Hiestand, Brand, Loughran, P.A.

SOC 3® REPORT ON CONTROLS RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY FOR ARAS INNOVATOR® SAAS APPLICATION SERVICES

ARAS CORPORATION

OCTOBER 16, 2022 TO OCTOBER 15, 2023

An Affiliate Company of
360ADVANCED

ARAS CORPORATION

Table of Contents

SECTION 1:

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Aras Corporation:

Scope

We have examined Aras Corporation's ("Aras") assertion of Aras Innovator® SaaS Application Services included in Section 2 of this report that the controls within Aras' system were effective throughout the period October 16, 2022, to October 15, 2023, to provide reasonable assurance that Aras' 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* (*With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*.

Aras uses Microsoft Corporation, a sub-service organization, for cloud hosting and managed services. Aras' assertion and description of the boundaries of the Aras Innovator® SaaS Application Services system, included in Section 2 and Section 3 of this report, respectively, indicate that certain applicable trust services criteria can only be met if certain types of controls at the aforementioned sub-service organization are suitably designed and operating effectively. The description does not include any of the controls expected to be implemented at the sub-service organization. Our examination did not extend to the services provided by the sub-service organization, and we have not evaluated whether the controls management expects to be implemented at the sub-service organization have been implemented or whether such controls were suitability designed and operating effectively throughout the period October 16, 2022, to October 15, 2023.

Service Organization's Responsibilities

Aras 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 Aras' service commitments and system requirements were achieved. Aras has also provided the accompanying assertion titled "Management of Aras Corporation's Assertion" included in Section 2 of this report about effectiveness of controls within the system. When preparing its assertion, Aras is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

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

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Aras' service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Aras' service commitments and system requirements based on the applicable trust services criteria

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

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

Inherent Limitations

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

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

Opinion

In our opinion, management's assertion that the controls within Aras' Aras Innovator® SaaS Application Services system were effective throughout the period October 16, 2022, to October 15, 2023, to provide reasonable assurance that Aras' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

January 19, 2024
St. Petersburg, Florida

SECTION 2:

MANAGEMENT'S ASSERTION

MANAGEMENT OF ARAS CORPORATION'S ASSERTION

January 19, 2024

We are responsible for designing, implementing, operating, and maintaining effective controls with Aras Corporation's ("Aras") Aras Innovator® SaaS Application Services system throughout the period October 16, 2022, to October 15, 2023, to provide reasonable assurance that Aras' service commitments and system requirements relevant to Security, Availability, and Confidentiality were achieved. Our description of the boundaries of the system is presented in Section 3 of this report and identifies the aspects of the system covered by our assertion. Aras uses Microsoft Corporation, a sub-service organization, for cloud hosting and managed services. The description included in Section 3 excludes the applicable trust services criteria and related controls of the sub-service organization.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period October 16, 2022, to October 15, 2023, to provide reasonable assurance the Aras' service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*. Aras' objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section 4 of this report.

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

We assert that the controls within the system were effective throughout the period October 16, 2022, to October 15, 2023, to provide reasonable assurance that Aras' service commitments and system requirements were achieved based on the applicable trust services criteria.

/s/ Aras Corporation

Boma Koko – Senior Director Global Cloud Services

SECTION 3:

DESCRIPTION OF THE SYSTEM

OVERVIEW OF OPERATIONS AND THE SYSTEM

Company Overview and Background

Aras is a global company providing enterprise-level Product Lifecycle Management (PLM) software. The company was established in 2000 by Peter Schroer, Founder, and is headquartered in Andover, Massachusetts, with more than 600 employees. The Aras team includes executives and technologists from across the PLM industry, and the company focuses on delivering a full-featured PLM suite out-of-the-box that is more easily adapted to companies' specific competitive practices rather than forcing them to compromise to fit the software.

An open architecture with advanced PLM platform technology makes Aras scalable, flexible, and secure for large organizations, and an array of applications provide functionality for companies of any size. With business solutions for global product development, multi-site manufacturing, supply chain operations, and quality compliance, Aras serves companies that have complex products and processes.

Aras is offered in a SaaS-style subscription (Software as a Service) which includes PLM license expenses for a lower total cost of ownership and faster time to value.

Overview of Aras Innovator® SaaS Application Services System

Aras Innovator®

Aras Innovator® is a scalable web-based platform with a suite of PLM business solutions that deploy and adapt to evolving business needs. This PLM platform is comprised of four layers that include the client, application, services, and repository, each designed to be open, flexible, scalable, and upgradable in efforts to simplify the complex product the customer is designing.

The software was designed using Aras' concept of the "Digital Thread". The "Digital Thread" links critical information allowing companies to track a product and its digital assets from concept through design, manufacturing, quality, and field maintenance. Aras Innovator® strives to achieve this concept through its solutions offerings, which include:

- Product Engineering
- Change Management
- Requirements Engineering
- Component Engineering
- Manufacturing Process Planning
- Enterprise Search
- Self-Service Reporting
- Supplier Collaboration
- Configuration Management
- Workflow
- Systems Architecture
- Quality Management System
- Digital Twin Core
- CAD Connector Framework
- Visual Collaboration
- Dynamic Product Navigation
- Bill of Materials
- Program Management
- Simulation Management
- Technical Documentation
- Maintenance Management
- Office Connector
- Document Management
- PDM / PLM Integration

Aras Enterprise Subscription

The Aras Enterprise Subscription consists of the Aras Innovator® application that is hosted via a SaaS model where subscribers can customize their platform and build unique solutions in a true, cloud native environment with scalability to meet complexity and size demands. It supports customer individuality by delivering the capabilities needed to solve specific, personalized challenges. The Aras Enterprise Subscription covers the following areas:

- SaaS
- Comprehensive Low Code PLM Platform
- Highly Available On the Cloud (Azure)
- Install and Maintain Infrastructure
- Install and Maintain Aras Environments
- Infrastructure Support
- Monitoring of Infrastructure
- Unlimited Deployment of Customizations
- Change Management Process
- Deployed in several regions around the world
- Secure and no dependencies or impact on other customers
- Personalized performance tuning to meet customers' needs
- Full Capabilities of Aras Innovator® Platform
- Fully confidential and customer owns their data
- DevOps provides Continuous Integration and Continuous Deployment (CI/CD) pipelines

Aras offers its customers either an enterprise subscription or managed services subscription; both allow for the customer to have their own dedicated Azure environments with a higher level of control and individual capabilities for their applications and operations. Having a dedicated environment allows for flexible upgrade schedules, personalized performance based on a customer's workload, and ensures that customer data does not reside physically or logically outside the customer's domain.

Aras Managed Services Subscription

Customers can choose to host Aras Innovator® within Aras' Azure environment with the enterprise subscription, or within the customer's Azure environment with the managed services subscription, and Aras' Global Cloud Services (GCS) team manages aspects of the environment alongside the customer. With the managed services subscription option, the customer is billed directly by Azure. With this subscription model, it is required that the environment be architected the same way as if it were to be implemented via the enterprise subscription. Customers are required to follow the same processes and utilize the same tools as well.

Sub-Service Organizations and Complementary Controls

Aras uses Microsoft Corporation ("Azure"), a sub-service organization, for cloud hosting and managed services. To monitor and evaluate the adequacy and effectiveness of controls in place at the sub-service organization, Aras' management obtains and reviews the Service Auditor's report and / or compliance certifications for the sub-service organization on an annual basis.

The sub-service organization is responsible for implementing logical, physical, and environmental control activities to ensure the IT infrastructure is protected from certain threats.

Control Considerations for the Sub-Service Organization

1. The sub-service organization is responsible for implementing physical security controls to ensure access to data centers and storage facilities are limited to authorized personnel and that information systems are protected from unauthorized access, damage, and interference.
2. The sub-service organization is responsible for implementing environmental security controls to ensure that critical information technology infrastructure is protected from environmental threats.
3. The sub-service organization is responsible for notifying Aras' personnel, in a timely manner, when changes are made to technical or administrative controls that may impact Aras' systems.
4. The sub-service organization is responsible for notifying Aras personnel of any actual or suspected information security breaches or fraud, including compromised user accounts.

Infrastructure

Aras leverages a cloud-based infrastructure for hosting the Azure environments supporting the Aras Innovator® SaaS Application Services system. Automated processes utilizing Infrastructure as Code (IaC) tools create consistency in building the Azure production and non-production environments for each customer. The basic architecture of these environments is documented using network diagrams, and includes, but is not limited to, resource groups for managing and storing metadata, identity access management (IAM) for customer-specific role-based access control (RBAC), network and application layer load balancing, and network security groups for filtering and restricting inbound and outbound network traffic.

Aras Innovator® is hosted using Internet Information Services (IIS) for web access and security, supporting data-in-transit encryption technologies.

The following describes the in-scope components supporting the Aras Innovator® SaaS Application Services system:

System / Application	Description
Azure DevOps	Change Management for customer deployment customization
Aras MyInnovator	Change Management for internal services
Aras Ticketing System	Subscriber Tickets / Customer Tickets / Help Desk Tickets
Microsoft Authenticator	Multifactor Authentication (MFA)
Terraform	IaC provisioning
Jenkins / Azure Pipelines	Code Pipelines and Builds

Software

The Aras GCS team utilizes a variety of tools and software for supporting the Aras Innovator® SaaS Application Services system. Predominately, Azure Native Services tools are used because the environments that host the application and related services are created and maintained using Azure.

People

The Aras Innovator® SaaS Application Services relies on GCS for infrastructure and software maintenance, cloud service operations, security and compliance efforts, and customer support. GCS consists of the following departments:

- **GCS Management –** Personnel that serve as an escalation point for other GCS teams for guidance and decision making. GCS Management personnel can approve blueprint changes (changes to architecture supporting the Aras Innovator® SaaS Application Services system) and include the Vice President (VP) of Engineering and the Senior Director of Global Cloud Services.
- **GCS Tools –** Personnel responsible for writing, managing, and maintaining IaC code, scripting (Terraform, Groovy, etc.), subscription creation, and high-level role permission assigning. Job roles include Site Reliability Managers and Software Engineers.
- **GCS Operations –** Personnel responsible for the normal operations of the services supporting the Aras Innovator® SaaS Application Services system consist of Site Reliability Engineers. Their standard job duties include, but are not limited to, provisioning environments and the deployment of solutions to production, cost and reporting, Operating System (OS) patching, and the setup of endpoints. In addition, they are responsible for monitoring and maintaining Azure monitoring tools and for responding to detected issues.
- **GCS Security / Compliance –** Personnel responsible for monitoring and maintaining Azure monitoring tools and for responding to detected security and compliance incidents / suspected events. These personnel have "Read" only access to systems for report generation and gathering evidence for compliance efforts. Job roles include the Director of Product Security and Manager Operations and Compliance.

Procedures

Aras' management is responsible for maintaining and implementing information technology general computer controls related to computer processing supporting the Aras Innovator® SaaS Application Services system. These controls are supported by information security-related polices and Standard Operating Procedures (SOPs) designed to be structured around the International Organization for Standardization (ISO) 27001 framework and are made available to appropriate personnel using information sharing tools such as Microsoft SharePoint and Teams.

Aras' management documents, maintains, and communicates relevant policies to its personnel to address the following lifecycle areas:

- Acceptable Use
- Privacy and Data Protection
- Data Retention & Disposal
- Risk Management
- Logical Security
- Vendor Management

User Access Management

Access Provisioning & Maintenance

Aras uses a combination of multiple systems to ensure personnel have proper access to resources utilizing RBAC while maintaining the principle of least privilege. Upon hire, a ticket is created to track and manage the process of granting access to systems. Human Resources (HR) is responsible for creating the ticket and for ensuring the appropriate technical personnel are assigned within the ticket for documenting the approvals for the access granted based on the new hire's job role. Accounts are reviewed annually by GCS to ensure user access levels are justified, and accounts discovered to not be justified are removed or disabled.

Access to customer production environments is governed using customer specific IAM plans that detail the roles and permissions of both the customer and Aras GCS personnel. Both parties agree to the plan and coordinate specific personnel for each role prior to commencing services.

Access Removal

The access removal process begins upon notification that the personnel is terminated. A termination ticket is created to track and document the process of removing system access for specified personnel, and access is removed the day of termination.

Access Control to Production

GCS personnel need access to Azure production environments to support and monitor infrastructure, implement deployments, and to perform maintenance services for customers. With the enterprise cloud subscription, Aras hosts both customer production and non-production subscriptions within Aras' Azure environment. Customers who use managed services host the production and non-production subscriptions within their own Azure environment.

Prior to accessing the Azure cloud management console, GCS personnel need to be authenticated through the corporate VPN. The Azure cloud management console is then accessible, and the user is further authenticated using the user's Microsoft Entra ID profile and MFA. Once authenticated through the console, the user connects to the production environment through a bastion host and jump box. Customer access to the application is limited through the use of a site-to-site virtual private network (VPN) or through the public internet with additional measures such as DDoS (Distributed Denial of Service) Protection and Web Application Firewall (WAF). The level of access GCS personnel with Owner permissions have to a customer's production environment depends on the permissions outlined per the customer IAM plan.

Application Access Control

Access to the Aras Innovator® application is restricted via unique username and password; these credentials are encrypted in transmission through the web portal via HTTPS. Aras employs application gateways and network parameters to block direct access to internal systems. Additionally, built-in Mandatory Access Control, Discretionary Access Control, and RBAC are in place to assign permissions and restrict access within the application.

Change Management

Software Development

Aras Innovator®

Aras uses an agile methodology for software development to ensure changes satisfy user requirements, segregation of duties, and quality assurance (QA). This process covers software development and changes made to the primary Aras Innovator® solution owned and managed solely by Aras. Aras uses its in-house ticketing system for documenting and keeping track of end user change requests throughout the software development lifecycle (SDLC). Product Owners organize these end user requests into stories, which are packaged and worked on in program increments. Once a story has been clarified by a Product Owner, it is assigned to a developer to review the change and develop necessary code. The story is then assigned to the validation stage, in which QA and various automated tests are performed. Once QA and testing have successfully been completed, a Product Owner formally approves the story before it can be released into the next iteration cycle. Aras ensures segregation of duties by restricting developer access to the production environment and by having systematic restrictions in place to disallow the promotion of code by developers. Code is migrated to production by GCS Operations personnel.

Customer Customizations

Aras allows customers the ability to customize deployments to better suit their needs and environments. Each customer has their own environment within Azure DevOps which allows the customer to work with Aras on customizing a deployment. Additionally, software development or customizations made within the customer hosting environment will follow the applicable change management process defined and managed by the customer.

Within Azure DevOps, customers can perform deployments of changes, when they are ready, to their non-production environments (Staging or UAT). These changes are compiled into a package using Azure tools and Jenkins. This process creates a clean environment and checks the latest build version. If checks are passed, the package is then deployed into a Systems Integration Testing (SIT) environment and passed through an automated pipeline. From there, the package is put into storage where it can be accessed for other forms of testing. Once the results of these tests are approved by QA, the package then goes through user acceptance testing (UAT). During UAT, the package is deployed into a staging environment where data migration is performed for the customer to validate and ensure changes are functioning as intended. To proceed from UAT, the customer is required to give explicit approval before the deployment can be implemented to the customer's production environment. After the customer approves, and after any additional required testing is performed, the non-production uniform resource locator (URL) is changed to a production URL.

System Patching

Aras follows a patching SOP in the event a system patch needs to be applied to customer environments. When Aras is notified of an emergency patch, the customer's cloud services coordinator (CSC) is notified. System patches identified as imminent are addressed as soon as Aras is notified by Microsoft. Testing and implementing the patch does not require a response from the customer to reduce the amount of time that systems are exposed to critical security vulnerabilities.

System patches deemed as non-imminent are addressed in coordination with the customer. System patches, regardless of nature, are manually tested locally before they are applied to customer environments for customers that elect to utilize Aras for patch management.

Availability / Backup Restoration / Disaster Recovery

Aras uses Azure Native Services' built-in high availability and redundancy features to meet Recovery Time Objective (RTO), Recovery Point Objective (RPO), and Recovery Consistency Objective (RCO) obligations. These objectives are defined within the Disaster Recovery (DR) plan and in written SOPs, which are in place to ensure personnel follow the necessary steps for recovery, have access to appropriate contact information, and are aware of their roles and responsibilities related to DR and backup restoration.

Aras performs system backups to ensure data remains recoverable; types of backups include database and vault backups. Point-in-time restore (PITR) backups are automatically performed in predefined intervals by default. These backups are retained for predefined number of days by default. Vault backups are performed daily to backup files. Customer data is duplicated across availability zones to guarantee redundancy. Additionally, Aras performs backup test exercises on the databases and vault files annually to ensure that processes related to backup restoration are current, efficient, and known to the appropriate personnel.

Incident Response

An incident response plan is in place that documents the procedures to follow during actual security events. Azure monitoring tools and internal communication channels are in place to detect and communicate potentially identified cloud security incidents. The incident is investigated by the Cloud/Product Incident Response Team (PSIRT/CSIRT) and if determined to be an incident, they communicate the actions needed to contain, eradicate, and recover from the incident within an action list and incident response checklist. GCS and corporate operations are responsible for implementing the actions put forth in the action list, and customers that are affected by the incident are notified as per SLA.

Responsibility for reviewing and approving documentation and templates related to cloud incident response is handled by the Cloud Incident Response Guidance Counsel (CIRGC). The CIRGC meets quarterly to review and update documentation and to discuss lessons learned from actual cloud security incidents. Incident response test exercises are performed annually to incorporate changes to the documentation and to test the efficiency of the procedures outlined within the incident response plan.

In the event of severe security incidents, such as data breaches, Aras has in place cybersecurity insurance to offset financial loss.

Customer Management

Customer management begins with the onboarding process. SOPs and customer onboarding presentations are used to guide personnel in the process of ensuring necessary information is gathered for setting up customer environments and role-based access. Prior to commencing services, customers and Aras both sign contracts agreeing to the responsibilities and agreed-upon services. Customers can contact Aras support via a dedicated subscriber portal where they can file support and incident tickets.

Data

Aras is not responsible for the data customers input within their application. However, Aras Innovator® does utilize forms that validate data entry appropriately and workflows to manage work assignments and notifications. Data reporting is available through built-in reporting tools. History can be enabled on each row to keep track of versioning and to track changes.

Aras also abides by an established data lifecycle SOP which outlines data destruction and encryption obligations. Furthermore, encryption standards for data are defined within an encryption policy, and data is encrypted at rest for the SQL databases, virtual machines (VM), and file storage locations.

A protection of data policy is established that outlines data handling requirements in accordance with General Data Protection Regulation (GDPR) standards. Additionally, a policy is in place for the protection of records that defines security and GDPR requirements for handling organizational records in Europe.

SECTION 4:

SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Aras designs its processes and procedures related to Aras Innovator® SaaS Application Services system to meet its objectives. Those objectives are based on the service commitments that Aras' management makes to user entities; the laws and regulations that govern the provisioning of the Aras Innovator® SaaS Application Services system; and the financial, operational, and compliance requirements that Aras' management has established for the services. The Aras Innovator® SaaS Application Services system of Aras is subject to the regulatory requirements of the State, Federal, and International governing bodies in the areas in which Aras operates.

Security, availability, and confidentiality commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offerings provided to customers. Commitments are standardized and include, but are not limited to, the following:

Trust Services Category	Service Commitments	System Requirements
Security	➢ Security principles within the fundamental design of the system that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role ➢ Breach, security incident, and critical system patching notification requirements	➢ Logical access standards and enforcement of least privilege permissions ➢ Incident management standards
Availability	➢ System uptime ➢ Maintaining sufficient backups and procedures for testing recovery capabilities	➢ System monitoring standards ➢ Backup and recovery standards
Confidentiality	➢ Use of encryption technologies to protect customer data both at rest and in transit ➢ Documented data retention requirements	➢ Encryption standards ➢ Data retention standards