BAKER NEWMAN NOYES

Akumina Inc.

Report on Akumina Inc.'s Description of Its Employee Experience Platform and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security, Availability and Confidentiality

For the Period March 16, 2022 through March 15, 2023

Baker Newman & Noyes LLC
MAINE | MASSACHUSETTS | NEW HAMPSHIRE
800.244.7444 | www.bnncpa.com
HLB WE ARE AN INDEPENDENT MEMBER OF THE GLOBAL ADVISORY AND ACCOUNTING NETWORK

AKUMINA INC.

REPORT ON AKUMINA INC.'S DESCRIPTION OF ITS EMPLOYEE EXPERIENCE PLATFORM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY, AVAILABILITY AND CONFIDENTIALITY

For the Period March 16, 2022 through March 15, 2023

TABLE OF CONTENTS

SECTION I

INDEPENDENT SERVICE AUDITORS' REPORT

BAKER NEWMAN NOYES

Baker Newman & Noyes LLC
MAINE | MASSACHUSETTS | NEW HAMPSHIRE
800.244.7444 | www.bnncpa.com

HLB WE ARE AN INDEPENDENT MEMBER OF THE GLOBAL ADVISORY AND ACCOUNTING NETWORK

INDEPENDENT SERVICE AUDITORS' REPORT

To Management of Akumina Inc.

Scope

We have examined Akumina Inc.'s (Akumina) accompanying description in Section III, titled "Description of Akumina Inc.'s Employee Experience Platform," throughout the period March 16, 2022 to March 15, 2023 (description) based on the criteria for a description of a service organization's system in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, in AICPA *Description Criteria* (description criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period March 16, 2022 to March 15, 2023 to provide reasonable assurance that Akumina'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* (AICPA, Trust Services Criteria).

Akumina uses the Microsoft Azure subservice organization for authentication services and hosting of its production infrastructure. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Akumina, to achieve Akumina's service commitments and system requirements based on the applicable trust services criteria. The description presents Akumina's controls, the applicable trust services criteria and the types of complementary subservice organization controls assumed in the design of Akumina's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with the controls at Akumina, to achieve Akumina's service commitments and system requirements based on the applicable trust services criteria. The description presents Akumina's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Akumina's controls. Our examination did not include such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Akumina 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 Akumina's service commitments and system requirements were achieved. In Section II, Akumina has provided an assertion about the description and suitability of design and operating effectiveness of the controls stated therein. Akumina is also responsible for preparing the description and assertion, including the completeness, accuracy and method of presentation of the description and assertion, providing the services covered by the description, selecting the applicable trust services criteria and stating the related controls in the description, and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

To Management of Akumina Inc.

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operating 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.

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

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the 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.

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 information 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 the policies or procedures may deteriorate.

To Management of Akumina Inc.

Description of Tests of Controls

The specific controls we tested and the nature, timing and results of our tests are presented in Section IV.

Opinion

In our opinion, in all material respects:

- The description presents Akumina's Employee Experience Platform that was designed and implemented throughout the period March 16, 2022 to March 15, 2023 in accordance with the description criteria.
- The controls stated in the description were suitably designed throughout the period March 16, 2022 to March 15, 2023 to provide reasonable assurance that Akumina's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Akumina's controls throughout that period.
- The controls stated in the description operated effectively throughout the period March 16, 2022 to March 15, 2023 to provide reasonable assurance that Akumina's 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 Akumina's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Akumina; user entities of Akumina's Employee Experience Platform during some or all of the period March 16, 2022 to March 15, 2023; business partners of Akumina subject to risks arising from interactions with the Employee Experience Platform; practitioners providing services to such user entities and business partners; prospective user entities and business partners; and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization;
- How the service organization's system interacts with user entities, subservice organizations, 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; and
- 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.

Baker Newman & Noyes LLC

Manchester, New Hampshire
May 30, 2023

SECTION II

AKUMINA INC.'S ASSERTION

DocuSign Envelope ID: A01C6BD4-FE52-4620-80EB-634C2B2166AE

AKUMINA INC.'S ASSERTION

We have prepared the accompanying description in Section III, titled "Description of Akumina Inc.'s Platform," throughout the period March 16, 2022 to March 15, 2023 (description) based on the criteria for a description of a service organization's system in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, in AICPA *Description Criteria* (description criteria). The description is intended to provide report users with information about the Employee Experience Platform that may be useful when assessing the risks arising from interactions with Akumina Inc.'s (Akumina) system, particularly information about system controls that Akumina has designed, implemented, and operated to provide reasonable assurance that its 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* (AICPA, *Trust Services Criteria*).

Akumina uses the Microsoft Azure subservice organization for authentication services and hosting of its production infrastructure. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Akumina, to achieve Akumina's service commitments and system requirements based on the applicable trust services criteria. The description presents Akumina's controls, the applicable trust services criteria and the types of complementary subservice organization controls assumed in the design of Akumina's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Akumina, to achieve Akumina's service commitments and system requirements based on the applicable trust services criteria. The description presents Akumina's controls, the applicable trust services criteria and the complementary user entity controls assumed in the design of Akumina's controls.

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

- The description presents Akumina's Employee Experience Platform that was designed and implemented throughout the period March 16, 2022 to March 15, 2023 in accordance with the description criteria;
- The controls stated in the description were suitably designed throughout the period March 16, 2022 to March 15, 2023 to provide reasonable assurance that Akumina's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Akumina's controls throughout that period; and

DocuSign Envelope ID: A01C6BD4-FE52-4620-80EB-634C2B2166AE

- The controls stated in the description operated effectively throughout the period March 16, 2022 to March 15, 2023 to provide reasonable assurance that Akumina's 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 Akumina's controls operated effectively throughout that period.

Akumina Inc.

DocuSigned by:
John DiBartolomeo
6B4C473BD3104A9...

John DiBartolomeo, Chief Financial Officer
Date: May 30, 2023

SECTION III

DESCRIPTION OF AKUMINA INC.'S EMPLOYEE EXPERIENCE PLATFORM

AKUMINA INC.

DESCRIPTION OF AKUMINA INC.'S EMPLOYEE EXPERIENCE PLATFORM

For the Period March 16, 2022 through March 15, 2023

DESCRIPTION OF SERVICES PROVIDED

System Overview

Akumina Inc.'s (Akumina or the Company) Employee Experience Platform (the "Akumina platform" or "the System") empowers small, medium and large enterprises to create personalized digital workplace experiences for their entire workforce. Akumina concentrates on the following distinct categories:

- Modern Intranet Solutions
- Digital Workplace Hub Solutions
- Employee Communications Solutions

Akumina is not an Identity and Access Management (IAM) provider; rather, the Akumina platform integrates with enterprise identities such as Azure Active Directory (AAD), Active Directory Federation Services (ADFS), and any other enterprise IAM solutions that federate with AAD. Akumina is not a Customer's primary source of data, rather most customer data is governed by pre-existing rules set up by the Customer and remains in the customers' data source systems, including O365, service request systems, HR platforms, and other integrations.

Akumina's Content and Site Management System enables Akumina users to envision, plan and create content for customers and their employees. Akumina's ServiceHub (an enterprise service bus offered by the Company) provides a way to host Akumina's and each Customer's REST APIs which integrate one or more data sources such as Microsoft 365, Salesforce.com, ServiceNow, Workday and other enterprise data systems that expose content and action for employees. The ServiceHub provides integration with Akumina's middle tier and frameworks for authentication/authorization, caching, performance and scalability. The ServiceHub can be hosted side by side with the AppManager or as a dedicated instance on a different URL.

Akumina's frontend is delivered via a 'headless runtime' whereas Akumina leverages the power of public cloud (such as MS Azure) to deliver a performant and scalable digital workplace experience that delivers only the Akumina framework in the runtime.

Customer experiences scale from modern intranets to immersive digital workplaces. These focused experiences are hyper-personalized and are designed to serve each consumer's needs on any device, in any language and at any time, while delivering on any consumable digital canvas such as:

- Browser on a PC, Mac or Smartphone;
- Native Mobile App (iOS and Android);
- Third-Party Applications such as Microsoft Teams;
- Kiosks; and
- Digital Signage overhead displays.

Akumina serves over six million end users across many industries and company sizes.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Akumina designs its processes and procedures related to its Akumina Experience Platform to meet its objectives. Those objectives are based on the service commitments that Akumina makes to user entities, the regulations that govern Software-as-a-Service (SaaS) providers, and the financial, operational, and compliance requirements that Akumina has established for the services.

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

- Security principles within the fundamental designs of the Akumina platform that are designed to permit system users to access the information they need based on the permission of least privilege provisioning; and
- Use of encryption protocols to protect customer data at rest and in transit.

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

- Managing capacity demand through the monitoring and evaluation of current processing capacity and usage rates; and
- Meeting company objectives through authorization, design, development, and monitoring of data backup processes, and recovery infrastructure.

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

- Information is defined and classified into categories with associated retention periods; and
- Data retention and disposal policies and procedures are documented and in place.

Akumina establishes operational requirements that support the achievement of security, availability, and confidentiality commitments, relevant regulations, and other system requirements. Such requirements are communicated in Akumina 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 have been documented on how to carry out specific manual and automated processes required in the operation and development of the Akumina platform.

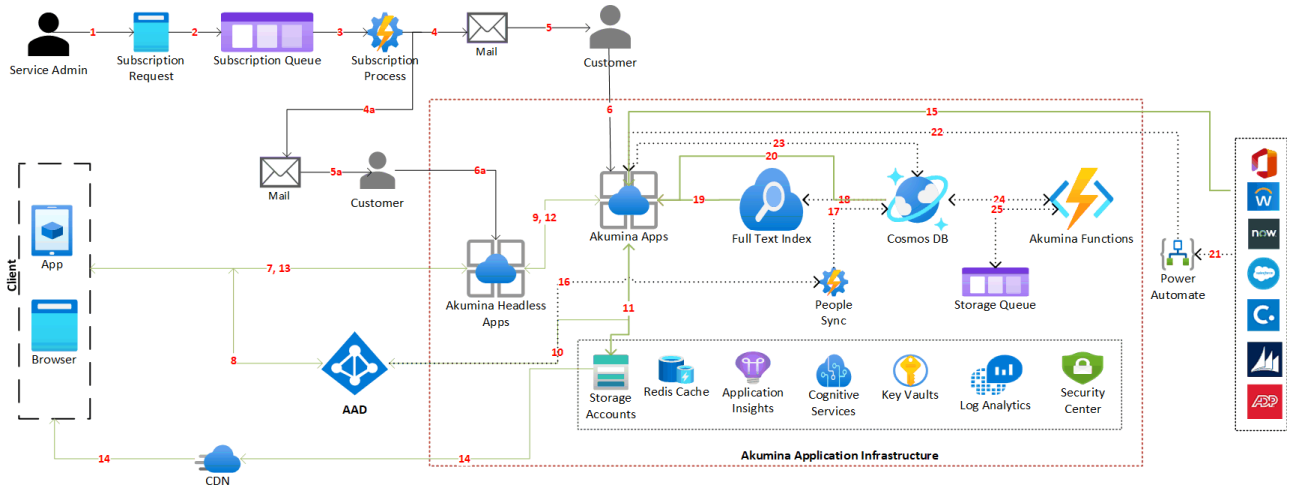
COMPONENTS OF THE SYSTEM USED TO PROVIDE SERVICES

Infrastructure

Akumina's platform is a web application developed and maintained by Akumina's in-house Development and Engineering Team and hosted on the Azure public cloud infrastructure. The Development and Engineering Team enhances and maintains the Akumina platform to provide the software and operations services.

The Akumina platform is a distributed set of computing services running in the cloud and in a customer environment. The Akumina Reference Architecture (below) is managed and maintained by Akumina technical staff.

Akumina Reference Architecture – SaaS



Akumina Application Flow

SUBSCRIPTION FLOW

(1) Initiate subscription request
(2) Complete customer's details
(3) Send customer details to subscription queue
(4) Process the AppManager subscription item
(5) Send email to customer with AppManager URL
(6) Customer opens the AppManager link to complete the tenant details
(4a) Process the Headless subscription item
(5a) Send Email to Customer with Headless URL
(6a) Customer Opens the Headless link to complete the tenant details

FRONT-END FLOW

(7) Users connecting to Front-End (SharePoint, Teams, or Akumina Headless)
(8) Application to Configured IDP (Identity Provider) for authentication
(9) Front-End requesting Akumina AppManager for data
(10) Akumina Application redirect for authentication, graph token acquired
(11) Token from "Previous Step" stored in storage for the user session
(12) Response returned to Front-End
(13) Client receives the response
(14) Static and framework files from CDN (Content Distribution Network)
(15) AppManager querying third party data through Service Hub custom implementation

PEOPLE SYNC PROCESS

(16) PeopleSync enumerates the user, group properties
(17) Exports the user, group properties to Cosmos DB
(18) Indexing user, group properties
(19) AppManager reading the Indexed Data for persona
(20) AppManager reading user, group properties for streams, social

BACKGROUND PROCESS

(21) Power automate checks the data changes
(22) Sends all enumerated changes to AppManager
(23) Writes all itemized data to Cosmos DB
(24) Cosmos DB triggers to Function App
(25) Function App writes the processing entries to queue and Cosmos DB

Access to the Akumina Application Infrastructure (above) environment is strictly controlled and explicitly authorized by management via service requests.

Servers – Akumina solutions operate exclusively on Microsoft Azure infrastructure using its platform as a Service (PaaS) environment for computing, databases, and monitoring.

Databases – Akumina uses Azure CosmoDB (SQL API) and Azure Storage (blobs, tables and queues). These database services are secured using at rest encryption and Azure virtual network.

Software

Akumina's platform leverages the following significant software products and solutions:

- Microsoft Azure – Infrastructure and hosting, and Azure-based web services and database services, including:
  - Azure DNS (Global DNS);
  - Front Door (Global Load Balancer);
  - Web Application Firewall (Global WAF);
  - Azure CDN;
  - Web Apps (Windows and Linux);
  - Function App;
  - Cosmos DB (SQL API);
  - Azure Storage (Blob, Table and Queue);
  - Cognitive Services (AI);
  - Cognitive Search (Full Text Indexing);
  - Key Vault;
  - Redis Cache;
  - Application Insight;
  - Log Analytics;
  - Virtual Networks;
  - Azure Sentinel; and
  - Microsoft Cloud Defender;
- Microsoft 365 – Email and collaboration including SharePoint and Teams;
- Microsoft Azure DevOps – Code repository and code workflow and tickets;
- Zendesk – Customer support management system;
- Sophos – Endpoint protection;
- Spiceworks – Service Desk Ticketing and Windows PC Mobile Device Management;
- HighTail – Secure Email Sharing Content; and
- Sendgrid – SMTP in cloud.

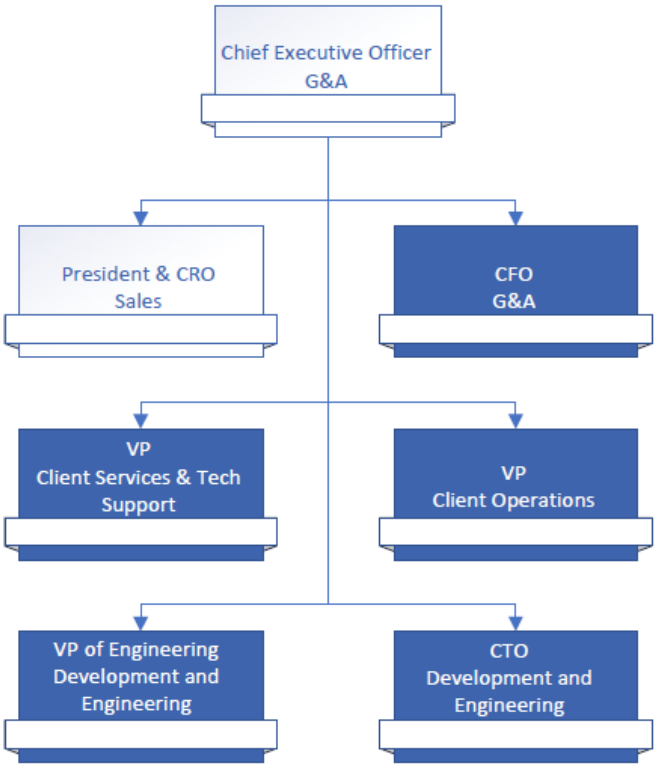
AKUMINA INC.

DESCRIPTION OF AKUMINA INC.'S EMPLOYEE EXPERIENCE PLATFORM

For the Period March 16, 2022 through March 15, 2023

People

Akumina has a staff of over 60 employees and full-time equivalent contractors organized in the following areas:



- *G&A* – This department is responsible for all General and Accounting concerns and includes Accounting, Finance, Human Resources, Legal and Procurement;
- *Development and Engineering* – This department designs and develops the Akumina applications and products. The staff includes software developers, quality assurance engineers, cloud operations, the IT Team and product managers; and
- *Client Services and Tech Support* – This department is responsible for supporting and communicating with the Akumina customer base in the implementation of and usage of the Akumina platform.

Procedures

Management has developed and communicated procedures to restrict logical access to Akumina. Changes to these procedures are performed annually and authorized by the Executive Management Team, comprising of members of management, who is responsible and accountable for designing, developing, implementing, operating, maintaining, monitoring and approving system controls and other risk mitigation strategies. These procedures cover the following key security life cycle areas:

- Acceptable Use Policy;

- Data Classification Policy;
- Encryption Policy;
- Backup and Retention Policy;
- High Availability and Disaster Recovery Policy;
- Incident Policy;
- Mobile Policy;
- New Hire and Termination Policy;
- Password Management Policy;
- Vendor Management Policy;
- Vulnerability Management Policy;
- Risk Assessment Policy;
- Cloud Access Control;
- Cloud Operations; and
- Client Onboarding processes.

Additionally, Akumina has regular penetration testing and vulnerability scans performed by a third-party. Results are communicated to the Development and Engineering Team who develop a remediation plan for all critical and high vulnerabilities.

Data

Data managed by Akumina includes:

- API keys;
- Customer endpoints configuration such as settings and attributes; and
- Application data including, but not limited to, streams and social features.

This customer data is logically separated and encrypted in transit and at rest, and all transport-level communication is encrypted using TLS 1.2.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCEDURES, INFORMATION AND COMMUNICATION SYSTEMS, AND MONITORING OF CONTROLS

Control Environment

Akumina's control environment is an integral part of its business activities, strategic planning, and assessment of risks. Relevant control environment factors that affect the services provided to user entities are listed and described below.

Human Resource Management

Written job descriptions for employees are maintained. The descriptions are reviewed and updated as needed. References are sought and background checks are performed for all employees. The responsibility of employees to comply with Akumina policies and protect confidential and proprietary information is explained during new employee orientation and documented in written policies. Employees are required to acknowledge receipt and understanding of the policies governing employee conduct as part of the onboarding process.

Akumina management performs annual performance evaluations to communicate and hold individuals accountable for performance of internal control responsibilities. The performance evaluation is signed by the manager and employee. Corrective actions, including training or sanctions, are taken as necessary.

Akumina conducts security awareness training during the onboarding of new employees and thereafter annually. The training is intended to enhance employees' understanding of a variety of sound security practices.

Physical Security and Environmental Controls

Akumina's applications are housed exclusively within Microsoft Azure facilities. Microsoft issues a third-party System and Organization Controls (SOC) 2 report. As part of management's vendor due diligence and ongoing monitoring process, Akumina receives and reviews the Microsoft Azure SOC 2 report at least annually to ensure that appropriate physical and environmental controls are in place and operating effectively at the subservice organization.

Akumina utilizes a proximity card system to control access to the Company facility, and access to the server room is restricted to appropriate individuals and is controlled by a physical key. The server room houses solely the Akumina Active Directory network.

Akumina relies on security infrastructure provided by Microsoft for all application hosting. The Development and Engineering Team monitors all the security events signaled by the Microsoft cloud monitoring system using Security Center.

Change Management

Akumina has a formalized change management process in place. Proposed changes are evaluated to determine if they present a security risk and what mitigating actions, including employee and user entity notifications, must be performed.

Changes to infrastructure and applications are designed, developed, and tested in separate development and test environments before applying changes to customers' environments. All changes are documented and triaged through an Agile development tool called Azure DevOps by the Development and Engineering Team. Once the changes are tested, confirmed, and ready for deployment, a person from the Deployment group will initiate the new deployment process to deploy to all or a particular cloud environment. This process requires additional approval from authorized individuals independent of development for code release.

Emergency changes follow the formalized change management process, but at an accelerated timeline. Prior to initiating an emergency change, necessary approvals are obtained and documented.

Akumina has a formalized security and systems development methodology that includes project planning, design, testing, implementation, and maintenance.

Akumina uses a standardized infrastructure as code and automated build server templates to help secure its servers and services, as well as conducts regular vulnerability assessments to identify potential system vulnerabilities.

System Monitoring, Incident and Problem Management

The Development and Engineering Team uses a variety of system monitoring and security utilities to identify and detect possible security threats and incidents. These utilities include, but are not limited to, vendor security notifications, intrusion detection system (IDS) or intrusion prevention system (IPS) alerts, vulnerability assessment reports, and operating system event logs. These alerts and notifications are reviewed by the security administration team using a security incident and event monitoring platform. The vulnerability assessment reports are reviewed by the Development and Engineering Team. System security event error logs are centralized and are monitored weekly by the respective team delegate. Issues are handled in accordance with the change management process.

Availability and security events requiring further investigation are tracked using an incident ticket and monitored until resolved. A technician or administrator responsible for security incident tickets follows a process of analyzing the security incident. The process begins with detailing what specific attack occurred, which system(s) were affected and what happened during the attack. Next the root cause is determined and the event is given a classification to assign the level of impact of the event. The impact level is based on guidelines detailed in the procedures. The remediation of the incidents of this type is considered an emergency and includes escalating the incident to the Development and Engineering Team to develop a fix (if required) and testify on the pre-production environment and then apply the fix to production.

Data Back Up and Recovery

Akumina uses data replication and snapshot techniques to back up its data files and software. Access to back-up storage, scheduling utilities, and systems is restricted to authorized personnel. Data backups are encrypted during transmission and storage and tested by the Development and Engineering Team at least annually.

System Account Management

Akumina has implemented role-based security to limit and control access within Azure. Employees are granted logical and physical access to in-scope systems based on documented approvals by appropriate management personnel through use of the ticketing system. The ability to create or modify user access accounts and user access privileges is limited to authorized personnel. User access is reviewed on at least an annual basis for the Akumina platform.

The G&A department manages employee terminations and works with the IT and Development and Engineering Teams to reconcile the termination report with current access privileges to determine if access has been appropriately removed or disabled.

Administrative access to identity directories and servers and databases is restricted to authorized employees.

Unique user identification numbers, names, and passwords are required to authenticate all users. Users are required to supply their credentials in order to access servers and systems and utilize a virtual private network (VPN) connection using multi-factor authentication. Additionally, passwords are required to meet minimum length and complexity characteristics. Monitoring systems provide monitoring and notification to the IT and Development and Engineering Teams. Intrusion attempts are logged, tracked, and communicated to affected parties until resolved.

Akumina ensures that only authorized devices connect to the Akumina system by utilizing IP address monitoring and where possible, just-in-time access is enabled for access to virtual machines. Additionally, Akumina logs access to information assets to ensure that an audit trail is available if there are any issues or noted unauthorized access.

Risk Assessment

Akumina regularly reviews the risks that may threaten the achievement of its service commitments and system requirements related to security, availability and confidentiality based on the applicable trust services criteria set forth in TSP section 100, *2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Akumina has established the Governance Committee consisting of:

- Chief Technology Officer
- Vice President, Client Operations
- Chief Financial Officer

The Governance Committee assesses security risks on an ongoing basis. This is done through regular management meetings, reviewing and acting upon security alerts and event logs, performing vulnerability assessments, and conducting a formal annual risk assessment.

The Governance Committee, as part of its annual policy review, considers the likelihood of fraud, developments in technology, and the impact of applicable laws and regulations on Akumina's security policies.

Information and Communication

Akumina has Information Security Policies to help ensure that employees understand their individual roles and responsibilities concerning processing and controls to ensure significant events are communicated in a timely manner. These include formal and informal training programs and the use of email and instant messaging to communicate time-sensitive information and processes for security and system availability purposes that notify key personnel in the event of problems.

Monitoring Activities

In addition to the daily oversight, periodic vulnerability assessments, and use of event monitoring tools, management provides further security monitoring through the Infrastructure group, which performs periodic audits to include information security assessments, such as an annual penetration test performed by a third party. The results of the test are reviewed by the Development and Engineering Team who develop a remediation plan for all critical and high vulnerabilities.

TRUST SERVICES CRITERIA AND RELATED CONTROL ACTIVITIES

Management selects, implements and manages control activities through Policies and Procedures. Refer to the above Procedures section and Section IV of this report for the Company's relevant control activities. Although the trust services criteria and related controls are presented in Section IV, they are an integral part of Akumina's system description.

TRUST SERVICES CRITERIA NOT APPLICABLE TO THE IN-SCOPE SYSTEM

All of the underlying Trust Services Criteria related to security, availability and confidentiality are applicable to the System.

INCIDENTS DURING THE EXAMINATION PERIOD

Akumina identified no system incidents that were the result of controls that were not suitably designed or operating effectively or that resulted in a significant failure in the achievement of one or more service commitments and system requirements during the examination period covered by management's description.

SIGNIFICANT CHANGES DURING THE EXAMINATION PERIOD

There were no significant changes to Akumina's systems or control environment during the examination period.

MONITORING OF THE SUBSERVICE ORGANIZATION

Akumina utilizes the services of Microsoft Azure (Azure), a subservice organization, to provide authentication services and third-party hosting of its production infrastructure. Akumina obtains and reviews copies of independent third-party reports of the controls in place at Azure and other third-party service providers that meet certain risk criteria at least annually in order to validate they are in line with Akumina's expectations and requirements. Akumina reviews the reports to ensure controls around security, availability and confidentiality are in place and operating. Additionally, Akumina adheres to complementary user entity controls required by the subservice organization.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

Akumina's controls related to the Employee Experience Platform cover only a portion of overall internal control for each client of Akumina. Certain service commitments and system requirements can only be achieved if the subservice organization's controls contemplated in the design of Akumina's controls are suitably designed and operating effectively along with the related controls at Akumina. Therefore, each client's internal control must be evaluated in conjunction with Akumina's controls and the related tests and results described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at Azure as described below.

Ref #	Complementary Subservice Organization Controls	Related Trust Services Criteria
1.	The subservice organization is responsible for implementing monitoring controls to ensure perimeter network alerts are evaluated, communicated, and corrected, as appropriate. The subservice organization is responsible for implementing monitoring controls to ensure anti-virus alerts are evaluated, communicated, and corrected, as appropriate.	CC4.1 CC6.6 CC7.2 CC7.4
2.	The subservice organization is responsible for managing logical access to the underlying network and storage devices for its cloud hosting services where the Akumina platform resides.	CC6.1 CC6.2 CC6.3

Ref #	Complementary Subservice Organization Controls	Related Trust Services Criteria
3.	The subservice organization is responsible for implementing physical security controls to restrict access to the sensitive system components to authorized personnel.	CC6.4
4.	The subservice organization is responsible for implementing controls for data wiping, destroying, and disposing of assets in their environment that are no longer required or have reached end of life.	CC6.5
5.	The subservice organization is responsible for deploying security patches to assets in the environment and monitoring for unauthorized or malicious software.	CC6.8 CC7.2 CC8.1
6.	The subservice organization is responsible for monitoring its environment to maintain security, availability and confidentiality, including having an incident handling process.	CC7.3
7.	The subservice organization is responsible for developing and implementing a change control process that requires formal request, documentation, testing, approval, and implementation.	CC8.1
8.	The subservice organization is responsible for developing, implementing, maintaining, and monitoring environmental protections of the assets hosted in the environment.	A1.2
9.	The subservice organization is responsible for implementing and testing recovery plan procedures to meet availability objectives.	A1.3

COMPLEMENTARY USER ENTITY CONTROLS

The Company's description and its described controls in Section IV are designed to achieve Akumina's service commitments and system requirements based on the applicable trust services criteria with the assumption that certain controls would be implemented by user entities. This section describes some of the controls that should be in operation to complement the controls at the Company. User entities and their auditors should determine whether user entities have established controls to provide assurance that:

- User entities should review and respond, as appropriate, to any notices provided by Akumina particularly any system changes impacting the security, availability, or confidentiality of content data through the Akumina platform (CC3.1 and CC8.1);
- User entities should ensure sound password security practices are implemented to ensure that access to content data through the Akumina platform is restricted to authorized users (CC6.1);
- User entities should ensure that only authorized users are granted access to content data through the Akumina platform, and should periodically review access granted to ensure that it remains appropriate to users' respective job functions (CC6.1 and CC6.2);
- User entities should ensure that the credentials provided to access the information resources for use with Akumina's platform are restricted to only the minimum access needed (CC6.1 and CC6.2); and
- User entities should ensure that the credentials used to access the information resources for use with Akumina's platform are subject to rotation based on each user entity's evaluation of relative risk (CC6.2 and CC6.3).

SECTION IV

APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS AND INDEPENDENT SERVICE AUDITORS' DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

INTRODUCTION

Akumina Inc. (Akumina) can achieve its service commitments and system requirements based on the applicable trust services criteria, within the overall internal control structure surrounding its Employee Experience Platform (the Akumina platform), if Akumina's subservice organization and user entities implement strong internal controls. Application of internal controls is necessary to meet many of the applicable trust services criteria listed in this report. Therefore, it is critical to evaluate each user entity's internal control structure in conjunction with Akumina's internal control structure as described in this report.

Category	**Definition**
Security	Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.
Availability	Information and systems are available for operation and use to meet the entity's objectives.
Confidentiality	Information designated as confidential is protected to meet the entity's objectives.

This section includes a description of the internal controls placed in operation by Akumina and the tests we performed to evaluate their effectiveness.

Test Procedure	**Description of Testing Performed**
Inquiries	Interviewed the applicable control owner about the relevant control descriptions and corresponding processes and procedures described within the system description.
Observation	Observed the performance of controls by Akumina personnel including, among other things, viewing the functionality of applications and automated controls and observing interactions with clients.
Inspection	Examined documents and reports that contain an indication of performance of the controls. This includes, among other things, reading of policy and procedure documents and management reports to assess whether processing activities are properly monitored and controlled and any problems or issues are resolved on a timely basis.

Inquiries were performed for all controls to both acquire an understanding of the controls and assess their application. Other test procedures were also performed as documented in this section.

For all controls and related trust services criteria documented in this section, no relevant exceptions were noted during the testwork performed, unless otherwise indicated.

Information Provided by Entity (IPE) Validation

For tests of controls requiring the use of IPE, we performed a combination of the following procedures, as applicable, based on the nature of the IPE to address the completeness, accuracy and data integrity of the data or reports used: (1) observed the generation of the IPE, (2) inspected the query, script, or parameters used to generate the IPE, and/or (3) inspected the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity. In addition to the above procedures, for tests of controls requiring management's use of IPE in the execution of the controls (e.g., periodic reviews of user access listings), as applicable, based on the nature of the IPE, we inspected management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

AKUMINA INC.

APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS AND
INDEPENDENT SERVICE AUDITORS' DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

For the Period March 16, 2022 through March 15, 2023

TRUST SERVICES CRITERIA FOR THE SECURITY, AVAILABILITY, AND CONFIDENTIALITY CATEGORIES MAPPED TO AKUMINA INC.'S CONTROLS

Controls that did not operate or partially did not operate during the period are noted with an "*". See further details at section "Akumina Inc.'s Control Descriptions and Service Auditors' Tests of Controls and Results" below.

CRITERIA	DESCRIPTION OF THE COMMON CRITERIA	SUPPORTING CONTROL ACTIVITY AT AKUMINA
CC1.0 Common Criteria Related to the Control Environment		
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	1, 2, 3, 4, 5, 6
CC1.2	The Board of Directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	7
CC1.3	Management establishes, with Board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	8, 9, 10, 11, 12
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	6, 13, 14, 15, 16, 18, 21
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	3, 4, 5, 12, 13, 14, 16, 37
CC2.0 Common Criteria Related to Communication and Information		
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	26, 28, 29*, 30, 31, 56*, 58
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	2, 9, 17, 18, 19, 20, 21
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	1, 23, 24, 25
CC3.0 Common Criteria Related to Risk Assessment		
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	26, 27, 28,
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	10, 26, 28, 29*, 67
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	28
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	28, 30, 31
CC4.0 Common Criteria Related to Monitoring Activities		
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	26, 28, 29*, 31
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the Board of Directors, as appropriate.	28, 29*, 31, 32

AKUMINA INC.

APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS AND
INDEPENDENT SERVICE AUDITORS' DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

For the Period March 16, 2022 through March 15, 2023

CRITERIA	DESCRIPTION OF THE COMMON CRITERIA	SUPPORTING CONTROL ACTIVITY AT AKUMINA
CC 5.0 Common Criteria Related to Control Activities		
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	28, 33, 34, 62
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	28, 35
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	19, 35, 36, 37, 38
CC6.0 Common Criteria Related to Logical and Physical Access Controls		
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	29*, 33, 39, 40, 41, 42, 43, 44, 45, 46, 65, 75, 76, 77
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	46, 47, 48
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	40, 46, 47, 49
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	50, 51, 78, 79
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	52*, 62
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	41, 45, 54
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	41, 53, 80
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	29*, 54, 55, 56*, 57, 58, 64, 65, 66*
CC 7.0 Common Criteria Related to System Operations		
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	29*, 56*, 58

CRITERIA	DESCRIPTION OF THE COMMON CRITERIA	SUPPORTING CONTROL ACTIVITY AT AKUMINA
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	20, 22, 24, 29*, 43, 56*, 59
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	22, 32, 60*, 61*
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	22, 32, 60*, 61*
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	61*, 62, 63*
CC 8.0 Common Criteria Related to Change Management		
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	62, 64, 65, 66*
CC 9.0 Common Criteria Related to Risk Mitigation		
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	67, 73
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	1, 11, 28, 50, 68, 69

CRITERIA	ADDITIONAL CRITERIA RELEVANT TO AVAILABILITY AND CONFIDENTIALITY	SUPPORTING CONTROL ACTIVITY AT AKUMINA
Additional Criteria for Availability		
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	31, 70
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	50, 71, 72
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	73, 74
Additional Criteria for Confidentiality		
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	39, 44, 52*, 53, 68
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	52*

AKUMINA INC.

APPLICABLE TRUST SERVICES CRITERIA, RELATED CONTROLS AND
INDEPENDENT SERVICE AUDITORS' DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

For the Period March 16, 2022 through March 15, 2023

AKUMINA INC.'S CONTROL DESCRIPTIONS AND SERVICE AUDITORS' TESTS OF CONTROLS AND RESULTS

Controls that did not operate or partially did not operate during the period are noted with an "*".

CONTROL	CONTROLS SPECIFIED BY AKUMINA	TESTS PERFORMED BY THE SERVICE AUDITOR	RELEVANT CRITERIA
1	Agreements are established through contracts with service providers and business partners that include clearly defined terms, conditions, and responsibilities for service providers and business partners which outline conduct guidelines.	For a sample of service providers or business partners selected from the vendor risk analysis, inspected the corresponding contract to confirm that it includes clearly defined terms, conditions, and responsibilities for service providers and business partners which outline conduct guidelines.	CC1.1 CC2.3 CC9.2
2	Akumina has a documented code of business conduct and ethical standards which are reviewed, updated as necessary, and approved by senior management annually.	Inspected the code of business conduct and ethical standards to confirm it contains information about Akumina's expectations for business conduct and ethical standards for employees. Inspected the code of business conduct and ethical standards to confirm it was reviewed, updated as necessary, and approved by senior management in the past year.	CC1.1 CC2.2
3	Employees are required to acknowledge a non-competition, non-solicitation, confidentiality and proprietary rights agreement upon their hire.	For a sample of new employees selected from the human resources (HR) system, inspected their acknowledgement of a non-competition, non-solicitation, confidentiality and proprietary rights agreement to confirm it was signed upon their hire.	CC1.1 CC1.5

CONTROL	CONTROLS SPECIFIED BY AKUMINA	TESTS PERFORMED BY THE SERVICE AUDITOR	RELEVANT CRITERIA
4	Employees are required to read and acknowledge the Employee Handbook and workforce conduct standards upon their hire and upon annual distribution of the policies.	For a sample of new employees selected from the HR system, inspected their acknowledgement of the Employee Handbook and workforce conduct standards to confirm it was signed upon their hire. For a sample of active employees selected from the HR system, inspected their acknowledgement of the Employee Handbook and workforce conduct standards to confirm it was signed within the past year.	CC1.1 CC1.5
5	Management monitors personnel compliance with the code of business conduct and ethical standards through annual reviews of employees and monitoring of customer and workforce member complaints.	For a sample of active employees selected from the HR system, inspected their most recent annual review to confirm it was completed as expected and their compliance with the code of business conduct and ethical standards was monitored. Observed the monitoring of customer and workforce member complaints.	CC1.1 CC1.5
6	The hiring process includes background checks for all candidates. Prior to employment, personnel are verified against regulatory screening databases, including at a minimum, criminal and employment checks.	For a sample of new hires selected from the HR system, inspected the results of their background check to confirm that, prior to employment, the new hire was verified against regulatory screening databases, including at a minimum, criminal and employment checks.	CC1.1 CC1.4

CONTROL	CONTROLS SPECIFIED BY AKUMINA	TESTS PERFORMED BY THE SERVICE AUDITOR	RELEVANT CRITERIA
7	The Board of Directors is responsible for overseeing the Executive Management Team and exercises oversight of the development and performance of internal control. The Board of Directors is independent of management and meets at least on a quarterly basis.	Inspected the composition of the Board of Directors to confirm that it comprises directors independent from management. For a sample of quarters, inspected the meeting minutes to confirm that the Board of Directors met as expected.	CC1.2
8	Akumina has defined organizational structures, reporting lines, authorities and responsibilities which are documented in its organizational chart.	Inspected the Akumina organizational chart to confirm that the chart documents organizational structure, reporting lines, authorities and responsibilities	CC1.3
9	Akumina maintains written job descriptions, which include roles and responsibilities and are updated as necessary based on changing job responsibilities, commitments and system requirements.	For a sample of active positions selected from the organizational chart, inspected the job description to confirm it exists and documents relevant roles and responsibilities of the position.	CC1.3 CC2.2
10	Akumina management and the Board of Directors evaluate its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process and revise these when necessary to support the achievement of objectives.	Inspected the most recent risk assessment performed to confirm that Akumina management and the Board of Directors evaluated the Company's organizational structure, reporting lines, authorities and responsibilities.	CC1.3 CC3.2
11	Akumina's organizational structure includes roles and responsibilities for interacting with and monitoring subservice organizations and vendors.	Inspected the job descriptions for the roles that have responsibilities for interacting with external parties to confirm the responsibilities are documented.	CC1.3 CC9.2

CONTROL	CONTROLS SPECIFIED BY AKUMINA	TESTS PERFORMED BY THE SERVICE AUDITOR	RELEVANT CRITERIA
12	The HR Team is responsible for ensuring staff understand and fulfill their responsibilities as defined in job descriptions and operational policy and procedure documents to meet the organization's commitments and system requirements.	Inspected the various policies and procedures provided to employees to confirm that they contain the necessary information for the employees to understand and fulfill their responsibilities to meet the organization's commitments and system requirements.	CC1.3 CC1.5
13	Akumina management performs annual performance evaluations to communicate and hold individuals accountable for performance of internal control responsibilities. The performance evaluation is signed by the manager and employee. Corrective actions, including training or sanctions, are taken as necessary.	For a sample of active employees selected from the HR system, inspected their most recent annual review to confirm it was completed as expected and signed by the employee and their manager.	CC1.4 CC1.5
14	Management establishes requisite skillsets for personnel, whether an employee or contractor, and provides continued training about its commitments and requirements for personnel to support the achievement of objectives. Management monitors compliance with training requirements.	Inspected the training provided to employees to confirm that it provides information about Akumina's commitments and requirements for personnel to support the achievement of objectives Observed the training console to confirm that management is monitoring compliance with training requirements.	CC1.4 CC1.5
15	The qualifications and skills of candidates are assessed by management as part of the hiring process through interviews and review of each candidate's resume.	For a sample of new hires selected from the HR system, inspected the assessment of each candidate by management to confirm the qualifications and skills of the candidates were assessed.	CC1.4
16	The Executive Management Team and HR Team are responsible and accountable for designing, developing, implementing, operating, maintaining, monitoring and approving system controls and other risk mitigation strategies and ensuring staff are trained and policies are implemented and being followed.	Inspected the various policies and procedures provided to employees to confirm that they contain the necessary information for the employees to understand and fulfill their responsibilities to meet the organization's commitments and system requirements.	CC1.4 CC1.5

CONTROL	CONTROLS SPECIFIED BY AKUMINA	TESTS PERFORMED BY THE SERVICE AUDITOR	RELEVANT CRITERIA
17	Akumina posts a description of its system, system boundaries and system processes that includes infrastructure, software, people, processes and procedures and data on its intranet for internal users.	Observed the Akumina intranet to confirm that a description of the system, system boundaries and system processes that includes infrastructure, software, people, processes and procedures and data was posted for internal users.	CC2.2
18	Akumina's commitments and system requirements are communicated to internal users as part of the annual training and are available on its intranet.	Observed the content of the annual training and the Akumina intranet to confirm that Akumina's commitments and system requirements have been communicated to internal users.	CC1.4 CC2.2
19	Information necessary for designing, developing, implementing, operating, maintaining and monitoring controls, relevant to the security, confidentiality, and availability of the system, is provided to personnel via policies and procedures to carry out their responsibilities.	Inspected the various policies and procedures to confirm that they provided employees with information necessary for designing, developing, implementing, operating, maintaining and monitoring controls, relevant to the security, availability, and confidentiality to carry out their responsibilities.	CC2.2 CC5.3
20	Internal users have been provided with information on how to report security failures, incidents, concerns and other complaints to appropriate personnel.	Inspected the procedures in place to confirm they have been provided to internal users and contain information about how to report security failures, incidents, concerns and other complaints to appropriate personnel.	CC2.2 CC7.2

CONTROL	CONTROLS SPECIFIED BY AKUMINA	TESTS PERFORMED BY THE SERVICE AUDITOR	RELEVANT CRITERIA
21	Management provides continued training about its security, confidentiality, and availability commitments and requirements for personnel to support the achievement of objectives and monitors compliance with training requirements. Akumina also provides user guides, security alerts and known issues on the Company's intranet to improve security knowledge and awareness.	Observed the content of the annual training and the Akumina intranet to confirm that Akumina's commitments and system requirements have been communicated to internal users. Observed the Akumina intranet to confirm that user guides, security alerts and known issues have been posted to improve security knowledge and awareness. For a sample of active employees selected from the HR system, inspected the training console to confirm that they completed the annual security awareness training.	CC1.4 CC2.2
22	Akumina has incident response policies and procedures in place that document the response process including identification, containment, mitigation and recovery, and follow-up and documentation.	Inspected Akumina's incident response policies and procedures to confirm that they contain information relating to the incident response process, including identification, containment, mitigation and recovery, and follow-up and documentation.	CC7.2 CC7.3 CC7.4
23	Akumina posts a description of its system, system boundaries, and system processes that includes infrastructure, software, people, processes and procedures, and data on the Company website for external users.	Observed the Akumina website to confirm that a description of the system, system boundaries and system processes that includes infrastructure, software, people, processes and procedures and data was posted for external users.	CC2.3

CONTROL	CONTROLS SPECIFIED BY AKUMINA	TESTS PERFORMED BY THE SERVICE AUDITOR	RELEVANT CRITERIA
24	Customers can submit cases and trouble reports ("support tickets") to Akumina through email or through the Akumina platform. The Master Services Agreement defines the required timeframes for response based on the assigned priority level.	Observed the process by which customers can submit cases or support tickets to Akumina via email or the website. Inspected the Master Services Agreement to confirm it defines timeframes for response based on assigned priority level.	CC2.3 CC7.2
25	The responsibilities of Akumina and customers are defined in a Master Services Agreement.	For a sample of customers selected from the customer relationship system, inspected the Master Services Agreement to confirm it contains information about the responsibilities of Akumina and the customer.	CC2.3
26	Akumina has established procedures to assess risks and conducts a risk assessment at least annually. The risk assessment is based on the objectives established by management under the oversight of the Board of Directors and identifies key information system processes that process relevant data into information to support the internal control and the achievement of Akumina's service commitments and system requirements.	Inspected the most recent risk assessment performed to confirm that it is based on the objectives established by management under the oversight of the Board of Directors and identifies key information system processes that process relevant data into information to support the internal control and the achievement of Akumina's service commitments and system requirements and was performed within the last year.	CC2.1 CC3.1 CC3.2 CC4.1
27	The Risk Assessment Policy details the process for identifying potential threats, assessing the likelihood, and assessing the impact.	Inspected the Risk Assessment Policy to confirm it contains information about process for identifying potential threats, assessing the likelihood, and assessing the impact.	CC3.1

CONTROL	CONTROLS SPECIFIED BY AKUMINA	TESTS PERFORMED BY THE SERVICE AUDITOR	RELEVANT CRITERIA
28	Akumina has established procedures to assess risks and conducts a risk assessment at least annually. As part of the risk assessment, Akumina identifies risks arising from external and internal sources and those findings are shared with management. In addition, the risk assessment includes: • Evaluating the effect of environmental, regulatory and technological changes on Akumina's system security • Involving appropriate levels of management • Analyzing risks associated with the threats • Identifying threats to operations, including security threats, using information technology asset records • Identifying threats to operations, including threats from vendors, business partners and other parties • Determining a risk mitigation strategy • Considering the potential for fraud in assessing risks to the achievement of objectives.	Inspected the most recent risk assessment performed to confirm that Akumina identified risks arising from external and internal sources and that it was performed within the past year.	CC2.1 CC3.1 CC3.2 CC3.3 CC3.4 CC4.1 CC4.2 CC5.1 CC5.2 CC9.2
29*	Akumina has vulnerability and penetration tests performed by a third party at least annually reporting to the Development and Engineering Team. A remediation plan is developed by the Development and Engineering Team and changes are implemented to remediate all critical and high vulnerabilities at a minimum.	Inspected the most recent vulnerability and penetration testing to confirm it was completed within the past year. *NOTE: Baker Newman & Noyes LLC (BNN) confirmed through inspection of the results of the vulnerability and penetration testing that there were no critical or high priority vulnerabilities found; as such, we were unable to test the remediation of findings.*	CC2.1 CC3.2 CC4.1 CC4.2 CC6.1 CC6.8 CC7.1 CC7.2

CONTROL	CONTROLS SPECIFIED BY AKUMINA	TESTS PERFORMED BY THE SERVICE AUDITOR	RELEVANT CRITERIA
30	Management subscribes to threat intelligence resources covering cybersecurity and risks present in the external environment.	Observed the subscriptions to threat intelligence resources covering cybersecurity and risks present in the external environment.	CC2.1 CC3.4
31	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity. Any unusual activity or items that need to be addressed are communicated to the IT and Development and Engineering Teams who are responsible for overseeing remediation, as necessary.	Observed the use of monitoring software to confirm it is utilized to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity Observed that any unusual activity or items that need to be addressed are communicated to the IT and Development and Engineering Teams who are responsible for overseeing remediation, as necessary.	CC2.1 CC3.4 CC4.1 CC4.2 A1.1
32	Akumina has established an incident response plan which includes communicating all security events to the Management Team.	Inspected the incident response plan to confirm the process includes the communication of all security events to the Management Team.	CC4.2 CC7.3 CC7.4
33	Akumina has designed application-enforced segregation of duties to define what privileges are assigned to users within applications.	Observed the application-enforced segregation of duties to confirm that it defines what privileges are assigned to users within applications.	CC5.1 CC6.1
34	Akumina has established policies and procedures designed for the mitigation of risk which include a mix of manual, automated, preventive and detective controls. These policies are reviewed and updated by the Executive Management Team at least annually.	Inspected the various policies and procedures provided to employees to confirm that they are designed for the mitigation of risk which include a mix of manual, automated, preventive and detective controls. Inspected the various policies and procedures provided to employees to confirm that they were reviewed and updated within the past year.	CC5.1

CONTROL	CONTROLS SPECIFIED BY AKUMINA	TESTS PERFORMED BY THE SERVICE AUDITOR	RELEVANT CRITERIA
35	Akumina has developed policies and procedures to manage the technology infrastructure. The Executive Management Team reviews and updates these policies at least annually.	Inspected the various policies and procedures provided to employees to confirm that they contain information relating to the technology infrastructure. Inspected the various policies and procedures provided to employees to confirm that they were reviewed and updated within the past year.	CC5.2 CC5.3
36	Akumina has established policies and procedures which address controls over significant aspects of its operations. These policies and procedures are available to relevant personnel on the Company's intranet. The policies and procedures are reviewed and updated by the Executive Management Team at least annually.	Inspected the various policies and procedures provided to employees to confirm that they address controls over significant aspects of its operations. Inspected the various policies and procedures provided to employees to confirm that they were reviewed and updated within the past year.	CC5.3
37	Akumina has written job descriptions specifying the responsibilities and the academic and professional requirements for key job positions. The HR Team screens internal and external job applicant qualifications based on the defined requirements within the job description.	For a sample of active positions selected from the organizational chart, inspected the job description to confirm it exists and documents the roles and responsibilities of the position, including the academic and professional requirements. For a sample of new hires selected from the HR system, inspected the assessment of each candidate by management to confirm the qualifications and skills of the candidates were assessed based on the defined requirements within the job description.	CC1.5 CC5.3

CONTROL	CONTROLS SPECIFIED BY AKUMINA	TESTS PERFORMED BY THE SERVICE AUDITOR	RELEVANT CRITERIA
38	The Governance Committee is charged with establishing, maintaining and enforcing the overall security policies and procedures.	Inspected the monthly Governance Committee meeting invitations to confirm that the Committee meets on a regular basis to discuss the establishing, maintaining and enforcing the overall security policies and procedures.	CC5.3
39	A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the data classification policy to confirm that it contains information to help ensure that confidential data is properly secured and restricted to authorized personnel.	CC6.1 C1.1
40	Akumina establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles.	Observed the use of role-based permission to confirm that Akumina establishes and administers privileged user accounts and organizes information system and network privileges into roles.	CC6.1 CC6.3
41	Akumina has established logical access controls and software for the identification and authorization of users, restriction of access to authorized users, and the prevention and detection of unauthorized access to the systems and infrastructure. These include limiting access to role-based permissions, and virtual private networks (VPNs) using multi-factor authentication (MFA).	Observed the use of role-based permissions, MFA and VPNs to confirm that Akumina has established logical access controls and software for the identification and authorization of users, restriction of access to authorized users, and the prevention and detection of unauthorized access to the systems and infrastructure.	CC6.1 CC6.6 CC6.7
42	Akumina has established procedures to identify and authenticate users including unique user IDs and complex passwords. Users are required to supply their credentials in order to access servers and systems.	Observed the use of unique user IDs and complex passwords to confirm that they are utilized to identify and authenticate users.	CC6.1
43	Akumina monitors all system components through an automated management interface to log, track and maintain all inventory components.	Observed the automated management interface to confirm that Akumina is using the interface to log, track and maintain all inventory components.	CC6.1 CC7.2

CONTROL	CONTROLS SPECIFIED BY AKUMINA	TESTS PERFORMED BY THE SERVICE AUDITOR	RELEVANT CRITERIA
44	Databases housing sensitive customer data are encrypted at rest.	Observed that databases housing sensitive customer data are encrypted at rest.	CC6.1 C1.1
45	Firewalls and monitoring systems have been deployed to protect and identify threats to the system. Access to modify firewall configuration settings is restricted to authorized IT personnel.	Observed the firewall console and rulesets to confirm that the firewall has been configured to protect and identify threats to the system. Observed the firewall console to confirm that only authorized IT personnel have access to modify the firewall configuration settings.	CC6.1 CC6.6
46	Management performs an annual access review for the Akumina platform to ensure that access is restricted appropriately.	Inspected the most recent access review performed and confirmed that access is restricted appropriately.	CC6.1 CC6.2 CC6.3
47	A termination checklist is completed and access is revoked for employees or contractors (unless otherwise specified in vendor management process and contract) as part of the termination process.	For a sample of terminated employees or contractors selected from the HR system, inspected the termination checklist to confirm it was completed and access was revoked in a timely manner.	CC6.2 CC6.3
48	A ticket must be completed and approved by the hiring manager to request system access for a new hire or contractor. The ticket is submitted which creates a help desk ticket to log the completion of access requests.	For a sample of new employees or contractors selected from the HR system, inspected the new hire ticket to confirm it was completed and approved by the hiring manager. Inspected Akumina's User Provisioning policy to confirm it contains procedures for access provisioning, changes, and termination.	CC6.2
49	Requests for changes in access rights follow the same process as granting and removing access, with the exception that requests can be initiated by staff or manager.	For a sample of position changes selected from the HR system, inspected the request for the change in access to confirm that it was completed and approved by the appropriate individuals.	CC6.3

CONTROL	CONTROLS SPECIFIED BY AKUMINA	TESTS PERFORMED BY THE SERVICE AUDITOR	RELEVANT CRITERIA
50	The Governance Committee obtains and reviews a copy of the subservice organization's SOC report at least annually in order to validate it is in line with Akumina's expectations and requirements. Akumina reviews the report to ensure controls around security, availability and confidentiality are in place and operating. Additionally, Akumina evaluates and ensures adherence to complementary user entity controls required by the subservice organization.	Inspected the most recent review of Akumina's subservice organization SOC report and the results of management's review of the SOC report, including evaluation of the complementary user entity controls.	CC6.4 CC9.2 A1.2
51	Akumina hosts its system infrastructure, software and data within Microsoft's Azure cloud platform, and Microsoft, the subservice organization, is responsible for physical access controls at its facilities.	Inspected the Microsoft Azure SOC report to confirm that it contains controls relating to the physical access controls at its facilities.	CC6.4
52*	Formal data retention and disposal procedures are in place to guide the secure disposal of customer data.	Inspected the data retention and disposal policies to confirm they contain information to guide the secure disposal of customer data. *NOTE: BNN confirmed through corroborative inquiry that there were no devices disposed of during the examination period and as such, we were unable to test the secure disposal of customer data.*	CC6.5 C1.1 C1.2
53	Access to all information is restricted to authorized users and processes through identification and authentication of users and role based access.	Observed the use of role-based access to confirm that access to all information is restricted to authorized users and processes through identification and authentication of users	CC6.7 C1.1

CONTROL	CONTROLS SPECIFIED BY AKUMINA	TESTS PERFORMED BY THE SERVICE AUDITOR	RELEVANT CRITERIA
54	Akumina has established security procedures to identify and prevent threats which include use of firewalls, anti-virus software and the use of monitoring systems.	Observed the use of firewalls, anti-virus software, and monitoring systems.	CC6.6 CC6.8
55	Anti-virus technology is deployed for environments commonly susceptible to malicious attack. This software is used to scan assets prior to being placed into production.	Inspected the anti-virus console to confirm that anti-virus technology is deployed for environments commonly susceptible to malicious attack. For a sample of assets selected from the device listing, confirmed that anti-virus software is installed on the device.	CC6.8
56*	Monitoring systems provide monitoring and notification to the IT and Development and Engineering Teams. Intrusion attempts are logged, tracked, and communicated to affected parties until resolved.	Observed the use of monitoring systems. *NOTE: BNN confirmed through inspection of the incident logging that there were no incidents noted; as such, we were unable to test the logging, tracking and communication of intrusion attempts.*	CC2.1 CC6.8 CC7.1 CC7.2
57	Only authorized system administrators are able to install software on system devices. Unauthorized use or installation of software is explicitly covered in the Employee Handbook and workforce conduct standards.	Observed a non-system administrator attempt to install software to confirm that only authorized system administrators are able to install software. Inspected the Employee Handbook and workforce conduct standards to confirm it contains language about the unauthorized use or installation of software.	CC6.8
58	Akumina utilizes monitoring tools to alert the IT and Development and Engineering Teams of any unauthorized modifications to the systems.	Observed the use of monitoring tools to confirm they are configured to alert of any unauthorized modifications to the systems.	CC2.1 CC6.8 CC7.1

CONTROL	CONTROLS SPECIFIED BY AKUMINA	TESTS PERFORMED BY THE SERVICE AUDITOR	RELEVANT CRITERIA
59	System security event logs are centralized and are monitored weekly by the respective IT and Development and Engineering Teams' delegate. Issues are handled in accordance with the change management process.	For a sample of weeks, inspected the weekly events report to confirm it was generated, reviewed and any issues were remediated.	CC7.2
60*	A technician or administrator responsible for security incident tickets follows a process of analyzing the security incident. The process begins with detailing what specific attack occurred, which system(s) were affected and what happened during the attack. Next, the root cause is determined, and the event is given a classification to assign the level of impact of the event. The impact level is based on guidelines detailed in the incident response procedures.	*NOTE: BNN confirmed through inspection of the incident logging that there were no incidents noted; as such, we were unable to test that the incident process was followed to analyze the security incident.*	CC7.3 CC7.4
61*	Akumina has developed security incident response policies and procedures that are communicated to authorized users. All incidents related to the security of the system are logged and tracked by management until resolved.	Inspected Akumina's incident response policies to confirm that they contain information about how to respond to an incident and confirm that the policies are communicated to Akumina users. *NOTE: BNN confirmed through inspection of the incident logging that there were no incidents noted; as such, we were unable to test the logging and tracking incidents.*	CC7.3 CC7.4 CC7.5
62	Akumina has a formalized security and systems development methodology that includes project planning, design, testing, implementation, maintenance and disposal or decommissioning.	Inspected the systems development methodology to confirm it includes processes relating to project planning, design, testing, implementation, maintenance and disposal or decommissioning.	CC5.1 CC6.5 CC7.5 CC8.1

CONTROL	CONTROLS SPECIFIED BY AKUMINA	TESTS PERFORMED BY THE SERVICE AUDITOR	RELEVANT CRITERIA
63*	An assessment of the incident response to better handle future incidents is performed through analysis after action reports or the mitigation of exploited vulnerabilities to prevent similar incidents in the future.	*NOTE: BNN confirmed through inspection of the incident logging that there were no incidents noted; as such, we were unable to test that an assessment of the incident response was performed.*	CC7.5
64	Akumina has an established change management process which includes authorization, design, development, configuration, documentation, testing, approval, and implementation in accordance with commitments and system requirements.	Inspected the change management process to confirm it includes processes relating to authorization, design, development, configuration, documentation, testing, approval, and implementation of changes in accordance with commitments and system requirements.	CC6.8 CC8.1
65	Changes to system infrastructure and software are developed and tested in a separate development or test environment before implementation. Additionally, developers do not have the ability to migrate changes into production environments without first obtaining the requisite approvals for the changes.	For a sample of changes selected from a system-generated listing of changes to production, inspected the change ticket to confirm the changes were developed and tested in a separate development or test environment before implementation. For a sample of changes selected from a system-generated listing of changes to production, inspected the change ticket to confirm that approval was obtained prior to the migration of the changes into the production environments.	CC6.1 CC6.8 CC8.1

CONTROL	CONTROLS SPECIFIED BY AKUMINA	TESTS PERFORMED BY THE SERVICE AUDITOR	RELEVANT CRITERIA
66*	Emergency changes follow the standard change management process but at an accelerated timeline. Prior to initiating an emergency change, all necessary approvals are obtained and documented.	*NOTE: BNN confirmed through inspection of a system-generated listing of changes to production that there were no changes deemed to be emergency changes; as such, we were unable to test the procedure for emergency changes.*	CC6.8 CC8.1
67	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. A risk assessment is performed on at least an annual basis. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments, policies, and procedures are identified and the risks are formally assessed. The risk management program includes the use of insurance to minimize the financial impact of any loss events.	Inspected the most recent risk assessment performed to confirm that it contained the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks and was performed within the past year. Inspected Akumina's insurance policy to confirm it includes the use of cyber insurance to minimize the financial impact of any loss events.	CC3.2 CC9.1
68	A vendor risk assessment is performed at the initial contract phase for all vendors that have access to confidential data or impact the security, availability or confidentiality of the system and on an annual basis thereafter.	For a sample of new vendors during the examination period selected from the vendor risk analysis, inspected the risk assessment activities performed during the initial contract phase to confirm that Akumina assessed the vendor as expected. Inspected the vendor risk assessment performed by Akumina to confirm that all vendors that have access to confidential data or impact the security, availability or confidentiality of the system were evaluated, as expected.	CC9.2 C1.1

CONTROL	CONTROLS SPECIFIED BY AKUMINA	TESTS PERFORMED BY THE SERVICE AUDITOR	RELEVANT CRITERIA
69	Formal information sharing agreements are in place with related parties and vendors. These agreements include the scope of services and security and confidentiality commitments applicable to that entity.	For a sample of vendors selected from the vendor risk analysis, inspected the agreements in place to confirm they include the scope of services and security and confidentiality commitments applicable to that entity.	CC9.2
70	Akumina has configured settings within Azure to monitor capacity metrics for the production network including disk usage, memory usage, processor load, and server downtime/ uptime. An alert is generated to members of infrastructure operations when defined performance metrics are exceeded. Alerts are researched and remediation steps are taken as necessary.	Observed the settings within Azure to confirm that settings are in place to monitor capacity metrics for the production network including disk usage, memory usage, processor load, and server downtime/ uptime. Observed a sample alert generated to confirm that it was generated in accordance with defined performance metrics and sent to members of infrastructure operations for investigation and resolution.	A1.1
71	Database logging technology is utilized to continually replicate all data and transmit the data to offsite identical databases for retention and disaster recovery purposes.	Inspected the management console for the replication of data settings in their live state to confirm that database logging technology is utilized to continually replicate all data and transmit the data to offsite identical databases for retention and disaster recovery purposes.	A1.2
72	The system infrastructure, software and data are hosted in Microsoft's Azure cloud platform with business continuity/disaster recovery processes created and managed by the IT Team.	Inspected the business continuity/disaster recovery processes created and managed by the IT Team to confirm that they exist to aid in the recovery of system infrastructure.	A1.2

CONTROL	CONTROLS SPECIFIED BY AKUMINA	TESTS PERFORMED BY THE SERVICE AUDITOR	RELEVANT CRITERIA
73	The Disaster Recovery Plan addresses recovering connectivity and supporting systems to ensure service commitments and system requirements can be met.	Inspected the Disaster Recovery Plan to confirm it addresses recovering connectivity and supporting systems to ensure service commitments and system requirements can be met.	CC9.1 A1.3
74	The Disaster Recovery Plan is tested by Akumina on an annual basis.	Inspected the results of the most recent Disaster Recovery Plan testing to confirm that it was completed within the past year.	A1.3
75	Akumina ensures that only authorized devices connect to the Akumina platform by utilizing IP address monitoring.	Observed the use of IP address monitoring to confirm it is utilized to ensure that only authorized devices connect to the Akumina platform.	CC6.1
76	Akumina logs access to information assets to ensure that an audit trail is available if there are any issues or noted unauthorized access.	Observed the logging of access to information assets to confirm that an audit trail is available for review if needed.	CC6.1
77	Where possible, Akumina utilizes a just-in-time access process to ensure only authorized users are able to access the system.	Observed the use of the just-in-time access process to confirm that it is utilized to ensure only authorized users are able to access the system.	CC6.1
78	Access to the server room is restricted to appropriate individuals and is controlled by a physical key.	Inspected the physical key listing of access to the server room to confirm that access is restricted to appropriate individuals. Observed the locked server room door to confirm that access is controlled by a physical key.	CC6.4

CONTROL	CONTROLS SPECIFIED BY AKUMINA	TESTS PERFORMED BY THE SERVICE AUDITOR	RELEVANT CRITERIA
79	Akumina utilizes a proximity card system to control access to the Company facility.	Inspected the proximity card access listing against the active employee list to confirm that access is controlled and restricted to authorized individuals. Observed the use of a proximity card to gain access to the Company facility to confirm access is controlled.	CC6.4
80	Akumina utilizes secure email for transmission of sensitive information.	Observed the use of secure email to confirm it is used for the transmission of sensitive information.	CC6.7