ARC Document Solutions, Inc

Independent Service Auditors' Report on Management's Description of a Service Organization's System Relevant to Security, Confidentiality, Availability and the Suitability of the Design and Operating Effectiveness of Controls

For the period, February 01, 2022 to May 31, 2022

(SSAE 18 - SOC 3 Report)

Prepared by : Manoj Jain, CPA in association with

www.riskpro.in

Independent Service Auditor's Report

To : Management of ARC Document Solution, Inc (ARC)

We have examined management's assertion related to ARC AIM Scanning Services (system) that, during the period February 01, 2022 to May 31, 2022, ARC maintained effective controls to provide reasonable assurance that:

- the system was protected against unauthorized access, use or modification;
- the system was available for operation and use as committed or agreed;
- information designated as confidential was protected by the systems as committed or agreed

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). This assertion is the responsibility of SmartStream's management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of ARC's relevant controls over security, availability and confidentiality (2) testing and evaluating the operating effectiveness of the controls and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of the nature and inherent limitations of controls, the Company's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct errors or fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the systems or controls.

In our opinion, ARC management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability and confidentiality.

Manoj Jain, CPA
(Colorado Membership Number - 0023943)

July 25, 2022

Mumbai, India

Management of ARC's Assertion

July 25, 2022

Management of ARC's Assertion

During the period February 01, 2022 to May 31, 2022, ARC maintained effective controls over ARC AIM Scanning Services (the "system"), to provide reasonable assurance that:

- the system was protected against unauthorised access, use or modification;
- the system was available for operation and use as committed or agreed;
- information designated as confidential was protected by the systems as committed or agreed

based on the criteria for security, availability and confidentiality set forth in the Description Criteria DC Section 200 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (description criteria).

The attached system description identifies the aspects of the Description of ARC AIM Scanning Services covered by the assertion.

_____
Darrell Leetz
ARC Document Solutions Compliance Manager

Description of ARC's AIM Scanning Services throughout the period February 01, 2022 to May 31, 2022

Background and Overview of Services

ARC Scanning Services Overview

ARC Document Solutions AIM scanning services provide essential digitization and indexing of client's large and small format documents. Our services include customized offerings to address client's needs throughout the US with a secure and flexible solution. Our scanning solution offers an on-premise, in-house or a hybrid option designed to minimize overhead and maximize quality and efficiency returning our clients physical documents in a digitized format. By leveraging ARC's Document Conversion Workflow projects from a single box to a full warehouses of documents receive a multistage process ensuring accuracy and quality. The Document Conversion Workflow will barcode, inventory, transport, prep, scan, index, QC, OCR, re-assemble, deliver a secure digital 1 for 1 version of the original documents.

Key Processes and Essential Services

Inventory Tracking and Control
With ARC's history of client services developing a consistent solution that reassures our customers that their documents are kept safe and secure at all times starts with our inventory tracking control process. ARC has implemented a process to help manage and track document inventory from the time it leaves our customer's facilities, and as we take possession of the documents, through the necessary processing stages, until delivery back to the source location and/or document destruction. This process includes the use of specialized Barcoding, Proper Labeling, Master Spreadsheets, and Chain-of-Custody Forms. We customize this process to meet our customers need, capturing the relevant data needed from the physical collection.

Document Transport
When entrusted to transporting customers documents prior to leaving their facilities ARC will verify each box is properly sealed and if necessary, provide temper evident tape. When transported boxes are received at the ARC facility, the tamper evident tape will be inspected on each box, confirming that the box remains sealed and has not been breached during transport.

Document Indexing
Utilizing a combination of barcode, data extraction (OCR), and data entry processes, ARC collects the required metadata and associates that data to the scanned image files.

Document Preparation
ARC Document Solutions maintains a standard procedure for the typical document preparation steps required to prepare a document collection for scanning. This procedure can be slightly modified to incorporate the special requests or processing needs for the customer. ARC prepares all hard copy documents by removing binding materials, unfolding pages, re-positioning and/or removing attachments, such as Post-it notes, and organizes the hard copy paper readying it for scanning.

Document Scanning
ARC Document Solutions prides itself on producing the very best quality images possible when converting a document collection into a digital file archive. This ability stems from our over-30-years of experience in the document imaging arena. Using only Production Grade Scanners, ARC captures the images from all hard copy document pages, both front and back sides to the required specification as determined by the project SOW.

Image QC
All scanned images are checked for readability and proper orientation. All index data is also checked for accuracy and completeness. Any errors or defect images are re-scanned and corrected in this

stage.

Image Processing and Data Migration
All Images and Index data will be programmatically processed via specialized software, and OCR technology is applied to ensure that all deliverable files meet the Customer specifications. In addition, the process software will validate that all images and documents within each batch are successfully output, and that all batches are properly processed.

Document Security
ARC Document Solutions takes the security of all its client's records seriously. This means we take precautions not only for the physical security of the records, but also to control accessibility to the record content as well as the resulting image and data files. ARC document Solutions meets or exceeds all regulations as set forth by the DHS pertaining to PHI and ePHI. All hard copy records are secured within our HIPAA Compliant facilities. These facilities maintain perimeter security, including 24/7 recorded video surveillance, monitored coded CardKey access, and clean desk practices, anytime a visitor is in the area.

Subservice Organizations

ARC does not use any subservice providers for client operations.

Boundaries of the System

The specific products and services and locations included in the scope of the report are given below. All other products, services, and locations are not included.

Products and Services in Scope

Products / Application

- None

Services

- Document Scanning Services at isolated AIM centers
- Support Functions

Scope Exclusions

- Any services carried out from 6 in scope AIM centers that are not listed as in scope services.
- Only the employees and contract staff who are directly working the AIM services from the 6 in scope services are part of this system description

Geographic Locations in Scope

Office Location	Address
Charlotte, NC	628 Griffith Rd Suite H Charlotte NC 28217
Addison, Il	1433 Jeffrey Dr, Addison, IL 60101
Columbia, Md	9130 Red Branch Rd Suite N, Columbia, MD 21045
Santa Clara, Ca	821 Martin Ave, Santa Clara, CA 95050

Costa Mesa, Ca	345 Clinton St, Costa Mesa, CA 92626
Dacoma, Tx	4900 Dacoma St, Houston, TX 77092

The report excludes all processes and activities that are executed outside the above locations. ARC has their offices in the USA. These offices are not included in the scope of the report. Unless otherwise mentioned, the description and related controls apply to locations covered by the report.

Description of Control Environment, Control Activities, Risk Assessment, Monitoring and Information, and Communication

Control Environment

ARC's internal control environment reflects the overall attitude, awareness, and actions of management concerning the importance of controls, and the emphasis given to controls in the Company's policies, procedures, methods, and organizational structure.

The Chief Executive Officer, the Senior Management Team, and all employees are committed to establishing and operating an effective Information Security Management System in accordance with its strategic business objectives. The Management at ARC is committed to the Information Security Management System and ensures that IT policies are communicated, understood, implemented, and maintained at all levels of the organization and regularly reviewed for continual suitability.

Board of Directors

Business activities at ARC are under the direction of the Board of Directors. The company is governed by its Board of Directors headed by its Chairman & CEO. Suriyakumar Kumarakulasingam who is in charge of the company's Global operations playing a key role in strategy and client management.

Risk Management and Risk Assessment

The application of protection measures is based on the risk associated with information assets and the importance of those assets to the organization. As part of this process, security threats are identified and the risk from these threats is formally assessed.

ARC has placed into operation a risk assessment process to identify and manage risks that could adversely affect their ability to provide reliable processing for User Organizations. This process consists of management identifying significant risks in their areas of responsibility and implementing appropriate measures to address those risks. The senior Management team is members of forums and core working groups in industry forums that discuss recent developments.

Information Security Policies

ARC has developed an organization-wide ARC Information Security Policies.

Relevant and important Security Policies (IS Policies) are made available to all employees via Company Intranet or as hard copy policies to new employees. Changes to the Information Security Policies are reviewed and approved before implementation.

Monitoring

Monitoring is a critical aspect of internal control in evaluating whether controls are operating as intended

and whether they are modified as appropriate for changes in business conditions. ARC management and Information Security personnel monitor the quality of internal control performance as a routine part of their activities.

Information and Communication

ARC has documented procedures covering significant functions and operations for each major workgroup. Policies and procedures are reviewed and updated based upon changes and approval by management. Departmental managers monitor adherence to ARC policies and procedures as part of their daily activities.

ARC management holds departmental status meetings, along with strategic planning meetings, to identify and address service issues, customer problems, and project management concerns. For each service, there is a selected service manager who is the focal point for communication regarding the service activity. Additionally, there are personnel that has been designated to interface with the customer if processing or systems development issues affect customer organizations. Electronic messaging has been incorporated into many of ARC's processes to provide timely information to employees regarding daily operating activities and to expedite management's ability to communicate with ARC employees.

Components of the System

Infrastructure

The infrastructure comprises physical and hardware components of the System including facilities, equipment, and networks.

Network Segmentation Overview

ARC offices are equipped with the latest hardware, software, and networking infrastructure. Offices are linked using high-speed communication links, backed up by redundant networks.

Physical Structures and Physical Access

Physical Access

The entrance for in-scope ARC's physical office(s) is secured by a security person, physical access control system, and CCTV surveillance. Physical and Environmental Security of ARC is controlled and governed by ARC ISMS Policy.

Entry to the ARC offices is restricted to authorized personnel and a physical access control system is installed at all entrances. All employees are provided with access cards / biometric access. All visitors have to sign the visitor's register and are given an inactive visitor card.

On separation of an employee from the organization, the HR group initiates the 'Exit Process' and circulates it to all the concerned groups. Based on this, the employee's privileges in the access control system are revoked.

Environmental Controls

ARC's power systems are designed to provide uninterrupted power, regardless of the availability of power from the local public utilities supplying the office premises. Backup UPS units and backup

generators supply (owned or provided by Building Maintenance) power to the center in the event of a power failure. All components are covered by maintenance contracts and tested regularly.

Software

Firewalls

Hardware firewalls are configured and in place to protect IT resources. Firewalls and switch configuration standards are documented. Firewall and switch configurations are reviewed by management periodically. The ability to modify firewalls is limited to the ARC IT Department. Specifically, the IT Department is authorized to request changes from the provider.

Network & endpoint protection / monitoring

Access to Internet services from any company computing device (laptop, workstation, server, etc.) or any company address designation should be made through the company's approved perimeter security mechanisms. External connections to company servers are not permitted.

Monitoring

ARC has devised and implemented adequate monitoring controls to detect unauthorized information processing activities. Critical servers and systems are configured to log user activities, exceptions, and information security events. System administrator and system operator activities are logged and reviewed periodically.

Patch Management

All security patches are tested for stability before applying to the production environment. The patches are applied regularly or as required to ensure the efficient operation of the servers, endpoints, and network devices. Operating system patches are managed and applied as they become available.

People

Organizational Structure

The organizational structure of ARC provides the overall framework for planning, directing, and controlling operations. It has segregated personnel and business functions into functional groups according to job responsibilities. This approach helps enable the organization to define responsibilities, lines of reporting, and communication, and helps facilitate employees to focus on the specific business issues impacting ARC clients.

New Hire Procedures

New employees are required to read ARC's' corporate policies and procedures and sign an acknowledgment form stating that they have read and understood them. Hiring procedures require that the proper educational levels have been attained along with required job-related certifications, if applicable, and industry experience. If a candidate is qualified, interviews are conducted with various levels of management and staff.

Background and reference checks are completed for prospective employees before employment over the phone. Employees are required to sign Employee Confidentiality Agreement and are on file for employees. Discrepancies noted in background investigations are documented and investigated by the Human Resources Department in conjunction with a third-party verification agency. Any discrepancies found in background investigations result in disciplinary actions, up to and including employee

termination.

Employee Terminations

Termination or change in employment is being processed as per ARC HR-related procedures. There are identified and assigned responsibilities about termination or change in employment.

Access privileges are revoked upon termination of employment, contract, or agreement. In case of change of employment /role, rights associated with the prior roles are removed and new access privileges are created as appropriate for the current job roles and responsibilities.

Procedures

IT policies and operating instructions are documented. Procedures described cover server management, server hardening, workstation security system, network management, security patch management, user creation, system audit, ID card activation, etc. Additionally, production and training standard operating procedures are available.

Change Management

ARC has implemented a well-defined Change management process to ensure that all changes to the information processing facilities, including equipment, supporting facilities and utilities, networks, application software, systems software, and security devices are managed and controlled. The Change Management process describes a methodical approach to handle the changes that are to be made to any work product. All the changes need to be subjected to a formal Change Management process.

Incident Response and Management

Procedures for the incident response including identification and escalation of security breaches and other incidents are included in the policy. Users or any other person log all incidents to the Helpdesk. The help desk personnel study and escalate all security incidents to the designated team for further escalation/resolution. Any event related to the security of Information assets including facilities and people is termed an Incident.

Logical Access

Security Authorization and Administration

Email is sent from HR to IT helpdesk for all new employees for a new workstation configured with minimum default access to company resources/applications required by an employee to perform the job duty. Any additional access is recommended by the line manager and/or Compliance Manager. The company has a standard configuration that is implemented across Desktops & laptops individually.

Outbound Communication

ARC developed applications are accessible in ARC Network. For uploading the files and communication to the client, external internet access is required. Internet usage is restricted through content filtering tools. The IT Team periodically reviews and recommends changes to web and protocol filtering rules. Human Resources review these recommendations and decide if any changes are to be made.

Confidentiality

ARC has implemented a data retention policy to ensure the confidentiality of client data. All agreements

with related parties and vendors include confidentiality commitments consistent with the company's confidentiality policy (as described in IT and Security Policies).

Availability

Backup and Recovery of Data

ARC has developed a Backup policy and suitable backups are taken and maintained. ARC has put in place backup processes that define the type of information to be backed up, backup cycles, and the methods of performing a backup.

The backup processes are approved by the business owners and comply with the requirements for business continuity, and legal & regulatory requirements. All backup and restoration logs are maintained for retention periods as defined in the backup procedures.

All backup copies are tested periodically to ensure that the data and information are securely retrievable in the event of an emergency without any loss of information. Users are made aware through adequate training of their responsibilities for ensuring backup of required data and information.