Afi's service commitments and system requirements were achieved based on the applicable trust services criteria.

Afi Technologies, Inc.
May 11, 2026

III. DESCRIPTION OF THE BOUNDARIES OF AFI TECHNOLOGIES, INC.'S AFI PLATFORM

Company Background

Headquartered in Coral Springs, Florida, with engineering offices in the U.S., Poland, Cyprus, Spain and Czech Republic, 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, and Microsoft Azure.

Overview of the Services Provided

Leveraging the capabilities of artificial intelligence (AI), Afi provides a 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 organizations' data, including metadata. All backup 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, context-aware access policies, lockdown mode protection for sensitive data management operations, detailed audit logs and SIEM integrations, SSO via Microsoft, Google, and Okta/SAML, 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 and availability 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 and availability 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.

The system is comprised of the following five components:

- Infrastructure (systems and networks)
- Software (utilities)
- People (consultants and project managers)
- Procedures (automated and manual)
- Data (transactions streams, files, databases, and tables)

The following sections of this description define each of these five components comprising Afi's system.

Infrastructure

The Company's IT infrastructure is geographically distributed across the United States, Europe (Netherlands), United Kingdom, Australia, and Canada. The core server infrastructure is deployed as Kubernetes clusters within the Google Cloud Platform (GCP) environment. The architecture leverages various GCP-managed services, including Google Cloud Storage, Managed Google Cloud SQL, and Managed Google Cloud Redis. Infrastructure deployment is automated and managed using Infrastructure as Code (IaC) principles through Terraform, along with policy-as-code practices for user management. Kubernetes clusters are actively utilized to orchestrate containerized applications. The database architecture is regionally segmented, with database instances deployed per region to support data locality and redundancy requirements. Internal domain management is conducted through Google Workspace Directory (GW Directory), with no traditional domain controllers managed internally. The operating system employed for server and workstation environments is Container-Optimized OS, designed specifically to support secure, efficient container deployments.

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

- Google Cloud Platform (GCP) – GCP hosts Afi's production IT environment. Infrastructure is deployed using Infrastructure as Code (Terraform), with policy-as-code practices also in place. Afi utilizes Kubernetes clusters, Google Cloud Storage, Managed Cloud SQL, and Redis instances, all within GCP. The environment spans multiple regions, including the United States, Europe (Netherlands), the United Kingdom, Australia, and Canada. Each region maintains its own dedicated database instance.

GCP undergoes a SOC 2 Type II 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.

Internally, Afi uses Google Workspace Directory for user management.

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-tenant, 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.

- Slack, Google Workspace and M365 - communications and collaboration.
- Atlassian - task tracking and internal documentation.
- Github - code collaboration and CI.
- CircleCI - CI/CD, Runs tests and deployments automatically after code changes.
- Sentry - error reporting, Monitors apps for crashes and bugs.
- Mailgun - email automation.
- Stripe - payment processing.
- Hubspot - Sales CRM, Manages contacts, deals, and email communication
- Zendesk - Support automation.

People

Afi is organized into functional areas: R&D, Support, Professional Service, Sales, Marketing, Legal and Administration, so personnel understand their responsibilities within the organization.

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
- Change Management
- Confidentiality

- Software Development Lifecycle
- Business Continuity
- Encryption
- Log Management and Audit
- Passwords
- Remote Access
- Incident Response
- 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.

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.