Publish Faster. Publish Smarter.

Aries Systems Corporation

Independent Service Auditor's SOC 3 Report

For the Editorial Manager System

June 30, 2019

Attestation and Compliance Services

Quality, above all.

Independent Service Auditor's Report

To Aries Systems Corporation:

Scope

We have examined Aries Systems Corporation's ("Aries Systems") accompanying assertion titled "Assertion of Aries Systems Management" ("assertion") that the controls within the Aries Systems' Editorial Manager system ("system") were effective as of June 30, 2019, to provide reasonable assurance that Aries Systems' 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)*.

Aries Systems uses various subservice organizations for data center hosting services. The description of the boundaries of the system indicates that complimentary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Aries Systems, to achieve Aries Systems' service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complimentary subservice organization controls.

The information included in, "Management's Response to Suitability of Design Qualification" is presented by Aries Systems management to provide additional information and is not a part of the description. Information about Aries Systems' response to a suitability of design qualification has not been subjected to the procedures applied in the examination of management's assertion that the controls within the Aries Systems' Editorial Manager system were effective as of June 30, 2019, to provide reasonable assurance that Aries Systems' service commitments and system requirements were achieved based on the applicable trust services criteria.

Service Organization's Responsibilities

Aries Systems 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 Aries Systems' service commitments and system requirements were achieved. Aries Systems has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Aries Systems 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 as of June 30, 2019 to provide reasonable assurance that the service organization's service commitments and systems 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 Aries Systems' service commitments and system requirements based on the applicable trust services criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Aries Systems' service commitments and system requirements based on the applicable trust services criteria.

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

Inherent Limitations

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

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

Explanatory Paragraph

The description of the Aries system does not specify how the potential for fraud is considered when assessing risks to the achievement of objectives. As a result, controls were not suitability designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on trust services criterion *CC3.3, The entity considers the potential for fraud in assessing risks to the achievement of objectives.*

Opinion

In our opinion, except for the effects of the matter giving rise to the modification, management's assertion that the controls within Aries Systems' Editorial Manager system were effective as of June 30, 2019, to provide reasonable assurance that Aries Systems' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Schellman & Company, LLC

Atlanta, Georgia
October 22, 2019

ASSERTION OF ARIES SYSTEMS MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Aries Systems Corporation's ("Aries Systems") Editorial Manager system ("system") as of June 30, 2019, to provide reasonable assurance that Aries Systems' service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented below and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system as of June 30, 2019, to provide reasonable assurance that Aries Systems' 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)*. Aries Systems' objectives for the system in applying the applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

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 as of June 30, 2019, to provide reasonable assurance that Aries Systems' service commitments and systems requirements were achieved based on the applicable trust services criteria.

We do not specify in our description how the potential for fraud is considered when assessing risks to the achievement of objectives. As a result, controls were not suitability designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved as of June 30, 2019, based on trust services criterion CC3.3 which states, "The entity considers the potential for fraud in assessing risks to the achievement of objectives."

System Description of the Editorial Manager System

Company Background

Aries Systems Corporation was founded in 1986 and has developed several generations of technologies that serve the needs of publishers, including Editorial Manager®, an online manuscript submission and peer-review system; ProduXion Manager®, an online production tracking system; and Commerce Manager, an e-commerce solution for efficient processing of non-subscription-type charges.

Editorial Manager grew out of Editorial Assistant, a desktop manuscript-tracking application used by journals since the early 1990s. Editorial Manager (the Web-based version) was launched in the spring of 2001 and has been rapidly adopted by scholarly societies and publishers.

Aries Systems is headquartered in North Andover, Massachusetts, USA, with local staff representing the company in Germany and the United Kingdom. Aries Systems was acquired by Elsevier in September 2018.

Description of Services Provided

Editorial Manager users are Authors, Editors, and Reviewers. Authors submit manuscript files and metadata and act on revision requests. Editors use the system to review submissions, assign to Reviewers, and make and communicate decisions to accept, revise, transfer or reject manuscripts. Reviewers are invited to work on manuscripts, can accept or reject assignments, flag their own availability and specialties for Editors, and perform and submit all review tasks right in the system.

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Principal Service Commitments and System Requirements

Aries is committed to providing customers a secure and reliable service through the Editorial Manager software. Commitments are defined in customer contracts that are designed between Aries and the client. In addition, commitments are defined via policies and procedures set forth by management and conveyed to employees during the new hire process. The contracts between Aries and clients contain specific language around the security procedures that Aries will provide as part of their ongoing services. Aries has implemented a security policy that is designed to achieve its commitments. In the event of a failure to meet commitments made to its customers, Aries has implemented an incident response and escalation procedures designed to identify, investigate, resolve, and communicate the incident to affected parties.

Aries warrants that the System will be available to Publisher and the Users at an average level of no less than 98% of each calendar month, 24 hours daily, with the exception of periods of unavailability caused by circumstances beyond Aries' control, and of pre-scheduled maintenance periods not to exceed four hours weekly. Aries shall notify publisher at least 48 hours in advance of pre-scheduled maintenance and describe the nature of the service organization's availability commitments and how those commitments are communicated and documented.

Aries further commits to exert reasonable commercial efforts to protect the content and publisher data within its possession from any dissemination not explicitly authorized by the client. Such efforts shall reflect the highly confidential nature of the client data.

In accordance with our assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

Infrastructure and Software

The Editorial Manager application is hosted at the NaviSite third-party facility. Aries owns and maintains hardware located in the NaviSite data center. The in-scope infrastructure consists of multiple applications, operating system platforms and databases, as shown in the table below:

Primary Infrastructure				
Production Application	**Business Function Description**	**Hardware Platform**	**Operating System Platform**	**Physical Location**
EM Web Servers	Front end portal access for customers	Virtual Machine	Windows Server 2012 Standard	NaviSite (Primary), Cyrus One (Disaster Recovery (DR))
EM Async Servers	Utility servers performing various functions for ingest	Virtual Machine	Window 8.1 Pro	NaviSite (Primary), Cyrus One (DR)
EM Database Servers	Servers to store customer data	HP Proliant Servers	Windows Server 2012 Standard	NaviSite (Primary), Cyrus One (DR)
Backup Servers	Manages the backups for production data	HP Proliant Servers	Windows Server 2012 Standard	NaviSite
VMware Hosts	Servers to manage the virtual environment of production	HP Proliant Servers	VMware 6.5	NaviSite (Primary), Cyrus One (DR)
Mail Servers	Facilitate communication for customers	Virtual Machine	Ubuntu	NaviSite (Primary), Cyrus One (DR)
DataDomain	Store customer data backups on prem and offsite	EMC Hardware	EMC	NaviSite (Primary), Cyrus One (DR)
Near Archive Servers	Database servers storing customer archive data	HP Proliant Server	Windows Server 2012 Standard	NaviSite (Primary), Cyrus One (DR)
Juniper Firewall Cluster	Security appliance for production. Manages Firewall rules, routing, network address translation (NAT), port address translation (PAT) policies	Juniper Firewall Cluster	Juniper Firewall Cluster	NaviSite (Primary), Cyrus One (DR)

Primary Infrastructure

Production Application	Business Function Description	Hardware Platform	Operating System Platform	Physical Location
Array Networks Load Balancer Cluster	Provides the distribution of traffic to webservers, reporting servers	Array Networks Appliance	Array OS	NaviSite (Primary), Cyrus One (DR)
Array Networks Virtual Private Network (VPN) Cluster	Provides remote access to end user network (Non production)	Array Networks Appliance	Array OS	NaviSite (Primary), Cyrus One (DR)
Sonicwall Unified Threat Management (UTM) appliance cluster	End User Security appliance (nonproduction)	Dell Appliance	Sonicwall (UTM) appliance cluster	NaviSite
Unity 400 Storage Area Network (SAN)	Backend Storage for data servers	EMC	EMC	NaviSite (Primary), Cyrus One (DR)
Unity 300 SAN	Backend Internet Small Computer Systems Interface (ISCSI) Storage for virtual environment	EMC	EMC	NaviSite (Primary), Cyrus One (DR)
EMC 5400	Near Archive Storage for Data Servers	EMC	EMC	NaviSite (Primary), Cyrus One (DR)
AQC Servers	Image Check Software	Mac	Mac OS	NaviSite (Primary), Cyrus One (DR)

People

The following personnel responsible for Aries operations:

- Engineers – Responsible for the development of Editorial Manager.
- Database Administrators – Responsible for migrations, upgrades, and database troubleshooting.
- Information Technology (IT) – Responsible for infrastructure support, deploying code, server administration, and backups.

The following functions are supplied by Elsevier corporate shared services and accessed as needed by the Aries team:

- Executive Management – responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
- Human Resources (HR) – responsible for HR policies, practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisitions, employee retention, compensation, employee benefits, performance management, employee relations and training, and development).

Procedures

Access Authentication and Authorization

Access to system information, including confidential data, is protected by authentication and authorization mechanisms. Standard build procedures for installation and maintenance of production servers are in place which includes the requirement for access control systems to enforce logical access controls. The authentication and authorization mechanisms include configurations to the in-scope systems which authenticate users with a unique user account and enforce minimum password requirements. In addition to the enforcement of password requirements, predefined security groups are utilized to assign role-based access privileges and segregate access to data. Administrative access privileges are restricted to user accounts accessible by authorized personnel. Shared account passwords are maintained in an encrypted data vault.

Management conducts user access reviews, including privileged users, semi-annually to help ensure that access to data is restricted to current employees. Accounts identified as inappropriate are investigated and resolved. Employee workstations are configured to enforce disk encryption to prevent unauthorized access should the workstation become compromised.

Furthermore, the Aries production network is segregated from that of the parent company. Parent company personnel are not authorized to access Aries network content.

A firewall system is in place to filter unauthorized inbound network traffic from the Internet. The firewall is configured to deny network connections that are not specifically authorized. Management reviews firewall rulesets semi-annually to help ensure only necessary connections are configured. In addition, the security incidents and event management (SIEM) application logs and alerts IT personnel in the event of a firewall configuration change. Web servers utilize transport layer security (TLS) encryption for web communication sessions. An intrusion prevention system IPS is utilized to analyze and report network events and to block suspected or actual network security breaches. Additionally, an encrypted VPN is required for remote access to production data. This remote access requires the use of two-factor authentication through the use of both a token and a passcode.

Access Requests and Access Revocation

User access requests are documented in help desk tickets and approved by management prior to access being granted. A ticket is also created to revoke system access for terminated employees as a component of the employee termination process.

Change Management

Aries monitors production change requests using a ticketing system that tracks and documents the progress of the change through implementation. Aries change management policies and procedures are in place to guide personnel in the request, documentation, testing, and approval of changes. The policies and procedures are available on the company intranet for employees to reference as needed. The project management team authorizes and prioritizes the changes to be made prior to the development of the changes. Changes are prioritized based on criteria level between low, medium, high, and ultra-high, which is determined based on the impact of the change. After development, changes are tested in the quality assurance (QA) environment. Prior to deployment, changes are bundled together into a Hotfix, where they undergo a code review and Hotfix checklist review. A code review is performed by the team lead for each change prior to application releases.

During the code review, team leads review the cause and resolution of bugs to determine if the change was made correctly and according to best practices. In addition, prefix review (PFR) meetings are held every four weeks, prior to a Hotfix deployment, in which groups of team seniors perform peer reviews on changes. During these meetings, groups of team seniors go through a HotFix checklist list to review and approve the changes, prior to implementation. Further, management approval is captured in a HotFix checklist prior to final implementation. Only authorized users have access to promote changes to the production environment once they have been approved. Finally, the development, QA testing, and production environments are physically and logically separated from one another to segregate production data from test and development environments.
Aries also utilizes version control software for application changes which is capable of rollback to a previous version if issues arise. In addition, access to write to the version control software is restricted to user accounts

accessible by authorized development personnel without access to production systems. Furthermore, access to promote changes to the production environment is restricted to authorized users.

Physical Security

Physical access to and within the office facility is restricted by proximity badges. Reviews of active badges and physical access permissions are performed as a component of the semi-annual user access review performed by management. NaviSite and Cyrus One are responsible for restricting physical access to data center facilities.

Enterprise Monitoring

Aries uses enterprise and security monitoring applications to monitor the production network for issues that could affect the availability of production systems. The applications display on-screen dashboard alerts which show the overall health of the system and alert the network monitoring team when issues or potential issues are identified. Furthermore, the monitoring tools are configured to send automatic e-mail notifications in the event of certain types of issues. Aries conducts meetings on a monthly basis to discuss operational activities and plans, review system availability, and review service level agreement (SLA) reports.

Data Backup and Disaster Recovery

To help ensure the availability and recoverability of backup data, formal policies and procedures around the data backup and recovery process have been established. Automated backups are performed by scheduled jobs which take incremental backups every six hours and a full backup each week, as well as write backups to tape bi-weekly. The backup system is configured to send alerts via e-mail to the network monitoring team at the end of each job to identify whether the backup was successful or failed. Failed backups are manually rerun to completion. Management uses a third-party media vaulting specialist to securely store backup media at an offsite location. IT personnel perform backup restoration testing of both the production data (customer data) and corporate data (internal documents, SharePoint documents, etc.) backups on a monthly basis. Disaster recovery plans are implemented to guide personnel in the procedures required to resume operations in the event of an unexpected event threatening business operations. In addition, the disaster recovery plan is tested annually to help ensure the disaster recovery plan operates as intended.

Incident Response

Incident response procedures are in place and to guide personnel throughout the incident response process including remediation of the incident, restoration of operations, communication protocols, and lessons learned. A SIEM application is implemented to monitor the in-scope systems for possible or actual security events and alert security personnel via e-mail when predefined events are detected. Reported or detected security incidents are tracked within a ticketing system until resolved.

System Monitoring

A log monitoring system is utilized to monitor and log events such as logons and configuration changes for certain in-scope windows systems. Similarly, enterprise monitoring applications are in place and configured to alert IT and operations personnel via e-mail when predefined thresholds are exceeded. In addition to monitoring internal factors, an IPS is utilized to analyze and report network events and to block suspected or actual network security breaches from external factors. Also, a SIEM application logs and alerts IT personnel in the event of a firewall configuration change.   Firewall rulesets are reviewed semi-annually to help ensure that only necessary connections are configured. Further, web application vulnerability scans are performed semi-annually using third-party scanning tools to identify threats and assess their potential impact to system security, availability, and confidentiality. Security vulnerabilities found during the assessment are monitored through resolution to help ensure Aries meets its commitment to providing customers a secure and reliable service. Lastly, management holds security meetings on a monthly basis to communicate departmental performance and address operational problems.

Data

Customers control the data in which they input into the Editorial Management system. Each customer owns its data and workflows. No customer has the ability to see another customer’s data. This data segregation is

adherent at the system and organizational level. All customer data is classified as confidential. Parent company personnel are also not authorized to access data or content on the segregated Aries network.
The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Customer/Journal (Meta/Submission)	Customer owned data is available through Aries SaaS application Editorial Manager	Company Confidential

Subservice Organizations

The data center hosting services provided by NaviSite and Cyrus One were not included within the scope of this examination. The following table presents the applicable Trust Services criteria that are intended to be met by controls at NaviSite and Cyrus One, alone or in combination with controls at Aries Systems, and the types of controls expected to be implemented at NaviSite and Cyrus One to meet those criteria.

Control Activity Expected to be Implemented by NaviSite and Cyrus One	Applicable Trust Services Criteria
NaviSite and Cyrus One are responsible for monitoring physical access to data center facilities.	CC6.3, CC6.4, CC7.2
NaviSite and Cyrus One are responsible for ensuring environmental protection controls are in place to meet Aries' availability commitments and requirements at their respective data centers.	A1.2

Management's Response to Suitability of Design Qualification

Security Category

Suitability of Design Qualification	
The description of the Editorial Manager system does not specify how the potential for fraud is considered when assessing risks to the achievement of objectives. As a result, controls were not suitability designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved as of June 30, 2019, based on trust services criterion CC3.3 which states, "The entity considers the potential for fraud in assessing risks to the achievement of objectives."	
Management's Response:	At the time of report preparation, subsequent to the examination date, the consideration of fraud has been added for consideration in the risk assessment process.