Report

SAP SE
Walldorf, Germany

Report on Ariba Inc.'s assertion
for the period from January 1, 2014 through June 30, 2014

WebTrust assurance service according Security, Confidentiality, Processing Integrity, and Availability

Engagement: 0.0712031.013

Independent Assurance Report

To SAP SE, Walldorf, Germany

I. Scope

We have examined Ariba's Assertion that during the period January 1, 2014 through June 30, 2014, Ariba, Inc. (Ariba) maintained effective controls over its hosted application environment (referred to as "the System"), which consists of the following applications:

- Ariba Network (AN), accessible from https://service.ariba.com
- Ariba Sourcing (AES), accessible from https://www.sourcingservice.com
- Ariba Analysis (ANL), accessible from https://www.sourcingservice.com
- Ariba Sourcing/Ariba Category Management/Ariba Analysis (collectively, S2), accessible from https://www.sourcingservice.com
- Ariba Discovery, accessible from http://discovery.ariba.com
- On-Demand versions of: 1) Sourcing, 2) Contract Management, 3) Supplier Management, and 4) Spend Visibility (collectively, S4), accessible from https://s1.ariba.com
- On-Demand versions of 1) Procure-to-Pay, 2) Travel and Expense, and 3) Invoice (collectively, SSP), accessible from https://s1.ariba.com,

to provide reasonable assurance that, based on the AICPA/CICA Trust Services Security, Confidentiality, Processing Integrity, and Availability criteria,

- the system was protected against unauthorized access (both physical and logical);
- information designated as confidential was protected by the system as committed or agreed;
- the system processing was complete, accurate, timely and authorized;
- the system was available for operation and use as committed or agreed; and
- Ariba complied with its commitments regarding security, confidentiality, processing integrity, and availability.

II. Ariba's Responsibility

This Assertion is the responsibility of Ariba's Management. Furthermore, Ariba is responsible for preparing the Description of the System, providing the services covered by the description, and specifying, implementing, and documenting the controls to meet the applicable trust services criteria.

III. Practitioner's Responsibility

Our responsibility is to express a conclusion based on our work performed. We conducted our work in accordance with International Standard on Assurance Engagements 3000, "Assurance Engagements Other Than Audits or Reviews of Historical Financial Information" issued by the International Auditing and Assurance Standards Board (IAASB). This Standard requires that we comply with ethical requirements and plan and perform the assurance engagement, under consideration of materiality, to express our conclusion with reasonable assurance.

The procedures selected depend on the practitioner's judgment. Our procedures included

(1) obtaining an understanding of Ariba's relevant security, confidentiality, processing integrity, and availability controls of the System,

(2) testing and evaluating the operating effectiveness of the controls,

(3) testing compliance with Ariba's commitments regarding the security, confidentiality, processing integrity and availability of its system, and

(4) performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

IV. Inherent Limitations

Due to the inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projections 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 system or controls, the failure to make needed changes to the system or controls, or deterioration in the degree of effectiveness of the controls.

V. Conclusion

In our opinion, in all material respects, Ariba's Assertion referred to above is fairly stated, in all material respects, based on the AICPA/CICA trust Services Criteria for Security, Confidentiality, Processing Integrity, and Availability.

Ariba's use of the WebTrust Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

VI. Restricted Use and Terms of Engagement

Our report is intended solely for the information and use of SAP SE and Ariba Inc. User entities of Ariba's hosted application environment (during some or all of the period from January 1, 2014 to June 30, 2014) and prospective user entities should have sufficient knowledge and understanding of the nature of the service provided by Ariba Inc., how Ariba's system interacts with user entities, of internal control system and its limitations, of the applicable trust services criteria and the risks, that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

We issue this report solely on the basis of the engagement agreed with the SAP SE, and this report is intended solely for the information and use of SAP SE and Ariba Inc. We do not accept any liability, responsibility or duty of care towards anyone other than SAP SE and Ariba Inc. Any deviating conditions shall be subject to a prior written agreement with us. Furthermore, the aforementioned conditions shall not apply in cases of willful behavior (*vorsätzliches Verhalten*).

December 12, 2014

PricewaterhouseCoopers
Aktiengesellschaft
Wirtschaftsprüfungsgesellschaft

Markus Vehlow

Heino Wehran
Wirtschaftsprüfer
(German Public Auditor)

Ariba's Assertion

The management of Ariba, Inc. ("Ariba") makes the following assertion pertaining to its hosted applications environment consisting of the following applications (collectively referred to as the "system"):

- Ariba Network (AN), accessible from https://service.ariba.com
- Ariba Sourcing (AES), accessible from https://www.sourcingservice.com
- Ariba Analysis (ANL), accessible from https://www.sourcingservice.com
- Ariba Discovery, accessible from http://discovery.ariba.com
- Ariba Sourcing 1 Category Management 1 Ariba Analysis (collectively, S2), accessible from https://www.sourcingservice.com
- On-demand versions of Sourcing, Contract Management, Supplier Management and Spend Visibility (collectively, S4), accessible from https://s1.ariba.com
- On-demand versions of Procure-to-Pay, Travel and Expense, and Invoice (collectively, SSP), accessible from https://s1.ariba.com

Ariba maintained effective controls during the period January 1, 2014 to June 30, 2014, to provide reasonable assurance that based on the AICPA/CICA Trust Services Criteria for Security Confidentiality, Processing Integrity, and Availability:

- The system is protected against unauthorized access (both physical and logical);
- Information designated as confidential is protected as committed or agreed;
- System processing is complete, accurate, timely and authorized;
- The system is available for operation and use as committed or agreed; and
- Ariba complied with its commitments regarding security, confidentiality, processing integrity, and availability.

The attached description identifies those aspects of the system covered by our assertion.

December 15, 2014

SAP SE and Ariba Inc.
Ralph Salomon
Head of Security, Processes and Compliance Office – Cloud & Infrastructure Delivery

Description of Hosting Application Environment

1. Background

Ariba, Inc. is a leading provider of on-demand spend management solutions. Ariba's mission is to transform the way companies of all sizes, across all industries, and geographies operate by delivering technology, service, and network solutions that enable them to holistically source, contract, procure, pay, manage, and analyze their spend and supplier relationships. Delivered on demand, Ariba's enterprise class offerings empower to achieve greater control if their spend and drive continuous improvements in financial and supply-chain performance.

2. Controls Framework, Risk Assessment, and Monitoring

The control environment reflects management's directive to establish Ariba's security policies, procedures and controls. Ariba's organizational structure, separation of job responsibilities by departments, roles and business functions along with documentation of policies and procedures are the methods used to define and implement operational controls. Ariba's control environment begins with the highest level of the company wherein executive and senior management play an integral role in setting the tone from the top and their direct leadership and example establishes integrity and ethics, which are part of Ariba's corporate culture.

Ariba's internal controls framework is based on two industry standards. The first is the WebTrust/ Trust Services criteria as propagated by the American Institute of Certified Public Accountants (AICPA), which includes criteria based on the principles of Security, Confidentiality, Processing Integrity and Availability. The second is the Payment Card Industry Data Security Standard (PCI-DSS). Ariba completes third party assessments against both of these standards on a regular basis.

Ariba has a security audit function within its Information Security Department. The security audit function uses the WebTrust and PCI-DSS standards as the basis for internal reviews and re-ports. Many of the controls are reviewed on a regular basis, either monthly or quarterly to ensure continued compliance outside of the semi-annual independent WebTrust examination and annual PCI-DSS assessments. Reporting on these controls has been incorporated into the monthly Information Privacy and Security Board meeting. In addition, Ariba management conducts an annual Risk Assessment based on the ISO 27002 standard. The internal audit function also manages monthly vulnerability scans as well as ad-hoc penetration tests and ethical hacks executed by Ariba customers.

3. Security Management and Monitoring

A dedicated Information Security Department has been established to assist with entity-wide compliance with internal information security controls. This department reports through the Chief Information Officer. In addition, Ariba has established the Information Privacy and Security Board which is described below.

A formal Information Security awareness program is in place. This program consists of an Ariba-wide Information Privacy and Security training program and quarterly Awareness emails. Completion of training is required upon commencement of employment, and then again on an annual recurring basis. Status of training completion is reviewed monthly at the Information Privacy and Security Board meeting.

Instances of employee non-compliance with Information Security policies are escalated to the Human Resources department and the Information Privacy and Security Board. Depending on the severity of the incident, an investigation is conducted and the employee is issued a formal warning or terminated.

Procedures exist to identify, report, escalate, and act upon system security alerts, defects and incidents.

The process for customers and external users to inform Ariba of possible security breaches and other incidents is communicated via a web portal.

Ariba's security commitments and required security obligations of its customers and web users are communicated via the website, http://www.ariba.com/legal/ariba_security_policy.cfm.

Intrusion detection/prevention tools are used to identify, log, and report potential security breaches and other incidents. An automated script generates a daily intrusion detection report which is reviewed by management.

Ariba conducts periodic security reviews and vulnerability assessments. Results are analyzed and followed up by the Information Security Department.

Customers and external users of the Ariba applications are able to report and track security related events through the Ariba Customer Support web portal. Appropriate communication and escalation plans are in place to insure that issues are resolved in a timely manner and that management oversight and involvement are maintained. The Information Security Department participates in the review and approval of the architecture and design specifications for new systems development and/or acquisition to ensure consistency with the entity's security objectives, policies, and standards.

Within the Ariba Engineering and Hosting Operations department a Change Control committee has been established to review, evaluate and promote the installation of hardware and security patches within the production environment. Appropriate testing and documentation are maintained to ensure compliance with Ariba's availability commitments and security standards.

Ariba has in place an Information Privacy and Security Board that is accountable and reports to Ariba Executive Management. Membership consists of representatives from all departments within Ariba. The mission of the Ariba Information Privacy and Security Board is to define, revise and approve policies which guide information privacy, security and confidentiality programs across the company. Likewise the Board serves to approve and enforce specific actions which have potential impact on information privacy, security and confidentiality beyond one function-al area. In addition, the Ariba Information Privacy and Security Board serves as the advisory and consultative body for all functions within Ariba on information privacy, security and confidentiality.

This board is chaired by the Ariba Chief Information Security Officer who establishes and communicates the agenda and meeting minutes to all participants. Agenda items include, but are not limited to, the following:

- current status of independent third party audits;
- the status of the Ariba Security Awareness Training program;
- the review of reports for critical control objectives delivered by different departments such as Human Resources for background checks for new hires, access control terminations of production access measured against Human Resources report for terminated employees and employees whose role has changed;
- corporate IT anti-virus status;
- Data Protection Agency registrations in relation to Safe Harbor;
- security hot fix and defect tracking submitted by Engineering; and
- security incident status to include formal closure by the board.

4. Infrastructure

The Ariba systems are co-located within regional data centers. Ariba uses an Equinix data center in San Jose, CA for North America and a TeleCity data center in Amsterdam for Europe. Secondary redundant data centers are located in an Ariba operated facility in Pittsburgh, PA for North America and an SAP operated data center in St. Leon Rot, Germany. Ariba is responsible for maintaining the software and hardware components of the system. Ariba uses Cogent and Internap networks as Internet Service Providers (ISPs) for connectivity to the Internet.

The main Ariba-maintained hardware and software components used to power Ariba include:

- web servers
- application servers
- database servers
- file servers
- load balancers
- switches and routers
- firewalls
- internet connections
- tape backup hardware

5. Software

Ariba solutions are deployed as a Software-as-a-Service (SaaS) system. Ariba hosts multiple customers on a load-balanced farm of identical instances, with each customer's data kept logically segregated, and with configurable metadata providing a unique user experience and feature set for each customer. The Ariba SaaS system is scalable to a large number of customers, because the number of servers and instances on the back end can be increased or decreased as necessary to match demand, without requiring additional re-architecting of the application, and changes or fixes can be rolled out to thousands of tenants as easily as a single tenant.

Ariba spend management is a Java based, N-tiered solution that leverages open standards, intranet and internet technology to deliver a broad range of functionality. Ariba was built using open standards such as Java, XML, HTTP(S), HTML and JDBC to enable support for a variety of computing platforms.

Ariba is a thin client solution. The Ariba client runs in a browser and uses HTML and JavaScript for presentation. Ariba uses an ActiveX plug-in only for its upstream solutions; its downstream solutions require no client-side software, plug-ins or applets. The client browser communicates with the web server tier using HTTPS over any connection to the Internet. Ariba supports Internet Explorer, Firefox, and Safari browsers on Windows and Mac platforms.

6. People

Ariba has a staff of approximately 2,700, with global offices in 21 countries, including North and South America, Europe, Asia/Pacific and Australia. This staff supports the Ariba Commerce Cloud for companies of all sizes across all industries by providing:

- On-demand technology to optimize the complete commerce lifecycle – from source-to settle and market-to receipt
- A web-based community to efficiently discover, connect and collaborate with a global network of trading partners
- Capabilities to augment internal resources and skills with always-on expertise and commerce services

7. Procedures

The services covered by this system description include:

- Ariba Network (AN)
- Ariba Sourcing (AES)
- Ariba Analysis (ANL)
- Ariba Discovery
- Ariba Sourcing / Category Management / Analysis (collectively, S2)
- On-demand versions of Sourcing, Contract Management, Supplier Management and Spend Visibility (collectively, S4); and
- On-demand versions of Procure-to-Pay, Travel and Expense, and Invoice (collectively, SSP)

These services are supported by Ariba's Information Technology Operations Department, which supports Ariba 24 hours a day, 7 days a week. The key support services provided by the Operations department include:

- Security Management and Monitoring
- Logical Security
- Physical Security
- Problem Management
- Systems Development and Change Management
- Backup and Recovery
- Organizational Management
- Invoice Payment Processing
- Confidentiality
- Availability

8. Data

Data for Ariba services may include one or more of the following customer data:

- Sourcing Data
- Category Management Data
- Analysis Data
- Contracting Data
- Invoice Data
- Error and suspense logs
- Transmission records
- System and security files

Processing integrity of invoice transactions is maintained by business rules that are defined by customers and executed by Ariba's automated system.