System and Organization Controls (SOC 1®) Type 2

Report on Managements Description of SAP's Ariba System and on the Suitability of the Design and Operating Effectiveness of Controls

For the Period October 1, 2022 to September 30, 2023

SAPSE

January 2024

THE BEST RUN SAP

Table of Contents

Section I

Independent Service Auditor's Report

Provided by KPMG LLP

KPMG

KPMG LLP
1601 Market Street
Philadelphia, PA 19103-2499

Independent Service Auditors’ Report

Management of SAP SE:

Scope

We have examined management of SAP SE’s (SAP) accompanying description of its Ariba System (the System) for processing user entities’ transactions throughout the period October 1, 2022 to September 30, 2023 titled “Management of SAP’s Description of its Ariba System” (the Description) and the suitability of the design and operating effectiveness of the controls included in the Description to achieve the related control objectives stated in the Description, based on the criteria identified in “Management of SAP SE’s Assertion” (the Assertion). The controls and control objectives included in the Description are those that management of SAP believes are likely to be relevant to user entities’ internal control over financial reporting, and the Description does not include those aspects of the System that are not likely to be relevant to user entities’ internal control over financial reporting.

The information included in Section V, “Other Information Provided by Management of SAP”, is presented by management of SAP to provide additional information and is not a part of the Description. Information about SAP’s management’s responses to exceptions identified in the report has not been subjected to the procedures applied in the examination of the Description and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the Description and, accordingly, we express no opinion on it.

SAP uses the subservice organizations identified in Section III to perform some of the services provided to user entities that are likely to be relevant to those user entities’ internal control over financial reporting. The Description includes only the control objectives and related controls of SAP and excludes the control objectives and related controls of the subservice organizations. The Description also indicates that certain control objectives specified by SAP can be achieved only if complementary subservice organization controls assumed in the design of SAP’s controls are suitably designed and operating effectively, along with the related controls at SAP. Our examination did not extend to controls of the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls assumed in the design of SAP’s controls are suitably designed and operating effectively, along with related controls at SAP. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization’s Responsibilities

In Section II, management of SAP has provided the Assertion about the fairness of the presentation of the Description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description. SAP is responsible for preparing the Description and Assertion, including the completeness, accuracy, and method of presentation of the Description and Assertion, providing the services covered by the Description, specifying the control objectives and stating them in the Description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the Assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the Description.

Service Auditors’ Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and in accordance with International Standard on Assurance Engagements 3402, *Assurance Reports on Controls at a Service Organization,* issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in the Assertion, the Description is fairly presented and the controls were suitably designed and operated effectively to achieve the related control objectives stated in the Description throughout the period October 1, 2022 to September 30, 2023. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our qualified opinion.

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

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description
- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved
- evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion.

We are required to be independent and to meet our other ethical responsibilities in accordance with the relevant ethical requirements in the United States of America relating to the examination engagement. We have complied with those requirements. We have also applied the statements on quality control standards established by the American Institute of Certified Public Accountants and accordingly maintain a comprehensive system of quality control. The firm also applies International Standard on Quality Management 1 which requires the firm to design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Inherent Limitations

The Description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the System that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives stated in the Description, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in Section IV.

Basis for Qualified Opinion

In Section III, SAP states that users' access is removed timely upon termination. However, the control to remove access for terminated users did not include procedures to monitor that the job which updates the identity access management system processes termination data from the employee and external worker systems on a timely basis. Also as stated in Section III, effective April 1, 2023, SAP implemented a quarterly review control to identify and assess post-termination login activity and review inappropriate events for internal employees and external workers. Consequently, the controls were not suitably designed or operating effectively during the period of October 1, 2022 to March 31, 2023 to achieve the control objective "Controls provide reasonable assurance that logical access to production systems and data files is restricted to authorized personnel."

Qualified Opinion

In our opinion, except for the matter described in the preceding paragraph, in all material respects, based on the criteria described in the Assertion:

- the Description fairly presents the System that was designed and implemented throughout the period October 1, 2022 to September 30, 2023 the controls related to the control objectives stated in the Description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2022 to September 30, 2023 and subservice organizations and user entities applied the complementary controls assumed in the design of SAP's controls throughout the period October 1, 2022 to September 30, 2023
- the controls operated effectively to provide reasonable assurance that the control objectives stated in the Description were achieved throughout the period October 1, 2022 to September 30, 2023 if complementary subservice organization controls and complementary user entity controls, assumed in the design of SAP's controls, operated effectively throughout the period October 1, 2022 to September 30, 2023.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of management of SAP, user entities of SAP's System during some or all of the period October 1, 2022 to September 30, 2023, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

KPMG LLP

Philadelphia, PA
January 5, 2024

Section II

Management of SAP SE's Assertion

Provided by SAP

Management of SAP SE’s Assertion

We have prepared the accompanying description of SAP SE’s (SAP) Ariba System (the System) for processing user entities’ transactions throughout the period October 1, 2022 to September 30, 2023 titled “Management of SAP’s Description of Its Ariba System” (the Description) for user entities of the System during some or all of the period October 1, 2022 to September 30, 2023, and their auditors who audit and report on such user entities’ financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the System themselves, when assessing the risks of material misstatement of user entities’ financial statements.

SAP uses the subservice organizations identified in Section III to perform some of the services provided to user entities that are likely to be relevant to those user entities’ internal control over financial reporting. The Description includes only the control objectives and related controls of SAP and excludes the control objectives and related controls of the subservice organizations. The Description also indicates that certain control objectives specified in the Description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively along with the related controls at SAP. The Description does not extend to controls of the subservice organizations.

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls assumed in the design of SAP’s controls are suitably designed and operating effectively, along with related controls at SAP. The Description does not extend to controls of the user entities.

In Section III, we state in our Description that users’ access is removed timely upon termination. However, the control to remove access for terminated users did not include procedures to monitor that the job which updates the identity access management system processes termination data from the employee and external worker systems on a timely basis. We also state in Section III that, effective April 1, 2023, we implemented a quarterly review control to identify and assess post-termination login activity and review inappropriate events for internal employees and external workers. Consequently, the controls were not suitably designed or operating effectively during period of October 1, 2022 until March 31, 2023 to achieve the control objective “Controls provide reasonable assurance that logical access to production systems and data files is restricted to authorized personnel.”

Except for the matter described in the preceding paragraph, we confirm, to the best of our knowledge and belief, that:

a) The Description fairly presents the System made available to user entities of the System during some or all of the period October 1, 2022 to September 30, 2023 for processing their transactions as it relates to controls that are likely to be relevant to user entities’ internal control over financial reporting. The criteria we used in making this assertion were that the Description

   i. presents how the System made available to user entities of the System was designed and implemented to process relevant user entity transactions, including, if applicable,

      (1) the types of services provided, including, as appropriate, the classes of transactions processed;

      (2) the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the System;

      (3) the information used in the performance of the procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities;

(4) how the System captures and addresses significant events and conditions other than transactions;

(5) the process used to prepare reports and other information for user entities;

(6) services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them;

(7) the specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the service organization's controls;

(8) other aspects of our control environment, risk assessment process, information and communication (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

ii. includes relevant details of changes to SAP's System during the period covered by the Description.

iii. does not omit or distort information relevant to SAP's System, while acknowledging that the Description is prepared to meet the common needs of a broad range of user entities of the System and their auditors, and may not, therefore, include every aspect of the System that each individual user entity of the System and its auditor may consider important in its own particular environment.

b) The controls related to the control objectives stated in the Description were suitably designed and operated effectively throughout the period October 1, 2022 to September 30, 2023 to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of SAP's controls throughout the period October 1, 2022 to September 30, 2023. The criteria we used in making this assertion were that:

i. the risks that threaten the achievement of the control objectives stated in the Description have been identified by management of SAP;

ii. the controls identified in the Description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the Description from being achieved; and

iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

SAP SE

January 5, 2024

Section III

Management of SAP's Description of its Ariba System

Provided by SAP

Corporate Introduction

Overview of Operations

Company Background

With a 51 year history of innovation, SAP is a market leader in enterprise application software, offering companies of all sizes and in all industries the Intelligence Enterprise solution. With more than 400,000 customers in more than 180 countries, the SAP Group employs more than 105,000 staff in over 140 countries. SAP's end-to-end suite of applications and services enables customers to operate profitably and continuously adapt.

Description of the Services Provided

SAP Ariba solutions enable customers to source, contract, procure, pay, manage, and analyze spend and supplier relationships. Customers use the applications to control spend and drive continuous improvements in financial and supply-chain performance.

SAP Ariba provides the following solutions

- SAP Ariba Strategic Sourcing solutions is used to manage entire sourcing, contracting, and spend analysis processes for all types of procurement. Customers can create a sourcing project or event.
- SAP Ariba Procurement Solutions are used to manage spend-related processes. Additionally, customers can integrate the solution to their back-end system to process invoices and payments.
- SAP Business Network is a hosted service that enables suppliers and buyers to conduct transactions over the internet.
- SAP Ariba Cloud Integration Gateway allows customers to integrate SAP ERP and SAP S/4HANA back-end systems with trading partners and SAP Ariba solutions.

References to “SAP Ariba” throughout this report refer to the Line of Business (LoB) within SAP.

Ariba System Topology

The SAP Ariba System is offered as a public cloud, multi-tenant Software-as-a-Service (SaaS). SAP Ariba hosts multiple customers on a load-balanced farm of identical instances, with each customer's data kept logically segregated, and with configurable metadata for customers. The SAP Ariba Cloud Solutions are 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. Changes or fixes can be rolled out to thousands of tenants. In SAP Ariba's technical terminology, the term “tenant” is rarely used; instead, “realm” is used in the context of the on-demand buyer applications and “customer accounts” is used in reference to the SAP Ariba Network. SAP Ariba uses the term “tenant” to refer to the general concepts, which apply to both cases.

Ariba System Architecture

The main SAP Ariba-maintained hardware and software components used in the SAP Ariba System include:

- Web servers
- Application servers
- Database servers
- File servers
- Load balancers
- Switches and routers
- Firewalls
- Internet connections

The SAP Ariba Cloud Solutions environment is designed as a three-tiered model with a web UI layer, a business application layer, and a database layer. Security zones are established based on this three-tier architecture, along with an internet-facing Demilitarized Zone (DMZ) and a secured back-office portal used by SAP Ariba personnel to maintain the environment and perform problem management as required. The communication protocols used between the systems are TCP/IP-based.

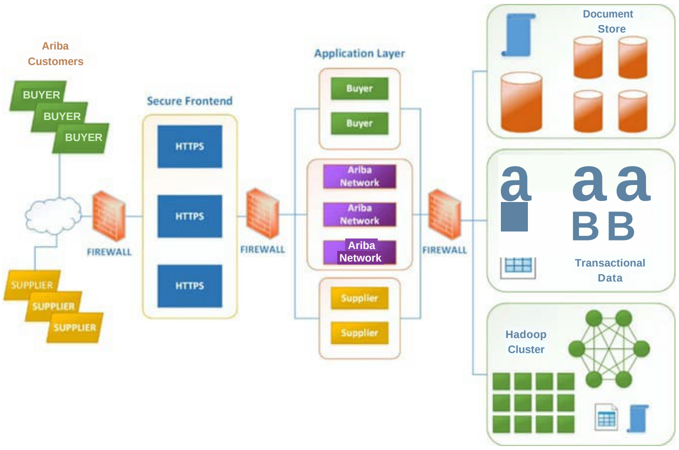


Figure 1: Logical Network Diagram

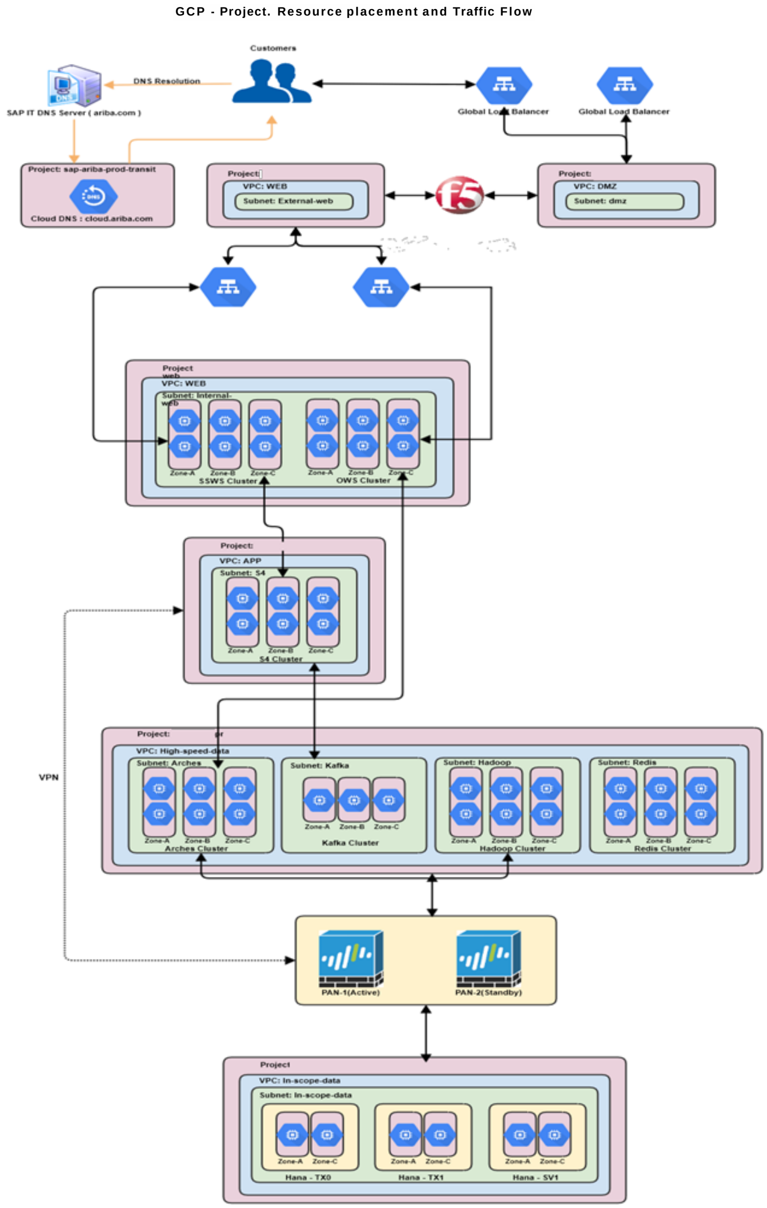


Figure 2: Logical Network Diagram for SAP Ariba on Google Cloud Platform

The SAP Ariba core stack is hosted on Google Cloud Platform in Australia, Europe, and Japan. The Google Cloud Platform (GCP) resource hierarchy is the mechanism for organizing and managing resources in GCP. The Organization is the root of the Google Cloud resource hierarchy and does not have a parent. Folders are a grouping mechanism under an organization which can have sub-folders. Projects are located under a folder and contain Google Cloud resources. Resources are at the lowest level and consist of Google Cloud services such as Virtual Private Cloud (VPC), Compute Engine, and Cloud Storage.

SAP Ariba will have a folder underneath the SAP organization. The following illustrates the logical hierarchy for SAP Ariba GCP resources:

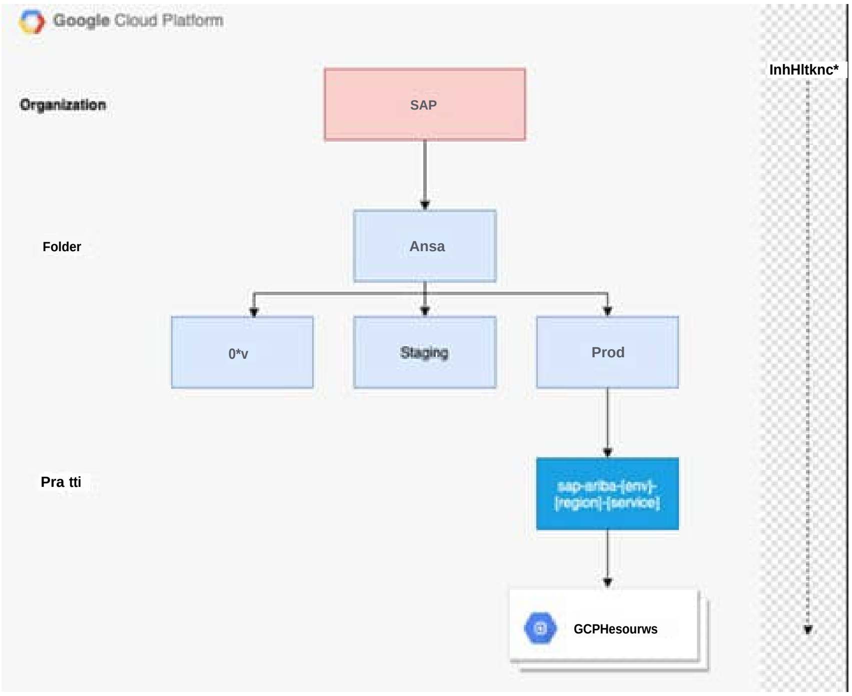


Figure 3: Logical hierarchy

SAP Ariba Cloud Integration Gateway

The SAP Ariba Cloud Integration Gateway facilitates the integration of buyers' SAP ERP or SAP S/4HANA systems with Ariba Network.

SAP Ariba Mobile Architecture

Security features in the SAP Ariba mobile app help protect data and communications between the application and the SAP Ariba Cloud. The SAP mobile architecture, as displayed in the figure below, helps ensure that proper security and authentication are in place.

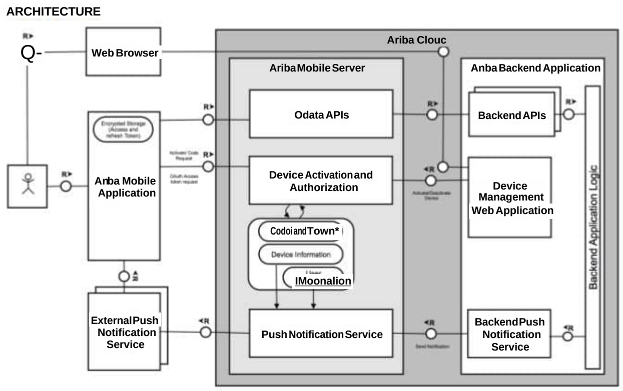

ARCHITECTURE
R
Q-
Web Browser
Ariba Clouc
AribaMobileServer
AnbaBackendApplication
Odata APIs
Backend APIs
Encrypted Storage (Access and refresh Token)
Anba Mobile Application
Device Activationand Authorization
Device Management Web Application
CodoiandTown*
Device Information
IMoonalion
Backend Application Logic
ExternalPush Notification Service
PushNotificationService
BackendPush Notification Service

Figure3: Mobile InfrastructureArchitectu re Diagram

Figure 4: Mobile Architecture

Information Systems Security

This section describes the end-to-end security architecture model for the SAP Ariba solutions. SAP Ariba Operations has standardized operating system installations based on predefined security policies. Servers are configured with just the applications and services required to run the server as designed. Services that are not required are disabled and binary files that are not required for operations are removed, which reduces the total number of vulnerabilities a system may have.

SAP Ariba Operations' standardized installation process also helps ensure that servers of the same type are configured in the same manner, utilizing a process that initiates an upgrade to system binaries across all systems. Based on the system type, the configuration will remain the same. If one server type needs to receive a patch for a vulnerable binary file, that patch is pushed to all systems of that server type. If that binary exists on all systems, it is patched across all systems. Patches are then included in the build process as well so that future systems built will follow security standards. SAP Ariba uses this configuration process to harden the operating system prior to implementing additional controls, as detailed below.

Web Servers. Authentication using a unique login/password pair is required when SAP Ariba users attempt to access corporate profile information, initiate a transaction, or retrieve information saved from a previous session. HTTPS (HTTP over TLS) is based on a minimum 128-bit encryption and is used for secure communications between the web browsers and the web servers.

Load Balancers. SAP Ariba load balancers control traffic and provide optimal utilization of webservers. Although they are not considered a security component, the load balancers provide access control functionality to help ensure authorized traffic flow. Access control entries (ACEs) deny all traffic through the load balancers except traffic between the internal interface of the firewall and the external interface of the web servers. ACEs also deny traffic that is not using one of the required protocols for firewall-to-web server communications.

Monitoring Servers. SAP Ariba uses a centralized monitoring server for alerting capabilities. It monitors network traffic, processes system messages and alerts, application status and transaction status.

Routers. Routers are the primary networking components in SAP Ariba. They coordinate the delivery of data packets between the various system components while providing several essential security controls and features. Routers provide packet filtering by creating access control lists (ACLs) that define the types of data packets (protocol, source, and destination) allowed to pass through the router interfaces. Data packets that do not meet the criteria specified in the ACLs are rejected.

Firewalls. Firewalls separate the SAP Ariba corporate network from SAP Ariba infrastructure computers. Therefore, unauthorized SAP Ariba employees cannot access SAP Ariba data from the SAP Ariba corporate network infrastructure. Access is limited to specific roles or functions within SAP Ariba Operations. Additionally, access is managed on an exception basis whereby personnel need clearance to be authorized as external connections. Access is time-limited, after which re-authentication is required.

Intrusion Detection System. SAP Ariba uses network and host-based intrusion detection. This technology provides logging and alert capabilities to assist in the detection of malicious acts and misuse. Intrusion detection/prevention tools are used to identify, log, and report potential security breaches and other incidents. An automated script generates an intrusion alert which is reviewed by management.

Separation of Customer Data

In the SAP Ariba Cloud Solutions environment, tenants share certain resources; however, their private data is isolated. All tenants share the same version of the application software. This means that only one version of the application is deployed for production use in a data center. Multiple tenants share the same hardware resources, the same applications server instances, and the same storage. Even though resources are shared between tenants, the data of each tenant is always isolated. SAP Ariba stores the data of multiple tenants in the same database tables, separated by the tenants' organizational and user IDs.

Components of the System Used to Provide the Services

Infrastructure

SAP Ariba is deployed in different regions. It is deployed on Google Cloud Platform in North America, Europe, Japan and Australia . It is deployed on SAP Cloud Infrastructure in China, United Arab Emirates (UAE) and Kingdom of Saudi Arabia. Each regional data center hosts the full SAP Ariba application suite, including all SAP Ariba Procure-to-Pay and Strategic Sourcing applications. The SAP Business Network is considered to be a transit network, like the internet, supporting connectivity between organizations and serving as a central marketplace. This shared resource is housed in SAP Ariba's North America data centers and colocation data centers. Application connectivity between the sites in North America, Europe, China, the United Arab Emirates, the Kingdom of Saudi Arabia, Australia and Japan is over the public network with secure HTTPs connections.

Within each region, SAP Ariba has deployed two data centers that act as redundant pairs. These data centers are built in a warm stand-by configuration. At any point in time, customers interact with servers in a single data center while data is copied in near real time to the other. For GCP and SAP Cloud Infrastructure, the underlying physical infrastructure is managed by Google and SAP Cloud Infrastructure (SCI) respectively and the software and virtual components are managed by SAP Ariba. For the purposes of this report, GCP and SAP Cloud Infrastructure (SCI) are subservice organizations. Controls at the respective subservice organizations are not included in the scope of the report.

Global Region	Primary DC Operated by	Data Center ID	Location	Data Center ID	Secondary DC Operated by	Location
USA	Google Cloud Platform	XG1	Council Bluffs, Iowa	XGO	Google Cloud Platform	Las Vegas, Nevada
Australia	Google Cloud Platform	XGA	Sydney, Australia	XGA Zonal DR	Google Cloud Platform- Zonal level DR	Sydney, Australia
Europe	Google Cloud Platform	XGB	Frankfurt, Germany	XGH	Google Cloud Platform	Eemshaven, Netherlands
Japan	Google Cloud Platform	XG9	Tokyo, Japan	XGJ	Google Cloud Platform	Osaka, Japan
China	SAP Cloud Infrastructure	SHA3	Shanghai, China	SHA4	SAP Cloud Infrastructure	Shanghai, China
Kingdom of Saudi Arabia	SAP Cloud Infrastructure	RI1	Riyadh, Kingdom of Saudi Arabia	DM1	SAP Cloud Infrastructure	Dammam, Saudi Arabia

Global Region	Primary DC Operated by	Data Center ID	Location	Data Center ID	Secondary DC Operated by	Location
United Arab Emirates	SAP Cloud Infrastructure	DB1	Dubai, United Arab Emirates	DB2	SAP Cloud Infrastructure	Dubai, United Arab Emirates
China	GDS Services Ltd.	SH3	Shanghai, China	BJ1	Telstra/Pacnet	Beijing, China
North America	Equinix	SJ1	San Jose,	North America	Equinix	SJ1
United Arab Emirates	Equinix DX2	DB1	Dubai, United Arab Emirates	DM1	Mobily	Dammam, Saudi Arabia

Table 1: SAP Ariba Primary and Secondary Data Centers

The infrastructure providers are part of the SAP Supplier Management process and are required to fulfill the security requirements defined in the SAP Cloud Data Center Security Requirements that are part of the supplier contracts.

Software

The following table details the key software components that support the system:

Component	Description
Operating Systems	Linux operating systems
Databases	HANA and Postgres
Monitoring Systems	An in-house tool is used for bandwidth, utilization, uptime, and capacity monitoring and is configured to send real-time email notifications to Cloud Operations personnel when pre-defined thresholds are exceeded on monitored devices.
Active Directory (AD)	AD is used to store the user accounts and group membership to manage access to the production systems. Authorized users are required to have a username and password and have membership on the domain in order to access the production servers.
Safeguard	Safeguard is an IP tables-based firewall system between the SAP corporate network and the Ariba production network that was developed in-house. It applies rules to control authorization and privileges by using Safeguard groups.
Lightweight Directory Access Protocol (LDAP)	Open LDAP is a directory service protocol used to authenticate users using AD information.
Multifactor Authentication	RSA authentication manager is used for two-factor authentications to the production environment.
VPN	Big IP F5 is used for VPN connections for remote access.
Anti-Malware	TrendMicro is used as anti-malware on servers and McAfee is used as anti-malware on endpoints.
SIEM	Splunk used as a SIEM solution and is configured to provide security alerts and act as central log storage tool.
Security Code Review	Source code is maintained in GitHub and Perforce. Fortify is used for static security scans, Webinspector for dynamic security scans, and Whitesource and Black Duck for open-source vulnerability scans.

Component	Description
Intrusion Detection System	Palo Alto Next Gen firewalls are installed as an intrusion detection & prevention solution (IDS/IPS).
GCP Project Provisioning	Terraform is used to provision projects in GCP.
Configuration Management	Linux, along with Salt and CFEngine, is used to push changes to the production environment and manage cron jobs.
Network Management	Palo Alto Next Gen firewalls are deployed.

Table 2: Software

People

Team	Responsibilities
Cloud Engineering Service (CES)	Delivering a complete end-to-end cloud service to the customer, which includes infrastructure, hardware, cloud solution of choice, operations, maintenance, and customer service.
Executive Management	— Establishment of product vision — Oversight of company-wide activities — Attainment of business objectives — Commitment and assignment of leadership responsibilities for information security and data privacy
Product Management	— Working with CES teams to help ensure product improvements are tracked, implemented, and released in a timely manner — Working with customers to get feedback and gather requirements for product improvements
Sales Operations	— Client implementation, renewal, and account management — Monitoring and managing inbound and outbound data flows and related processes
Customer Support	- Single point of contact for customer issues - Day-to-day customer support - Monitoring and managing inbound and outbound data flows and related processes; involves internal departments such as Cloud Operations, Engineering, Information Security and Compliance teams as required
Information Security and Compliance	— Security program ownership, assignment of security responsibilities and policy management — Security monitoring and compliance — Vulnerability management and penetration testing — Organizational security awareness and training — Vendor management and compliance

Table 3: People

Procedures

SAP Global Security has developed the SAP Security Policy Framework, which comprises the security-relevant requirements and implementation guidelines for business units and subsidiaries of the company. The framework is built on the following structure:

- Security Policy: A high-level document that defines management strategy, expectations, and direction. It establishes the strategic goals and objectives that the organization strives to achieve in order to maintain the highest level of security.
- Security Standards: A document that defines the minimum requirements for adherence to a policy. These requirements can be met by executing the corresponding procedure(s).
- Security Procedures: A series of sequential tasks that are performed to achieve an outcome. Procedures can be the step-by-step instructions to implement a standard when appropriate.
- Security Good Practices: A checklist for employees to simplify the policy implementation process.

Refer to the “Overview of Processes” section for additional information on policies and procedures used across the various aspects of the control environment.

Data

The following describes the different types of data used by SAP Ariba Cloud solutions:

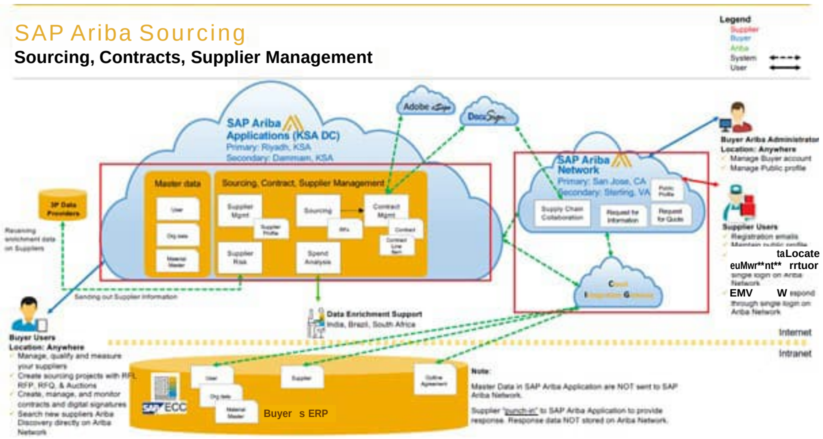
- Master Data: Master data are data that are relatively static and represent a common point of reference. Examples of master data in an SAP Ariba cloud solution are:
  - Employee (user) data
  - Organizational hierarchy and accounting data
  - Product information, including pricing
  - Payment terms
  - Supplier company name, address, and other identification information
  - Customer identification information
  - Currency information
  - Unit of measure information

The specific master data supported and required depends on the customer’s SAP Ariba cloud solution and business process requirement. For a full list of available master data, see the product documentation of the respective customer solution. Most master data can be imported and synced with the customer’s back-end system.

Transaction Data: Typical transactions in SAP Ariba cloud solutions include purchase orders, order confirmations, invoices, service sheets, and payment advice documents. A transaction describes a specific event, such as sending a purchase order to a supplier or alerting a supplier that payment of an invoice has been approved.

Project Data: Project data is a type of transaction data for SAP Ariba Strategic Sourcing solutions. Project data includes sourcing events such as requests for information (RFI), requests for proposal (RFP), or auction events or contract data consisting of contract workspaces, documents, clauses, and tasks.

The data flows for the main SAP Ariba applications are depicted in the figures below. The services within the red box are within the scope of the system covered by this report.

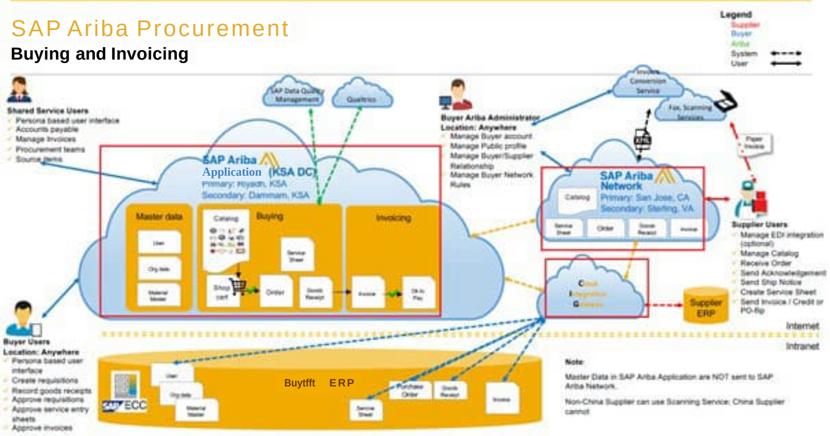


Note:

Master Data in SAP Ariba Application are NOT sent to SAP Ariba Network.

Supplier "punch-in" to SAP Ariba Application to provide response. Response data NOT stored on Ariba Network.

Figure 5: SAP Ariba Sourcing Data Flow

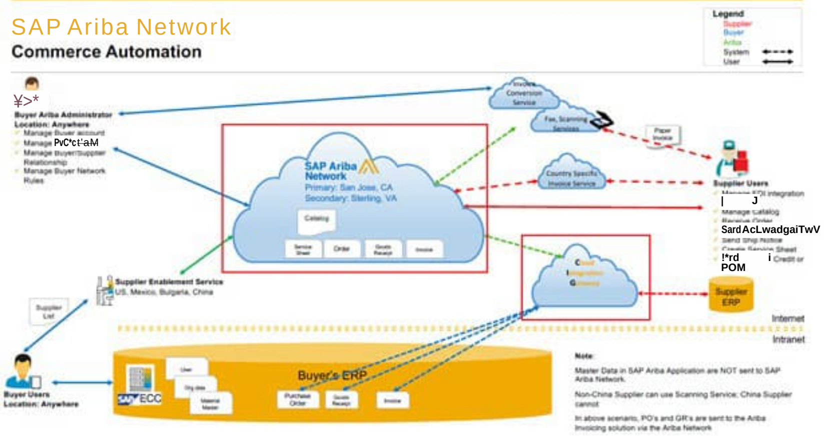


Note:

Master Data in SAP Ariba Application are NOT sent to SAP Ariba Network.

Non-China Supplier can use Scanning Service; China Supplier cannot

Figure 6: SAP Ariba Procurement Data Flow



Note:

Master Data in SAP Ariba Application are NOT sent to SAP Ariba Network.

Non-China Supplier can use Scanning Service; China Supplier cannot

In above scenario, PO's and GR's are sent to the Ariba Invoicing solution via the Ariba Network

Figure 7: SAP Ariba Network Data Flow

Significant Changes to the System During the Period

The following table details the relevant changes to the SAP Ariba system during the examination period.

Change	Description of Change
Inclusion of GCP into the Ariba report	As of April 1, 2023 Ariba System Supported by Infrastructure Managed by Google Cloud Platform was fully incorporated into Ariba System Supported by Infrastructure Managed by SAP. As a result the report and related system was simplified and now referred to as “Ariba System.” The nuances of the separate reports for the period October 1, 2022 through March 31, 2023 are captured throughout with time-bound language.
China Data Center Region	SAP Ariba applications were migrated from the China Data Center Region colocation data centers to SAP Cloud Infrastructure data centers as of December 3, 2022.
US Colocation Data Center Region	SAP Ariba applications were migrated from the US Data Center Region colocation data centers to Google Cloud Platform as of February 4, 2023.
UAE Data Center Region	SAP Ariba applications were migrated from the UAE Data Center Region colocation data centers to SAP Cloud Infrastructure data centers as of March 04, 2023.
Physical Security Controls	The physical security control objective is only in-scope for the period October 1, 2022 to March 4, 2023. As of March 5, 2023, all data centers are now co-location data centers that are carved out, as they fall under the SAP Cloud Infrastructure and Google Cloud Platform sub-service provider
PS02, PS03, PS03_Ger_R, PS03a, PS03a_R, PS04, PS05	These controls are out of scope for the audit period October 1, 2022 to March 4, 2023.
UAM04a_Ariba	The control was sunsetted effective July 23, 2023 and was replaced by the following two controls UAM04a_Internal_Leavers_Ariba and UAM04a_ External- Leavers_Ariba.
UAM04a_Internal_Leavers_Ariba	Control operated from July 24, 2023 to September 30, 2023.
UAM04a_ External- Leaver Ariba	Control operated from July 24, 2023 to September 30, 2023.
AS_AM0N4	Control operated from July 24, 2023 to September 30, 2023.
AS_AM0N5	Control operated from July 24, 2023 to September 30, 2023.
AS_AM0N6a	Control operated from July 24, 2023 to September 30, 2023.
AS_AM0N6b	Control operated from July 27, 2023 to September 30, 2023.
AS_AM0N7	Control operated from July 24, 2023 to September 30, 2023.

Change	Description of Change
HR05	Control operated from October 1, 2022 to September 30, 2023.
HR09	Control operated from July 17, 2023 to September 30, 2023.
UAM04_ Term_ Impact	Control operated from June 30, 2023 to September 30, 2023.
UAM04_ Changers_ Impact	Control operated from June 30, 2023 to September 30, 2023.
UAM04_PIT	Control operated from July 4, 2023 to September 30, 2023.

Subservice Organizations

Subservice organizations' compliance with SAP's security requirements is periodically reviewed and verified by SAP. For further information, please also refer to the Supplier Management Process as described in "Relevant Aspects of the Overall Control Environment".

Complementary Subservice Organization Controls

SAP uses subservice organizations to perform various functions that support the delivery of services. Certain control objectives can be met only if the subservice organization's controls, assumed in the design of SAP's controls, are suitably designed, and operating effectively along with related controls at SAP. The following is a description of services provided by subservice organizations. The controls relating to the infrastructure services provided by the subservice organizations GCP and SAP Cloud Infrastructure below have been carved out of the scope of this report.

Subservice Organization	Services Provided
SAP Cloud Infrastructure (SCI)	Infrastructure Provider: SAP Cloud Infrastructure (SCI) spearheads SAP's 4+1 strategy and supports the adoption and governance of all services deployed as part of SAP's Cloud Infrastructure Strategy. Specifically, this refers to the management of four public cloud hyperscalers, namely, Microsoft Azure, AWS, Google Cloud Platform and AliCloud (China) which is managed by the SAP Multi Cloud Team and 'Plus One', SAP's internal IaaS known as SAP Converged Cloud.
Google, LLC	Infrastructure Provider: Ariba runs on Google Cloud Platform. Google LLC accesses data to enable and operate the Google Cloud Platform, and to provide support and consulting.
Equinix EMEA (Europe, Middle East, and Africa)	Colocation Data Center Physical access only (no logical access). Provides only rack space; no access to personal data.
Equinix Inc.	Colocation Data Center Physical access only (no logical access). Provides only rack space; no access to personal data.
Etihad Eitsalat Company	Colocation Data Center Secondary Production/Disaster Recovery Data Centers: Physical access only (no logical access). Provides only rack space; no access to personal data.
(EEC.) - Mobily	Colocation Data Center Physical access only (no logical access). Provides only rack space; no access to personal data.
GDS	Colocation Data Center Secondary Production/Disaster Recovery Data Centers: Physical access only (no logical access). Provides only rack space; no access to personal data.

Table 4: Subservice Organizations

In the design of their internal procedures and controls, SAP has assumed the following procedures and controls in place at the subservice organizations:

Control Objectives	Controls Expected to be Implemented at Subservice Organizations
Backup and Restore	The hyperscaler and SAP Cloud Infrastructure (SCI) are responsible for establishing backup and recovery controls, including redundancy and encryption.
Change Management	The hyperscaler and SAP Cloud Infrastructure (SCI) are responsible for establishing procedures for the inventory of assets under their responsibility in order to record the required information throughout the asset lifecycle. The hyperscaler and SAP Cloud Infrastructure (SCI) are responsible for technical and organizational safeguards for Change Management of system components of the cloud service, including segregation of duties, testing and approval of changes. SAP Cloud Infrastructure is responsible for controls over the complete account lifecycle, from request to tracking and then removal, to support that the process is effective, controlled, and managed in line with governance standards and business demands.
Network and Communication Management	The hyperscaler and SAP Cloud Infrastructure (SCI) are responsible for implementing technical safeguard to detect and respond to network-based attacks and for maintaining account and customer segregation.
Physical Security	The hyperscaler and SAP Cloud Infrastructure (SCI) are responsible for implementing physical security and environmental safeguards and controls for premises, buildings, and data centers. Additionally, the hyperscaler is responsible for controls over proper operation of their physical environments and data centers.
User and Access Management	The hyperscaler and SAP Cloud Infrastructure (SCI) are responsible for implementing technical and organizational safeguards over access to systems components and such access is approved, created, maintained, reviewed, and terminated. Access to the production environment requires strong authentication mechanisms. SAP Cloud Infrastructure is responsible for controls for implementing technical and organizational safeguards to help ensure that access to systems components they are responsible for is approved, created, maintained, reviewed, and terminated. Access to production environment requires strong authentication mechanisms.

Table 5: Controls Expected to be Implemented at Subservice Organizations

Complementary User Entity Controls

SAP’s services have been developed on the assumption that specific controls and procedures are implemented by the customer (“user entity”). The application of such internal controls by customers is necessary for SAP to achieve its Control Objectives listed below.

This chapter describes those additional policies, procedures, and controls that are within the responsibility of the customer to complement the controls operated by SAP, as described in this report. The customer auditor should consider whether procedures and controls similar to those suggested by SAP are put into effect at the customer site.

In general, the customer is responsible for processes or a portion of the processes that were not covered by the contract between the customer and SAP. Customers are therefore responsible for verifying whether SAP’s services and the functionalities provided meet their general requirements.

The responsibilities of the customer are listed in the table below:

Control Objective	Complementary User Entity Controls
Change Management	Customers are responsible for communicating with SAP Ariba regarding the timing and implementation of changes to their systems.
Invoice Payment Processing	Customers are responsible for configuring custom business rules for invoice processing reconciliation and validating the error-free operation of custom business rules when implemented. Customers are responsible for controls over managing their own access control systems on their infrastructure in regard to the use of the SAP Ariba Network Open adapter and any other document exchange adapters supported by SAP Ariba. Customers are responsible for controls over making additions, changes, or deletions to the authorization list for access to the SAP Ariba Network Open adapter and any other document exchange adapters supported by SAP Ariba.
User and Access Management	As applicable, customers are responsible for maintaining their digital certificates as they apply to the use of the SAP Ariba solution and adhering to the certificates’ intended use. Customers are responsible for the proper configuration of their browser in order to interact with the Ariba system supported by infrastructure managed by SAP. Customers are responsible for controls for assigning authorized users are appointed as organizational administrators for granting user access to the Ariba system supported by infrastructure managed by SAP and optional features such as the SAP Ariba Mobile App. Customers are responsible for controls over configuring their Ariba system supported by infrastructure managed by SAP user accounts and shared secrets such that passwords or Personal Identification Numbers (PINs) are sufficiently strong and properly managed. Customers are responsible for controls over their passwords and PINs are kept confidential. Customers are responsible for notifying SAP Ariba of possible security breaches or incidents using a web form. Customers are responsible for leveraging SSO authentication. Customers are responsible for performing periodic access reviews of their user’s authorization to access the Ariba solution.

Table 6: Complementary User Entity Controls

Relevant Aspects of the Overall Control Environment

Control Environment

The control environment at SAP is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment include integrity and ethical values, management's commitment to competence, the organizational structure, the assignment of authority and responsibility, and the oversight and direction provided by the management of SAP.

SAP Code of Business Conduct

SAP defines standards for conduct in business, legal, and ethical matters carried out on a daily business. The Code of Business Conduct is reviewed and acknowledged by each employee as part of the new hire onboarding and annually thereafter. Employees are notified of amendments to the Code of Business Conduct via the corporate portal and email.

Corporate Governance

The SAP SE Supervisory Board ("Supervisory Board") is an independent governing and supervising body that provides oversight and strategic direction for the organization. The size and the composition of the Supervisory Board are determined by the Articles of Incorporation and the Agreement of the Involvement of the European Employees in SAP SE. SAP's Supervisory Board is comprised of members elected by the shareholders at their General Meeting and members representing the European employees of the SAP Group.

The Supervisory Board has defined a catalogue of skills and expertise collectively required of its members so that it possesses the knowledge, ability and professional experience required to properly perform its function.

The Supervisory Board has appointed committees to prepare its deliberations and implement resolutions. Information about each Supervisory Board member, and the Committees and their composition, is available on the company website.

On an annual basis, the status of internal controls is formally reported to management and the Supervisory Board. The report details assessment results, as well as related follow-up activities.

In addition, SAP has an independent Internal Audit function reporting to the Chief Financial Officer, the Chief Executive Officer of SAP SE, and the Supervisory Board's Audit and Compliance Committee. SAP's audit charter defines Internal Audit's purpose, authority, responsibility, and position. Internal Audit reports on the audit planning and the audit results to the Board of Directors on an at least annual basis. The audit program is developed following a risk-based approach and includes, amongst other areas, IT Security related topics.

Security Governance

The SGS (SAP Global Security) organization is led by SAP's Chief Security Officer, who reports directly to the CEO. SGS is responsible for protecting the brand, people, assets, intellectual property, customer data, and information technology of SAP from misuse or compromise.

SGS supports cross functional end-to-end security processes, by

- Providing a clearly defined Security Governance Model. The Model builds on SAP Global Security Governance Framework as well as the Operating Model for Security at SAP. It streamlines the interaction within SAP Global Security (SGS) and the alignments between SGS and key stakeholders. It comprises the management of day-to-day activities, the execution of key security projects as well as the interaction with critical stakeholders on an execution, steering, executive, and Board level.
- Defining an Operating Model for Security at SAP with clear roles and responsibilities. The Operating Mode defines how the security functions are delivered through the central security departments. It defines actions, sets priorities, assigns clear roles and responsibilities. Performs periodic reviews that identifies areas for improvements within SGS, Intelligent Enterprise Solutions (IES), Global Cloud Services (GCS), Product Engineering (PE), Technology and Innovation (T&I), and other areas.
- Supporting process implementation and adoption,
- Harmonizing security tools in use.

The SAP Security Policy Framework (SPF) consists of several levels of security documents that support the requirements set forth in the SAP Global Security Policy (Policy). Lines of Business may also have supporting policies, standards, procedures, and good practices. SGS maintains the Global Security Policy, Standards, Procedures, and Good Practices to effectively provide global security governance. The Policy is a living document subjected to modification as needed to protect SAP as new threats and vulnerabilities are identified or the risk profile of the organization changes. The Policy must be reviewed annually or sooner if significant changes occur. Formatting, editorial, clarification, and minor content revisions are approved by the SAP Chief Security Officer.

SGS partners with the Business Information Security Officers (BISO) and other security representatives from all Lines of Business (LoB), Global Cloud Services (GCS), Intelligent Enterprise Solutions (IES), and central development teams from several board areas, such as Product Engineering (PE) and Technology & Innovation (T&I), to provide centralized and federated coverage through various functional areas that included but not limited to Security Operations, Security Training, Communications, Cyber Intelligence, Vulnerability Management, Security Architecture, Product Security, Governance, Risk, & Compliance (GRC), Sales & Enablement, and SecDevOps Guilds.

SGS pursues the following key objectives:

- For both Cyber and Physical Security, enact a multi-dimensional security and compliance approach for development units and security stakeholders to address legal requirements.
- Safeguard SAP’s customers, employees, data, and assets.
- Meet market security requirements: Support LoBs, Customer Success, and centralized stakeholders (IES, GCS, Secrecy, Data Protection and Privacy (DPP), etc.) by securing products, development lifecycle, and sales.

- Detect, monitor, and mitigate security risks and prepare SAP to meet security compliance requirements.
- Train SAP employees in security basics and train experts to proactively reduce security risks. SAP internal and external employees are informed about SAP Global Security Policy and the SAP Global Information Classification & Handling standard.
- Mitigate the damage/impact of possible forces of nature, they cannot guarantee protection.
- Make security training mandatory for existing personnel, newly hired employees, and external staff members. The manager of each employee/staff member is informed regarding the completion of, or failure to complete, the mandatory training.

Risk Management

Risk Management Overview

The objective of the Risk Management process is to properly identify, assess, prioritize and manage (i.e. minimize, monitor, and control the probability and/or impact of events with negative impact) risks (e.g. regulatory, financial, operational, and fraud risks) to the company. The SAP Global Risk Management Policy communicates the SAP Executive Board's expectations on how risks are to be managed within SAP. It sets out company-wide standards for managing risk across the Lines of Business (LoBs) and establishes the key risk management responsibilities within SAP.

The Global Risk Management Policy defines risk management methodologies, activities, and organizational requirements for achieving the policy objectives. SAP's risk management model comprises of five process steps:

- Risk Planning
- Risk Identification
- Risk Analysis
- Risk Response
- Risk Monitoring

SAP performs risk assessments to identify, quantify, and prioritize risks against criteria published in the SAP Global Risk Management Policy. Each cloud service performs risk assessments in alignment with the Global Risk Management policy and guidelines. Risks that exceed a certain level of risk exposure are documented in the Central Risk Repository (GRC Software Solution). Each risk is then mitigated to an acceptable level, or the risk is accepted in accordance with the Global Risk Management Policy. Risks may be accepted if, for example, the cost of implementing the mitigation exceeds the risk exposure or business impact.

Supplier Management

The objective of the Supplier Management process is to provide assurance that critical suppliers adhere to the agreed level of security and service delivery.

The compliance of subservice organizations with SAP's security requirements is periodically reviewed and verified by SAP audit procedures. Certain control objectives can be met only if the subservice organization's controls, assumed in the design of SAP's controls, are suitably designed, and operate effectively along with related controls at SAP.

Critical suppliers are identified as those who have access/potential access to customer data and those who are critical for the continuation of operations. These suppliers' contracts are reviewed for changes to compliance requirements. Evidence (e.g. audit reports, certificates) is requested from the suppliers if additional compliance requirements need to be fulfilled. Existing critical suppliers are reviewed (on an annual basis) for changes to their supplier type, information access types, and the criticality of the confidentiality, integrity, and availability of the Cloud offering. The existing supplier contracts are reviewed for changes to compliance requirements. Evidence (audit reports, certificates, etc.) is requested from the suppliers if additional compliance requirements need to be fulfilled.

New suppliers are screened against the Sanction Party List, which is a list of persons and companies with whom trade is prohibited by law. New suppliers that have access to production data and/or process customer data for Cloud Services (also called “critical suppliers”) are subject to specific checks required by SAP’s Global Procurement Organization depending on the type of the supplier. New, critical suppliers with access to personal and/or confidential data of SAP or SAP’s customers are required to complete a data processing enablement process or Third-Party Risk Management process.

Data Center Audits

SAP-owned and co-located data centers hosting productive customer systems are audited in accordance with the SAP Compliance Framework at least every two years.

Internal SAP data center auditors coordinate and perform physical security audits of co-located data centers. When physical data center audits are completed, the auditors create a report that is reviewed with the responsible person at the data center.

A data center audit follows a standard procedure, including a check of the adherence to internal requirements, resulting in an audit report.

Non-compliance is documented, tracked, and followed up in SAP's central managed ticketing system. For each documented issue, a risk mitigation response is mandatory. The issues are also communicated to the data center provider to help ensure that mandatory requirements are met. If an issue is deemed acceptable by SAP, the acceptance of the remaining risk is documented within the ticket.

Review of Infrastructure as a Service (IaaS) Provider Compliance Documents

Periodic reviews of IaaS attestation reports and/or compliance documents are performed to detect compliance issues. If non-compliance is detected, the risk is evaluated, and appropriate action is taken to mitigate non-compliance.

Monitoring

Management Review

SAP has developed and implemented an integrated framework based on information security management, quality management and business continuity principles. The framework brings the SAP Security Policy with SAP’s Security Standards, the SAP Quality Policy and Standards on Business and Service Continuity together.

SAP maintains and updates its management system by establishing policies, procedures, and processes to achieve its control objectives. Management review meetings occur at least annually, where management reviews SAP’s management system to help ensure its continuing suitability, adequacy, and effectiveness. The management review includes, at a minimum, the status of action items from previous management reviews, helps identify and implement required changes to the management system, encompasses feedback from audit results, including the results of examinations performed over the carved-out subservice organizations, identifies and assesses requirements of each stakeholder, legal and regulatory body, and reviews the results from regular risk assessments. Finally, the management review analyzes whether management fulfilled their objectives, records opportunities for continual improvement, and sets action items for tracking.

Information and Communication at SAP

Internal Communication on Security Topics

SAP has implemented various methods of communication at a global level to help ensure employees understand their roles and responsibilities and to communicate significant events in a timely manner. These methods include orientation and specific security training programs for newly hired employees, regular management meetings for updates on business performance and other matters, mandatory security awareness and secure communication training, the use of email messages for time-sensitive information, and articles on the SAP intranet. Any changes to the security policies and standards are communicated via email campaigns and articles on the SAP intranet.

Procedures for Exchanging Information

SAP IT systems are configured to protect transmitted information in accordance with requirements. Suitable measures for securing the exchange of information are in place, including:

- Utilization of email encryption
- Provisioning of secure network protocols and interfaces
- Encrypted communication lines
- Application of the Information Classification Security Standard

Communication of the Cloud Contract Information

Contracts for cloud services from SAP consist of three components:

- Cloud Service Description: This includes the term of the specific cloud service, the support schedule, and the operational availability of the cloud service.
- Data Processing Agreement (DPA): Based on the instruction from the data processor who handles the personal data uploaded to the cloud service, SAP implements and maintains technical and organizational measures to adequately protect personal data.
- General Terms and Conditions (GTC): The GTC document describes the essential legal terms that apply to the specific cloud service, including the related usage rights, customer data, warranties, confidentiality, and the limitations of liability provisions.

SAP Trust Center

SAP has implemented and maintains a review and audit program to comply with the requirements of specific compliance and security standards. The list of applicable attestations and certifications is available online in the Compliance section of the SAP Trust Center.

The SAP Trust Center is a self-service center where customers can initiate requests and collect information related to security and compliance for cloud services and on-premises software. The SAP Cloud contract information is also available for customers in the SAP Trust Center.

In the other subsections of the SAP Trust Center, customers can confirm data center locations and view cloud-based status information such as availability, downtime, and maintenance window. SAP has established dedicated notification processes, in accordance with contractual requirements, in case they fail to achieve one or more of their control objectives. Confidential information, such as mentioned above, is only disclosed via these dedicated channels.

Control Activities

Control activities include the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to the achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, and reviews of operating performance.

Within SAP's entities, various delegations of authority (DOAs) have been set up to help ensure dual or multiple validations/signatures on important transactions (such as contracts or recruitment) and to prevent single manager interference/override. On a regular basis, the Internal Audit function verifies SAP’s entities are adhering to established policies and procedures.

Control Objectives

To mitigate the identified risks to the achievement of the entity's objectives appropriately, SAP has defined control objectives for each process in scope of this report.

Control Objective	Control Objective Description
Backup and Restore	Controls provide reasonable assurance that computer systems are backed up to storage media and that procedures are employed to maintain the integrity of the storage media.
Change Management	Controls provide reasonable assurance that changes to the production environment are authorized, tested, approved, and implemented in a controlled manner.
Invoice Payment Processing	Controls provide reasonable assurance that invoice and payment transactions are processed completely, accurately, and in a timely manner.
Network and Communication Management	Controls provide reasonable assurance that network security measures are implemented to protect against threats from sources outside its system boundaries.
Physical Security	Controls provide reasonable assurance that physical access to server rooms and secured areas within data centers is restricted to authorized personnel and such facilities are protected from environmental hazards.
User and Access Management	Controls provide reasonable assurance that logical access to production systems and data files is restricted to authorized personnel.

Table 7: Control Objectives

Other Information about Management’s Description

SAP’s controls are included in Section IV of this report, “SAP’s Control Objectives, Related Controls, and KPMG LLP’s Test Procedures and Results.” Although the controls are presented in Section IV, they are, nevertheless, an integral part of SAP’s description of its system.

Overview of Processes

The following section provides an overview of the processes in scope for this report.

Backup and Restore

The objective of the Backup and Restore process is to back up (copy) and store data in remote locations where it is protected until needed, such as when a loss of data has occurred, and the data must be restored. The Backup and Restore process is supported by Backup and Restore services, which help ensure the integrity of customers' data by restoring corrupted data when necessary.

The loss of data can have a significant impact on IT systems. Loss or corruption of business data or customer master data can even threaten the existence of a company. Similarly, if key data is lost or is corrupted at a company, it can delay administrative or operational activities, or even bring them to a complete standstill. The Backup and Restore process mitigates these kinds of risks. The following process describes why and how backups are taken, how the data is protected and how backups are restored.

Data can be lost for many reasons:

- Demagnetization of magnetic data carriers as a result of aging or unsuitable ambient conditions (temperature, air humidity)
- Interference on magnetic data carriers caused by external magnetic fields
- Destruction of data carriers through natural disasters
- Inadvertent deletion or overwriting of files
- Technical failures on peripheral memories (head crash)
- Defective data carriers
- Uncontrolled changes to stored data (integrity loss)
- Deliberate destruction of data by computer viruses

The Backup and Restore process is based on the SAP Security Policy Framework, which follows SAP's Cloud Infrastructure Security Procedure and Key Management Security Procedure.

There are two processes for protecting data: Backup Management and Restore Management.

Backup Management

Backup agents are installed and backup jobs are scheduled on the corresponding database server. An initial full database backup is performed. After the successful initial backup, the new system is integrated into the landscape and the backup status is monitored via the respective monitoring tool.

Backups are performed on a regular basis for in-scope production systems. Relevant backup database systems are monitored on a daily basis. If backups are not running or encounter errors, backup error alerts are generated. The alerts are addressed within predefined timeframes and corrective actions are initiated and documented. Errors are either resolved by the Backup team or forwarded to the appropriate support group if needed.

Backup data is encrypted according to SAP policies and standards in accordance with the requirements related to the data being backed up. Encryption keys are managed and protected against modification and unauthorized disclosure.

Backup data is stored on two different backup devices physically located in different data centers. This is achieved via replication. However, during the period October 1, 2022 to October 22, 2022, SAP Ariba did not have encryption enabled for the replication communication channel.

Restore Management

Customers or customer representatives from cloud units (restore requestor) can request restores by submitting a Service Request (SR) in the respective ticketing system. The restore requestor must use the corresponding template and provide the necessary information.

The Restore Processor receives and validates the restore requirements, validates that the restore requestor is authorized to request the restore and documents the results in the ticket. If the validation fails, the SR is rejected, and the Restore Processor provides the reasons for the rejection. If the validation is successful, the Restore Processor proceeds with the restore. The Restore Processor checks that the backup data and backup media are available as required to perform the restore.

The Restore Processor documents the successful completion of the restore procedure in the ticket. The Restore Requestor can manually confirm the restore success. If this is not performed manually, the ticket will be confirmed automatically within a predefined timeframe. To validate the reliability of the backup media and restore process, data restoration functionality testing is performed at least annually. The testing procedures and results are documented.

Change Management

The objective of the Change Management process is to provide reasonable assurance that changes to the production environment are authorized, tested, approved, and implemented in a controlled manner.

Overview

SAP Ariba follows a Product Lifecycle Methodology (PLM) for product development. The methodologies vary slightly depending on product maturity and the type of development (e.g. new applications versus incremental features). In all cases, the methodologies define:

- Specific phases, activities, and deliverables.
- Entry and exit criteria, including reviewing feature completeness, quality trends, test case execution, and test case automation, as well as security reviews.
- Formal exit reviews, with final approval by SAP Ariba Products Development leadership or their delegates.

SAP Ariba’s development process is based on the Agile development methodology, with cross-functional teams called “feature teams” or “scrum teams.” Since requirements are difficult to capture in documents, Agile concentrates on having constantly running software in development that can be iterated quickly. Feature teams are responsible for planning and delivering sets of related features. Those teams typically include members from Development, Quality Assurance, Product Management, User Assistance, Globalization, and Readiness. In some cases, the team may also include members from the Production Operations and the User Experience teams.

Changes are developed and delivered via one of the following approaches:

- Feature-Based Development: New features and enhancements are developed independently utilizing Agile with Scrum for execution.
- Sustaining: Production defects are reviewed and resolved under a controlled change management process. Critical defects are fixed via hot fixes (HFs) or data fixes. Other important fixes are addressed via regularly scheduled service packs.

SAP Ariba releases software updates on a frequent basis to customers. Each release contains:

- Feature-based development features
- Incubation features
- Defect fixes

SAP Ariba typically deploys one consolidated customer-facing release per month containing:

- SAP Ariba Applications: A release that delivers updates to SAP Ariba Sourcing and Procurement Solutions
- SAP Ariba Network: A release that delivers updates to the Ariba Network

To help ensure customers know what each release contains, a release information is published to customers that includes a bill of materials (BOM) that highlights the content contained in the release.

In addition, SAP Ariba may deploy additional releases of underlying infrastructure applications that are not directly exposed to the customer. These releases support the Sourcing, Procurement, and Network solutions.

Feature-Based Development Model

A key aspect of feature-based development is that features are developed and deployed independently. Once a feature has met the exit criteria and has been approved, it is considered ready for production. Teams will frequently work on multiple features concurrently. In some cases, a collection of features may have cross-dependencies, as in the case when a new internal service is being delivered for the first time.

Planning

In feature-based development, features are reviewed, prioritized, and slotted for future sprints on a regular basis. This may be quarterly for some teams and as often as weekly for more dynamic teams.

Development

The Development phase is defined by a set of development sprints. A sprint is a fixed unit of time, where new units of functionality (“use cases”) are added to SAP Ariba applications. Sprints are generally two to four weeks long. The result of each sprint is workable, demonstrable code that can be shown to customers for feedback. Features will be developed in one or more sprints.

For a selected innovation, SAP Ariba development may work with customers. During development, features may be reviewed with select design partners after every sprint, and requirements are adjusted based on this feedback loop.

New feature code is protected by a toggle that disables the code until the feature is enabled once it has met standard release requirements. Customers may enable the feature in their test sites to prepare for the adoption of changes.

The Development phase for a feature ends once all exit criteria are met and approved. Exit criteria include security reviews, testing, documentation, and other requirements. Once the feature has been approved, it is considered ready for production pending further readiness activities.

Sustaining

SAP Ariba formally tracks production system changes in Jira for full change management.

Changes to production follow a defined review and approval process:

- Changes are deployed in the monthly or weekly release.
- Urgent issues that cannot wait for the next release are deployed through HFs. HFs undergo review, build qualification, testing, and approval.
- Releases undergo a full qualification cycle with automated and manual testing and must meet specified exit criteria.
- Change requests (features, enhancements, and defect fixes) are tracked in Jira and all code changes are managed in a version control system (e.g. Perforce, GitHub).

Quality Assurance

SAP Ariba uses the following quality control processes and tools:

- Technical Reviews (during design and implementation)
- Automated Testing and Manual Testing (including ad hoc testing)
- Performance and Stress Testing, as needed

Technical Reviews

Prior to implementation, design reviews by either a principal Engineer or Architect are required. During implementation, a code review, performed by two reviewers, is required. Code cannot be checked in until both reviewers approve the code (system-enforced). Application changes are managed in GitHub and host level changes are managed by Perforce. Code reviews for Perforce are tracked within the Crucible code review tool.

Testing

SAP Ariba leverages an automation test suite (both unit and UI-level). Automation also allows SAP Ariba to manage and maintain the release quality throughout the development lifecycle. The automation suite is run for every build during the full development lifecycle.

In addition to the automation suite, SAP Ariba executes a test suite of manual test cases. Each week, feature teams perform regular ad-hoc “group” testing on new functionality.

Code is scanned using dynamic and static code scanning tools to identify potential security and code flaws.

SAP Ariba management reviews the pass rate for all releases for both automation and manual testing prior to approving a release.

Performance / Stress Testing

Performance testing, validation and monitoring are integral parts of the SAP Ariba development and production operational models for larger changes.

During feature development, the design of every feature is reviewed for performance impacts. Where applicable, automated unit tests are written to help ensure critical performance measures are met as part of the feature development exit review.

SAP Ariba executes performance testing in a lab environment to simulate the production environment. Two different types of testing are performed in this environment:

- Stress testing is a test suite designed to simulate production-like transactions under load (thousands of users over multiple realms/communities with 30 million catalogue items).
- Stability testing (or longevity testing) is a long-running test suite used to help ensure that there are no issues due to extended usage of the system.

After product release, SAP Ariba has metrics that are constantly monitored to help ensure the performance of the production system from system level (memory, disk I/O, database connections, etc.) to the application level (page response times, business transitions, etc.). The SAP Ariba teams work with customers to understand their usage requirements to help ensure their needs are accounted for during production capacity planning and that production system performance standards are maintained during peak periods. Trend-based monitoring is used to track production system metrics and help ensure that there is sufficient capacity for ongoing growth.

SAP Ariba PLM Adherence

Regardless of the methodology followed, change control releases are documented within source code control systems such as Git or other document management systems such as the Confluence Wiki. This includes requirements, design, and test approach documents for all features. All test cases and results are documented and tracked.

All exit criteria, including release approval documents, are tracked in a document management system. All source code and important project documentation is kept in a version control system.

Features undergo a security impact analysis before implementation.

Prior to production implementation, all changes to applications, including emergency changes, require complete documentation based on established procedures and checklists with sign-off approval from Engineering Development management before the Production Operations team will apply the changes.

Asset Management

Asset Management includes a range of activities that allows SAP to manage the inventory and monitor assets related to the system during their lifecycle. This comprises assets located in SAP internal data centers, including physical and virtual servers. Core Asset Management activities rely on the integration of asset data across several Asset Management tools. Key attribute data for physical and virtual assets is recorded. Production assets are identified in an asset inventory.

Hyperscaler and SAP Converged Cloud Account Management

Hyperscaler accounts within SAP are tracked and managed against each organization unit. A central catalogue of hyperscaler accounts utilized within SAP is maintained, providing information about key data elements. The tracking of this information allows for proper governance and security.

Invoice Payment Processing

The objective of the Invoice Payment Processing process is to provide reasonable assurance that invoice and payment transactions are processed completely, accurately, and in a timely manner.

Data Validations: Data validations checks are done to help ensure data integrity for invoice payment processing. Ariba Network validates invoices according to the buyer-configured rules and rejects invoices that do not pass validation, e.g., Ariba Network validates online invoices during data entry and displays onscreen messages for any errors that must be corrected.

Errors in Batch Payment: The application is configured to identify errors related to duplicate batch and unbalanced batch payments and provide notification to buyers when such errors occur.

Invoice Reconciliation Exception: An invoice exception is a discrepancy between the data on the invoice and the data on the associated order, contract, or receipt. Invoice exceptions can represent a variety of issues, such as missing receipts, mismatched quantities or prices, duplicate invoices, or tax variances. Exceptions can occur at either the line-item level or the header level of an invoice and require manual intervention per the Invoice Exception configuration. User’s group membership determines the invoice exceptions that user can reconcile.

Supplier Bank Validation: Application is configured to validate supplier bank account before payment is processed. Invalid supplier accounts are detected, blocked for payment, and the buyer is notified.

Customers can refer to guides available on SAP Help for further details on SAP Ariba Invoice Payment processing.

Network and Communication Management

The objective of the Network Communication and Security Architecture process is to provide security measures that prevent unauthorized logical access on the SAP Cloud Network levels where the customer systems are managed and run. The SAP Cloud Network is separated from the SAP Corporate Network via a firewall.

Firewalls and Network Architecture

Firewalls are implemented at the network level to help ensure that unauthorized network traffic is filtered, and security at the network level is provided. Changes to the filter set are approved, logged, and traceable to the user who performed the change. Firewall configurations are reviewed at least every quarter.

Network architecture diagrams for the production environment include the design of security zones for network segmentation. These diagrams are documented and reviewed at least annually.

Encryption in Transit

Ariba uses, at a minimum, 128-bit TLS encryption for the transmission of private or confidential information over public networks.

Intrusion Detection

SAP Ariba deploys network intrusion detection/prevention appliances. The intrusion detection/prevention solution provides logging and alert capabilities to assist in the detection of potentially malicious acts or misuse. Logs are sent to the central SIEM for triaging and tracking. The SAP Ariba Central Security team reviews logs generated by the intrusion detection/prevention sensors, and potential incidents are subsequently addressed, resolved, and reviewed by management. Palo Alto Intrusion Detection & Prevention Systems provides additional vulnerability protection, network anti-malware and anti-spyware into one service that scans all traffic for threats - all ports, protocols, and encrypted traffic. This provides for scanning for threats at all points within the cyber-attack lifecycle, not just when it first enters the network - providing a layered defence, zero trust model with prevention at all points.

Physical Security

October 1, 2022 to March 4, 2023

The objective of the Physical Security process is to help ensure that data centers are protected by adequate controls. These controls include facility and environmental security (for SAP-owned data centers), access controls, and integrated surveillance.

Facility and Environmental Security

A backup power supply is available for the SAP-owned data centers in case of primary power failure, the backup power generators are maintained on a regular basis. Proof of their maintenance is documented in a report provided by the supplier company.

In order to protect against damage from fire, the SAP-owned data centers are equipped with appropriate fire emergency systems, including smoke and heat sensors and fire extinguishers. To help ensure their functionality, the fire emergency systems are tested and maintained on a regular basis. Proof of their maintenance is documented in a report provided by the supplier company.

The climate control of the SAP-owned data centers is controlled via redundant air conditioning systems operating within a predefined temperature range. To help ensure functionality, the air conditioning systems are tested and maintained on a regular basis, which is documented by the supplier company in a report.

Access

In order to gain physical access to a data center, an individual with an SAP user ID should request the access via the Cloud Datacenter Access Workflow Tool. On a monthly basis, Global Physical Security and Data Center Management review access to SAP-owned and Colocation data centers for valid approval and appropriateness. Access that is no longer needed is removed in a timely manner. If necessary for terminations, a lookback analysis is performed to determine if there was unauthorized access to data centers.

Access is granted by the Supervisor or Cost Center Owner and the Local Area Owner. The access request, together with the approval, is stored in the Cloud Data center Access Workflow Tool. The access control system, SIPORT (Germany), is then used to manage the data center access. These systems log access according to the badge swipes. An access card is required to enter the data center, and access attempts are recorded in a log file. The data center is guarded 24x7x365, and access is only granted to individuals with appropriate access cards.

Colocation Data Centers

If a person with unescorted access to the data center leaves the company, the access is revoked within 48 business hours of their contract end date.

Surveillance

The SAP-owned data centers are equipped with motion sensors.

Unauthorized access to secure areas of the SAP-owned data centers is monitored by motion sensors. The on-duty security staff are alerted via alarms when the motion sensors have detected movement. Motion sensors are maintained on a regular basis. Maintenance is documented by the supplier company in a report.

The areas surrounding the SAP-owned data center and facility buildings are monitored by security guards on a 24x7x365 basis using surveillance cameras. Surveillance cameras are maintained on a regular basis. Maintenance is documented by the supplier company in a report.

In some SAP-owned data centers, motion sensors are embedded in the surveillance cameras and, when activated, begin recording. The feeds from these cameras are monitored live 24x7 from a security operations center in the respective data centers. If footage is interrupted, the security operations center staff will triage, and if the feed cannot be restored, a service call is made to the supplier for rectification.

User and Access Management

The objective of the User and Access Management (UAM) process is to help ensure that logical access to the solutions' production systems and supporting tools is reasonable and restricted to properly SAP-authorized individuals.

SAP has established and documented identity management, access control and password policies. These policies define password requirements and access controls to help maintain authorized user access and to prevent unauthorized access to information systems. The allocation and use of privileges are restricted and controlled. Appropriate authentication methods are used to control access by remote users.

Identity Management and Authentication

All users, SAP employees and external workers, have a unique identifier (user ID), and a suitable authentication technique is used to substantiate the user's claimed identity. These unique user identifiers are used whenever an employee or an external worker accesses production systems.

Session management mechanisms are in place for to manage the lifecycle of user sessions.

Employee Central (EC) serves as the HR system for SAP employees, while Fieldglass (FG) functions as the HR system for external workers. SAP utilizes the SAP IT Identity Management System (SAP IT IDM) to synchronize SAP Global Activity Directory (SAP Global AD) daily, which is then used to access Safeguard for authenticating to production with role-based privileged credentials.

Individual accounts for SSH access are managed in LDAP.

Logical Access

Policies governing logical access to the SAP Ariba solutions, including segregation of duties (SoD), have been documented and communicated to System Administrators. User additions and modifications must be authorized by SAP Ariba Operations management and user revocation must happen in a timely manner after employees are terminated.

Further, system administration level access to the production servers is restricted to authorized personnel and subject to two-factor authentication. SAP Ariba’s password settings are configured in accordance with the SAP Global Security Standard.

A production access request workflow has been created to grant access to the production environment. Each production access request is required to be approved by the requestor’s manager, the Security team and the Operations team. This is applicable to all type of users and roles such as System Administrators, Database Administrators, Network Engineers, and the Deployment and Tools teams. An SoD policy has been established for the various roles and each production access request is validated to help ensure that SoD is not violated.

Developers do not have direct access to the production environment. The Dev/Test and Production environments are segregated. As per SoD, all code pushes to production can only be done by members of the Cloud Operations team.

Access to SAP Ariba Buyer and Business Network Supplier Mobile Applications

For the buyer mobile application, access requires authorized permission, which allows for activation of the user’s mobile device with their user account. Login requires the use of a password. A user may optionally use phone-provided PIN or biometrics to access the application.

For the business network supplier mobile application, login requires a valid username and password. A user may optionally use phone-provided biometrics to access the application.

Access Revocation for Leavers and Job Transfers

Employees and external workers who leave SAP (leavers) are first identified by HR systems (EC for employees and FG for external workers) via employee termination dates and external worker close dates. FG via C-IDM (an intermediary system for external workers) and EC then interface the termination data to SAP IT IDM. SAP IT IDM synchronizes with SAP Global AD.

The deactivation of a user in AD prevents the user from logging into access management tool (Safeguard).

An automated script compares the Cloud Operations access management tool (Safeguard) with AD daily to identify user accounts of terminated employees. Jira tickets are created by the script when Safeguard accounts are found with no corresponding account in SAP’s AD. Within seven business days, such accounts are deactivated by the responsible team in Cloud Operations.

External workers are required to have a worker end date field populated in FG which cannot be set to greater than 13 months from the account creation or extension date. Once the worker end date is reached, or if the FG account status is manually disabled, an automated workflow within FG will trigger the user account deactivation process.

On July 24, 2023, SAP split the user access rights revocation control into two separate controls - one covering internal employee leavers and one covering external worker leavers. For the period October 1, 2022 to July 23, 2023, the control to revoke access rights for leavers was not suitably designed. The control design did not include an attribute to monitor the automated job that processes leavers from the HR systems (EC for employees and FG for external workers to SAP IT IDM. As such user access rights revocations of leavers was not processed timely throughout the period October 1, 2022 to July 23, 2023. Additional information can be found in Section IV. See Section V for management's response to exceptions noted.

For employees who change roles, an automated Jira ticket is generated indicating the move. The manager and the employee are automatically notified via email. The manager confirms in the Jira ticket whether access to Safeguard shall be maintained or revoked. Without confirmation, Cloud Operations will deactivate the account within 30 business days after ticket creation.

However, the control described above was not suitably designed for the period October 1, 2022 to July 23, 2023 to modify access for employees that have transferred roles as the control design did not include an attribute to monitor the automated job that processes job transfers from the HR system (EC for employees) to SAP IT IDM. As such user access right modification of access were suitably designed to be processed timely throughout the period October 1, 2022 to July 23, 2023. Additional information can be found in Section IV. See Section V for management's response to exceptions noted.

Quarterly Lookback Reviews

To address risks associated with untimely user access revocation due to delays in the automated revocation process, SAP has implemented additional lookback controls. These controls involve quarterly reviews and assessments of leavers and changers, and active IDM accounts. Each control is further described below.

- A quarterly review of all terminated internal employees and external workers is completed. Any terminated individuals who are removed untimely are further assessed for post-termination login activity to the production environment. For any terminated individuals who are identified as having post-termination login activity to the production environment, their activity logs are reviewed for any inappropriate events.

  The control was implemented on June 30, 2023. For the operation of the control, the review included the period from April 1, 2023 to September 30, 2023.

- A quarterly review of all internal employee changers / transfers is completed. Any transfers who are reviewed or removed untimely are further assessed for post-transfer login activity to the production environment. For any transfers who are identified as having post-transfer login activity to the production environment, their activity logs are reviewed for any inappropriate events.

  The control was implemented on September 15, 2023. For the operation of the control, the review included the period from April 1, 2023 to September 30, 2023.

- A point-in-time quarterly review of all active internal employees and external workers SAP IT Identity Management (IDM) accounts is completed. Active IDM accounts identified without an associated active HR (Employee Central/Fieldglass) record are further assessed for post-termination login activity to the production environment. For any employees and external workers who are identified as having post-termination login activity to the production environment, their activity logs are reviewed for inappropriate events.

The control was implemented on July 4, 2023. For the operation of the control, the review was as of July 4, 2023 and September 29, 2023.

Job Monitoring and Weekly Reconciliation

Additional monitoring controls were implemented to address the design deficiencies related to the absence of monitoring over the automated job that processes leavers and transfers from the HR systems (EC for employees and FG for external workers (leavers only) to SAP IT IDM. Each control is further described below:

- On a daily basis, the 1AM Product Support team reviews the IDM job sync logs and the error notification email alerts for any errors in the transfer of D/I-user account changes or terminations from Employee Central to IDM. The team validates that the user accounts are locked/disabled in IDM and the information is fed to downstream systems that are integrated directly with IDM. Errors are resolved in a timely manner.

  The control was implemented on July 24, 2023.

- On a daily basis, the 1AM Product Support team reviews the IDM job sync logs and the error notification email alerts for any errors in the transfer of C-user terminations from Fieldglass to IDM. The team validates that the user accounts are locked/disabled in IDM and the information is fed to downstream systems that are integrated directly with IDM. Errors are resolved in a timely manner.

  The control was implemented on July 24, 2023. The control was not suitably designed to monitor whether the job that processes external worker contract termination data from Fieldglass to SAP IT IDM completes on a timely basis. Additional information can be found in Section IV. See Section V for management’s response to exceptions noted.

- The 1AM Product Support Team reconciles the HR IT lists of terminated users from EC to data in the IT-IDM system. Discrepancies are investigated and required changes to IDM data are input manually as needed.

  This control operates three times per week and was implemented on July 27, 2023.

- The 1AM Product Support Team reconciles the Fieldglass IT lists of terminated users to data in the IT-IDM system. Discrepancies are investigated and required changes to IDM data are input manually as needed.

  This control operates three times per week and was implemented on July 27, 2023.

  The control was not suitably designed to monitor the consistency of the data between Fieldglass and SAP IT IDM and to effectively address discrepancies. Additional information can be found in Section IV. See Section V for management’s response to exceptions noted.

- On a daily basis, the 1AM Product Support Team monitors the IDM internal jobs for any errors or long-running scripts (>16 hours runtime). The team creates an IAM JIRA Defect ticket to prioritize and resolve any issues.

  The control was implemented on July 24, 2023.

These controls contribute to the accurate synchronization of user data and effective monitoring of SAP IT IDM internal jobs, to timely resolve malfunctions or delays in the automated access revocation process.

Account Review

Quarterly, every production user account within Ariba is reviewed to help ensure that permissions are still required for the job role of the individual user. Any unnecessary access identified is removed by the Site Reliability Engineering (SRE) team.

Session Management

SAP Ariba solutions limit sessions to 30 minutes of idle time before timing out. Prior to a session timing out, the solutions send an alert to notify the idle user that their session is pending timeout, providing the user with an opportunity to intervene and cancel the timeout. If the user does not respond before the timeout period is reached, their work will be saved, and they will be logged out of the system.

Keyshell logging

Once a user logs onto bastion host to access production, a keyshell script will capture user activity in keyshell logs to maintain audit trail of actions. Access to keyshell logs is restricted to privileged sys admins.

Section IV

SAP's Control Objectives, Related Controls, and KPMG LLP's Test Procedures and Results

Provided by KPMG LLP

Description of Testing Performed

Test procedures performed in connection with determining the operating effectiveness of controls are described below.

Type	Description
Inquiry	Interviewed appropriate personnel about timing, performance and review of relevant controls.
Inspection	Reviewed documents and reports that provide an indication of the design of controls. This includes among other things: — Reading and reviewing of management reports if certain actions were performed — Inspection of documentation for evidence of placement in operation — Inspection of operation manuals, flow charts, system documentation
Observation	Observed responsible staff personnel perform the control activities which included the collection of supporting documentation (e.g., screen shots).
Re-performance	Re-performed selected transactions (including control activities) described in the provided process description or documentation.

Assessing the Completeness and Accuracy of Information Provided by the Entity

When using information produced by SAP, which includes, but is not limited to, management's reports used in the performance of controls and reports generated to facilitate testing of control populations (e.g. controls which require system-generated populations for sample based testing), KPMG evaluated whether the information was sufficiently reliable for our purposes, including, as necessary, obtaining evidence about the completeness and accuracy of the information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Subsequent Events

Between the end of the examination period and the signature of our report we did not become aware of any reportable topics.

KPMG's Detailed Test Procedures and Results of Testing

On the following pages, the control activities have been specified by and are the responsibility of SAP. KPMG's test procedures and test results are the responsibility of the service auditor.

Control Objectives Summary

Control Objective Ref.	Control Objective	Control Objective Description
BR	Backup and Restore	Controls provide reasonable assurance that computer systems are backed up to storage media and that procedures are employed to maintain the integrity of the storage media.
CM	Change Management	Controls provide reasonable assurance that changes to the production environment are authorized, tested, approved, and implemented in a controlled manner.
IPP	Invoice Payment Processing	Controls provide reasonable assurance that invoice and payment transactions are processed completely, accurately, and in a timely manner.
NC	Network and Communication Management	Controls provide reasonable assurance that network security measures are implemented to protect against threats from sources outside its system boundaries.
PS	Physical Security	Controls provide reasonable assurance that physical access to server rooms and secured areas within data centers is restricted to authorized personnel and such facilities are protected from environmental hazards.
UAM	User and Access Management	Controls provide reasonable assurance that logical access to production systems and data files is restricted to authorized personnel.

Control Objective Backup and Restore

Control Objective Ref.	Control Objective Description
BR	Controls provide reasonable assurance that computer systems are backed up to storage media and that procedures are employed to maintain the integrity of the storage media.

Control Ref.	Control Description Provided by SAP	KPMG's Test Procedures	KPMG's Test Results
BR01	Backups are performed at planned intervals for backup relevant production systems in accordance with documented procedures.	Inspected the Cloud Engineering Services - Data Backup Policy to determine whether the backup requirements were defined and documented. For a selection of databases, inspected backup configurations to determine whether backups were configured and performed according to the policy.	No exceptions noted.
BR02	A backup monitoring tool is in place to monitor the backup process. Repeated backup failures are followed-up and actions taken are documented.	Inspected the backup monitoring process document to determine whether the backup monitoring process was defined and documented. Inspected the configuration of alerts from the monitoring tool to determine whether alerts were configured to monitor backups for failures. For a selection of backup failure alerts, inspected related tickets to determine whether the alerts were remediated and resolved.	No exceptions noted.
BR03_ Ariba	To help ensure the durability, the backup data is transmitted through encrypted communication channel to a remote site.	Inspected the Ariba Data Backup Policy to determine whether replication and encryption requirements were defined and documented. Inspected the configuration of the replication alerts for servers to determine whether they were designed to alert relevant personnel based on pre-defined thresholds. For a selection of replication alerts, inspected tickets to determine whether replication alerts were triaged and remediated.	No exceptions noted.

Control Objective Ref.	Control Objective Description
BR	Controls provide reasonable assurance that computer systems are backed up to storage media and that procedures are employed to maintain the integrity of the storage media.

Control Ref.	Control Description Provided by SAP	KPMG's Test Procedures	KPMG's Test Results
BR03b	To help ensure durability, an encrypted communication channel is used for the replication of full copies of production data.	Inspected the Ariba Data Backup Policy and inquired with management to determine whether Ariba used an encrypted communication channel for replication. **October 23, 2022 to September 30, 2023:** For a selection of production databases, inspected encryption configuration to determine whether they were configured to encrypt data.	**October 1, 2022 to October 22, 2022:** Exception noted. The control was not designed appropriately to use an encrypted communication channel for the replication of full copies of production data. *Refer to Section V for management's response.* **October 23, 2022 to September 30, 2023** No exceptions noted.
BR04	Backup data at rest is encrypted according to SAP policies and standards, if the original data is not encrypted. Encryption keys are securely protected against modification and unauthorized disclosure. Confidentiality and integrity of the keys is supported by dedicated tools and processes.	Inspected the Ariba encryption standard to determine whether encryption standards for backup data at rest were defined and documented. Inspected the configuration of the managed encryption keys to determine whether dedicated tools and processes were in place. For a selection of backup storage devices, inspected the configuration backup storage devices to determine whether they were configured to encrypt backup data and protected against modification and unauthorized disclosure.	No exceptions noted.

Control Objective Ref.	Control Objective Description
BR	Controls provide reasonable assurance that computer systems are backed up to storage media and that procedures are employed to maintain the integrity of the storage media.

Control Ref.	Control Description Provided by SAP	KPMG's Test Procedures	KPMG's Test Results
BR05	Upon a restore request, restore is performed either automatically or manually and documented.	Inspected the Ariba Restore Management process documentation to determine whether the restore process was defined and documented. For a selection of backup restore requests, inspected tickets to determine whether the restore was completed successfully and results were documented.	No exceptions noted.
BR06	Data restoration functionality testing is performed semi-annually to verify the usability of backup data. The testing procedures and results are documented.	Inspected the Ariba Data Backup Policy to determine whether the requirements for restore testing were defined and documented. Inspected the semiannual backup restore request determine whether the restore was completed successfully and results were documented.	No exceptions noted.

Control Objective Change Management

Control Objective Ref.	Control Objective Description
CM	Controls provide reasonable assurance that changes to the production environment are authorized, tested, approved, and implemented in a controlled manner.

Control Ref.	Control Description Provided by SAP	KPMG's Test Procedures	KPMG's Test Results
5.01_Ariba	The documented systems development methodology describes the change initiation, software development, change documentation, and approval processes.	Inspected the Ariba’s Product Lifecycle Methodology (PLM) document for product development to determine whether a systems of development methodology exists, is documented, and defines change initiation, software development, change documentation, and approval processes.	No exceptions noted.
5.06_Ariba	The revision control system is configured to require all changes to hosts to be approved, documented in the ticketing system, and checked in prior to deployment.	Observed a submitted host change in Perforce to determine whether the change was required to be approved and documented in the ticketing system prior to deployment. Observed a submitted host change without approval or documentation in the ticketing system in Perforce to determine whether the change submission would be rejected.	No exceptions noted.
5.08_Ariba	Development and test environments are segregated from production.	Observed an administrator establish network connections to a production server as well as development and test environments to determine whether these environments were segregated from production.	No exceptions noted.

Control Objective Ref.	Control Objective Description
CM	Controls provide reasonable assurance that changes to the production environment are authorized, tested, approved, and implemented in a controlled manner.

Control Ref.	Control Description Provided by SAP	KPMG's Test Procedures	KPMG's Test Results
5.09_Ariba	Two code management data base tools, Perforce and GitHub, are utilized to maintain the production code base and feature code review functionalities. These functionalities help ensure that code changes are not merged to the main branch prior reviewing it, following the segregation of duties principle.	Observed a change request in GitHub that had not yet been approved to determine whether the system was configured to prevent the changes from being merged. Observed a change request in GitHub that had been peer reviewed to determine whether the system allowed the code to be merged. Inspected GitHub code repository branch protection settings to determine whether code changes required a secondary reviewer and approval prior to merging the changes. Inspected the listing of GitHub owners to determine whether access to modify branch protection settings was restricted to appropriate individuals. Inspected Perforce configurations to determine whether code changes required reviews and approvals prior to merging the changes.	No exceptions noted.
AM01_ Ariba	Production assets are identified in an asset inventory. Key attribute data for physical and virtual assets is recorded.	Inspected the SAP IT Asset Management policy to determine whether asset management procedures were defined and documented. Inspected job configurations to determine whether asset inventory discovery has an established schedule and frequency. Inspected population of assets from the inventory management system to determine whether the key attribute fields were recorded. For a selection of months, inspected the monthly reconciliation of physical and virtual assets to determine whether the asset listing was reviewed for completeness.	No exceptions noted.

Control Objective Ref.	Control Objective Description
CM	Controls provide reasonable assurance that changes to the production environment are authorized, tested, approved, and implemented in a controlled manner.

Control Ref.	Control Description Provided by SAP	KPMG's Test Procedures	KPMG's Test Results
AM14	Infrastructure as a Service (IaaS) Accounts are identified and mapped to the organizational unit and mapped to the used landscapes (Prod, Dev & Stage/Test) and tracked in an inventory. *This control was in place from October 1, 2022 to March 31, 2023.*	Inspected the Ariba asset management policy to determine whether established procedures for inventorying assets are defined and documented. Inspected the Google Cloud Platform inventory configuration to determine whether projects were mapped to the used landscapes (Prod, dev, stage) and tracked in the inventory management system.	No exceptions noted.

Control Objective Ref.	Control Objective Description
CM	Controls provide reasonable assurance that changes to the production environment are authorized, tested, approved, and implemented in a controlled manner.

Control Ref.	Control Description Provided by SAP	KPMG's Test Procedures	KPMG's Test Results
CM02_ Ariba	Infrastructure changes are handled in accordance with SAP Ariba's change management procedures. Changes are requested, approved prior to implementation and include change plan, rollback plan, and test plan (where applicable). Standard and emergency changes are approved by an individual other than the requestor.	Inspected the Ariba Change Management Guiding Principles wiki site to determine whether requirements for risk assessments, change types, and maintenance notifications were defined and documented. Inspected the Change Management Overview wiki site to determine whether levels for risk and impact assessments were defined and documented. For a selection of infrastructure change requests, inspected change documentation to determine whether changes were categorized per impact and risk level assessment and approved according to the guidelines of a routine, standard and emergency change, including change approval requirements. For a selection of infrastructure change requests, inspected change documentation to determine whether changes included change plan, rollback plan and test plan prior to implementation.	No exceptions noted.
CM03a_ Ariba	Software releases are tested and approved prior to deployment. Changes are approved by an individual other than the requestor. Documentation for externally facing features is provided as the features become generally available to customers.	Inspected the Feature Exit Criteria wiki to determine whether requirements for approvers were defined and documented. Inspected the Weekly and Monthly Deployment Approval Matrix to determine whether guidelines were defined for deployment approval. Inspected the Ariba Release Portal to determine whether release notes and their features were available for customers. For a selection of software changes, inspected change documentation to determine whether changes were tested and approved prior to deployment and changes were approved by an individual other than the requestor.	No exceptions noted.

Control Objective Ref.	Control Objective Description		
CM	Controls provide reasonable assurance that changes to the production environment are authorized, tested, approved, and implemented in a controlled manner.		
Control Ref.	**Control Description Provided by SAP**	**KPMG's Test Procedures**	**KPMG's Test Results**
CM03b_ Ariba	SAP Business Network Supplier mobile app is tested and approved prior to deployment. Changes are approved by an individual other than the requestor. Documentation for externally facing features is provided as the features become generally available to customers.	Inspected the Feature Exit Criteria wiki to determine whether requirements for approvers were defined and documented. Inspected the Weekly and Monthly Deployment Approval Matrix to determine whether guidelines were defined for deployment approval. Inspected the Ariba Release Portal to determine whether release notes and their features were available for customers. For a selection of supplier mobile application changes, inspected change documentation to determine changes were tested and approved prior to deployment and changes were approved by an individual other than the requestor.	No exceptions noted.
CM03c_ Ariba	SAP Ariba Procurement mobile app is tested and approved prior to deployment. Changes are approved by an individual other than the requestor. Documentation for externally facing features is provided as the features become generally available to customers.	Inspected the Feature Exit Criteria wiki to determine whether requirements for approvers were defined and documented. Inspected the Weekly and Monthly Deployment Approval Matrix to determine whether guidelines were defined for deployment approval. Inspected the Ariba Release Portal to determine whether release notes and their features were available for customers. For a selection of mobile application changes, inspected change documentation to determine that they were tested and approved prior to deployment and changes were approved by an individual other than the requestor.	No exceptions noted.

Control Objective Ref.	Control Objective Description
CM	Controls provide reasonable assurance that changes to the production environment are authorized, tested, approved, and implemented in a controlled manner.

Control Ref.	Control Description Provided by SAP	KPMG's Test Procedures	KPMG's Test Results
NWS04	Changes of firewall rules are approved, logged, and can be traced back to the user performing the change.	Inspected the Ariba Cloud-Ops Firewall Procedure, Network Team Change Process, and Routine Changes documents to determine whether the process for firewall rule changes was defined and documented. For a selection of firewall rule changes, inspected change tickets to determine whether changes to firewall rules were approved, logged, and could be traced back to the user performing the change.	No exceptions noted.

Control Objective Invoice Payment Processing

Control Objective Ref.	Control Objective Description		
IPP	Controls provide reasonable assurance that invoice and payment transactions are processed completely, accurately, and in a timely manner.		
Control Ref.	**Control Description Provided by SAP**	**KPMG's Test Procedures**	**KPMG's Test Results**
8.01_Ariba	Data entry screens for manual invoices entry contain mandatory fields and edit/validation checks to enforce completeness of inputs.	Inspected the Ariba Network ("AN") application configuration logic used to verify that the mandatory fields were enforced within the system. Observed application demonstration of AN to determine whether data entry screens for invoice manual entry contained required fields and edit/validation checks to enforce completeness of inputs.	No exceptions noted.
8.03_Ariba	Duplicate payment batches received from buyers are identified and ignored and the buyer is notified.	Inspected the AN application configuration logic to determine whether duplicate payment batches created are flagged as exceptions within the AN application. Observed the process owner attempt to submit a duplicate batch to determine if the batch was placed in an error queue and the buyer was notified. Observed the process owner submit a payment batch to determine whether the batch was processed successfully.	No exceptions noted.
8.04_Ariba	Payment batch aggregate amounts not in balance are identified, errored out, and the buyer is notified.	Inspected the configuration code logic to determine whether the system was configured to flag any mismatch in the payment batch aggregate amounts and notify the user of the mismatch. Observed the process owner attempt to submit a batch with balanced payment amounts to determine whether the batch was processed successfully. Observed the process owner attempt to submit a batch with unbalanced payment amounts to determine whether the payment batch was placed in an error queue and the system notified the buyer.	No exceptions noted.

Control Objective Ref.	Control Objective Description		
IPP	Controls provide reasonable assurance that invoice and payment transactions are processed completely, accurately, and in a timely manner.		
Control Ref.	**Control Description Provided by SAP**	**KPMG's Test Procedures**	**KPMG's Test Results**
8.06_Ariba	Invoice reconciliation exceptions are identified in accordance with customer specified business processes and require manual intervention when tolerances are exceeded.	Inspected the code logic to determine whether the Ariba system was configured to fire an exception based upon the values to be checked during invoice reconciliation. Observed the process owner attempt to submit an Ariba Network payment remittance file in accordance with customer specified business processes to determine whether it was processed successfully. For a selection of header and line level exceptions, observed the process owner attempt to submit an Ariba Network payment remittance file in violation of customer specified business processes to determine whether the exception was flagged in the Ariba invoice system.	No exceptions noted.
8.07_Ariba	Supplier accounts are validated based on their proxy ID prior to a payment being processed- invalid supplier accounts are detected, blocked for payment, and the buyer is notified.	Inspected the configuration code logic to determine whether supplier accounts were verified against their IDs. Observed the process owner attempt to submit an Ariba Network payment remittance file with invalid supplier information to determine whether the AN application identified the error, blocked the payment, and notified the buyer. Observed the process owner attempt to submit an Ariba Network payment remittance file with valid supplier information to determine whether it was processed successfully.	No exceptions noted.

Control Objective Network and Communication Management

Control Objective Ref.	Control Objective Description		
NC	Controls provide reasonable assurance that network security measures are implemented to protect against threats from sources outside its system boundaries.		
Control Ref.	**Control Description Provided by SAP**	**KPMG's Test Procedures**	**KPMG's Test Results**
NWS05	Firewall rule sets are reviewed on a quarterly basis.	For a selection of quarters, inspected the firewall review tickets to determine whether firewall rule sets were reviewed on a quarterly basis.	No exceptions noted.
NWS23	Network diagrams for the production environment have been documented and are reviewed at least annually. Network diagrams include the design of separate security zones.	Inspected the network architecture diagrams to determine whether network diagrams for the production environment were documented, included the design of separate security zones. Inspected the Ariba Cloud Ops Firewall Procedures to determine whether procedures for the configuration of security zones and review of network diagrams were defined and documented.	No exceptions noted.
NWS30a_ Ariba	Intrusion detection/prevention tools are configured to scan and block network threats for vulnerabilities, malware, and spyware.	Inspected the IPS and IDS configurations to determine whether they were configured to protect internet facing customer systems. Inspected the PAN threat Protection procedure to determine whether a process for handling intrusion detection events was defined and documented. Inspected the IDS/IPS configurations to determine whether IDS/IPS tools were configured to block network threats for vulnerabilities, malware, and spyware. Inspected the Use Case Catalog and Splunk configurations to determine whether alerts were configured to analyze the IDS logs and notify personnel of identified threats.	No exceptions noted.

Control Objective Ref.	Control Objective Description
NC	Controls provide reasonable assurance that network security measures are implemented to protect against threats from sources outside its system boundaries.

Control Ref.	Control Description Provided by SAP	KPMG's Test Procedures	KPMG's Test Results
NWS31_ Ariba	Ariba uses, at a minimum, 128-bit TLS encryption for transmission of private or confidential information over public networks.	Inspected SAP's Encryption Management Standard to determine whether encryption requirements for securing web communications sessions (data-in-transit) were defined and documented. For a selection of public facing websites, inspected TLS certificate details to determine whether Ariba uses at a minimum, 128-bit TLS encryption for transmission of private or confidential data over public networks.	No exceptions noted.

Control Objective Physical Security

Control Objective Ref.	Control Objective Description
PS	Controls provide reasonable assurance that physical access to server rooms and secured areas within data centers is restricted to authorized personnel and such facilities are protected from environmental hazards.

Control Ref.	Control Description Provided by SAP	KPMG's Test Procedures	KPMG's Test Results
PS01	For SAP-owned and Colocation data centers, new or modified access for an employee or external worker is requested and approved within an access workflow system, for no more than one year. The requested access is approved by at least the Supervisor / Cost Center Owner and the local area owner prior to provisioning access. The access provisioned must match the access approved. *This control was in place from October 1, 2022 to March 4, 2023*	Inspected the policies regarding data center access to determine whether processes and guidelines for the assignment of permanent access to the data centers were defined and documented. Inspected the workflow access request tool to determine whether all data center access requests were configured to require approval by at least the Supervisor / Cost Center Owner and the local area owner. Inspected the access workflow system configuration to determine whether access could only be requested for a maximum time frame of one year. Inspected the permanent accesses granted during the examination period for the German data centers to determine whether the access to the data center was requested via the access workflow system and the request was approved by at least the Supervisor / Cost Center Owner and the local area owner. Inspected the permanent accesses of all users granted during the examination period for the colocation data centers to determine whether the access to the data center was requested via the access workflow system and the request was approved by at least the Supervisor / Cost Center Owner and the local area owner.	No exceptions noted.

Control Objective Ref.	Control Objective Description
PS	Controls provide reasonable assurance that physical access to server rooms and secured areas within data centers is restricted to authorized personnel and such facilities are protected from environmental hazards.

Control Ref.	Control Description Provided by SAP	KPMG's Test Procedures	KPMG's Test Results
PS01. Ariba	Quarterly reviews are performed to verify that access to colocation data centers is restricted to authorized individuals. *This control was in place from October 1, 2022 to March 4, 2023*	Inspected the Ariba Data Center Quarterly Review Policy to determine whether requirements for performing quarterly data center access reviews were defined and documented. For a selection of quarters, inspected quarterly user access review documentation to determine whether quarterly reviews were performed to verify that access to colocation data centers was restricted to authorized individuals and corrective action was taken, where required.	No exceptions noted.

Control Objective Ref.	Control Objective Description
PS	Controls provide reasonable assurance that physical access to server rooms and secured areas within data centers is restricted to authorized personnel and such facilities are protected from environmental hazards.

Control Ref.	Control Description Provided by SAP	KPMG's Test Procedures	KPMG's Test Results
PS03b	When access to a Colocation data center is no longer required (such as expiration of access authorization, transfer, or termination), access is removed in a timely manner. *This control was in place from October 1, 2022 to March 4, 2023*	Inspected the policies regarding data center access to determine whether processes and guidelines for the revocation of permanent access to the data centers were defined and documented. For all employees and external workers terminated during the examination period, inspected the data center access lists for the Colocation data centers to determine whether access rights were revoked in a timely manner.	No exceptions noted.
PS06	Backup power supply is available for the data centers in case of primary power failure. To help ensure proper functionality, backup power generators are maintained on a regular basis. Maintenance is documented by the supplier company providing a report. *This control was in place from October 1, 2022 to March 4, 2023*	Inspected the maintenance requirements for SAP-owned German data centers to determine whether regular maintenance and specific procedures for the backup power supply were defined. Inspected the power supply maintenance reports to determine whether maintenance was conducted by a supplier company on a regular basis. Observed the main power supply and backup power supply for all SAP-owned data centers to determine whether backup power supply was available for the data centers in case of primary power failure. Inspected the maintenance plan for SAP-owned German data center facilities to determine whether regular maintenance for backup powers supplies was scheduled in accordance to the frequency defined in the maintenance requirements for SAP data centers.	No exceptions noted.

Control Objective Ref.	Control Objective Description
PS	Controls provide reasonable assurance that physical access to server rooms and secured areas within data centers is restricted to authorized personnel and such facilities are protected from environmental hazards.

Control Ref.	Control Description Provided by SAP	KPMG's Test Procedures	KPMG's Test Results
PS07	The data center is equipped with appropriate fire emergency systems. To help ensure proper functionality, fire emergency systems are tested and maintained on a regular basis. Maintenance is documented by the supplier company providing a report. *This control was in place from October 1, 2022 to March 4, 2023*	Observed the fire emergency systems in the data centers to determine whether fire detection systems were in place. Inspected the maintenance plan for SAP-owned German data center facilities to determine whether regular maintenance for the fire suppression system was scheduled in accordance to the frequency defined in the maintenance requirements for SAP data centers. Inspected the documentation of the fire protection exercises and fire protection inspections for the SAP-owned data centers to determine whether the fire protection exercise and fire protection inspection was regularly conducted. Inspected the fire emergency system maintenance reports for the German data center facilities to determine whether maintenance was conducted by a supplier company on a regular basis. Inspected the maintenance requirements for SAP-owned German data centers to determine whether regular maintenance and specific procedures for the fire suppression system were defined.	No exceptions noted.

Control Objective Ref.	Control Objective Description		
PS	Controls provide reasonable assurance that physical access to server rooms and secured areas within data centers is restricted to authorized personnel and such facilities are protected from environmental hazards.		
Control Ref.	**Control Description Provided by SAP**	**KPMG's Test Procedures**	**KPMG's Test Results**
PS08	Systems are operating within a required temperature scale. The data center is equipped with air conditioning systems. To help ensure proper functionality, the air conditioning systems are tested and maintained on a regular basis. Maintenance is documented by the supplier company providing a report. *This control was in place from October 1, 2022 to March 4, 2023*	Inspected the maintenance requirements for SAP-owned German data centers to determine whether regular maintenance and specific procedures for the air conditioning systems were defined. Observed the cooling systems in the SAP-owned data centers to determine whether they were equipped with air conditioning systems. Inspected the maintenance plan for SAP-owned German data center facilities to determine whether regular maintenance for the air conditioning systems was scheduled in accordance to the frequency defined in the maintenance requirements for SAP data centers. Inspected maintenance reports for the SAP-owned German data center facilities to determine whether maintenance and testing of air conditioning systems was conducted by a supplier company.	No exceptions noted.

Control Objective User and Access Management

Control Objective Ref.	Control Objective Description
UAM	Controls provide reasonable assurance that logical access to production systems and data files is restricted to authorized personnel.

Control Ref.	Control Description Provided by SAP	KPMG's Test Procedures	KPMG's Test Results
2.01_Ariba	Formal user access management procedures have been documented and made available to relevant administrative users.	Inspected the SAP Ariba Cloud Ops - Production Access Request Process document to determine whether formal user access management policies were defined, documented, and communicated to system administrators.	No exceptions noted.
2.02_Ariba	User additions to production systems are required to have authorization by Operations Management.	Inspected the Cloud Ops - Production Access Request Process document to determine whether the provisioning process was defined and documented. For a selection of users provisioned to the production environment, inspected access request tickets and a user access list to determine whether access was documented and authorized by Operations Management and access was provisioned according to the request.	No exceptions noted.

Control Objective Ref.	Control Objective Description
UAM	Controls provide reasonable assurance that logical access to production systems and data files is restricted to authorized personnel.

Control Ref.	Control Description Provided by SAP	KPMG's Test Procedures	KPMG's Test Results
2.03_Ariba	System Access procedures are documented that define access control requirements for restricting access to the least privilege necessary for privileged users to perform job responsibilities and maintain segregation of duties for production access.	Inspected the Cloud Ops - Segregation of Duties and Safeguard Access - Roles Definition policies to determine whether requirements for segregation of duties were defined and documented. Inspected job titles and assigned teams for all users with access to deploy application changes to determine whether they were appropriate. Inspected the GitHub admin listing, deployer listing, and production listing to determine whether: • GitHub admins (with access to modify branch protection to the code repositories) were appropriate based on their job titles. • Deployers (with access to the master password) were appropriate based on their job titles. • GitHub admins and deployers were segregated. • GitHub admins and production users were segregated.	No exceptions noted.
2.05_Ariba	SAP Ariba's password settings are configured in accordance with the SAP Global Security Standard.	Inspected the SAP Global Security Standard for Accounts and Passwords to determine whether password requirements were defined. Observed a user attempt to change their password using invalid parameters to determine whether the system was configured to enforce the password settings. Inspected the system password settings to determine whether they were configured in accordance with the SAP Global Security Standard.	No exceptions noted.

Control Objective Ref.	Control Objective Description
UAM	Controls provide reasonable assurance that logical access to production systems and data files is restricted to authorized personnel.

Control Ref.	Control Description Provided by SAP	KPMG's Test Procedures	KPMG's Test Results
2.06_Ariba	The ability to login, via shell or command line to production servers is restricted to authorized personnel by a Bastion Host using two-factor authentication.	Inspected the Pluggable Authentication Module (PAM) configuration to determine whether two-factor authentication was in-place. Observed a system administrator traverse the authentication points required to gain logical access to the production network to determine whether the user was required to authenticate via a bastion host and that two-factor authentication was required.	No exceptions noted.
2.07_Ariba	Keyshell logging is in place to provide an audit trail of actions performed while logged into the production environment via the Bastion Host.	Inspected a system output of accounts that are not configured with keyshell logging to determine whether there were any user accounts that were identified. Observed a system administrator run a key-capture command to determine whether user input was captured and logged. Inspected the list of individuals with the ability to view or modify keyshell log permissions to determine whether it was limited to appropriate personnel.	No exceptions noted.
2.08_Ariba	Access to hardware and operating system configuration tables within the revision control tool (Perforce) is restricted to authorized personnel.	Inspected a sample change pushed to production from the revision control tool to determine whether it was performed by an authorized individual. Inspected the access control lists within the revision control tool and the active HR listing to determine whether the privilege to make changes to an operating specific function to the host was restricted to authorized and appropriate personnel based on job title.	No exceptions noted.

Control Objective Ref.	Control Objective Description
UAM	Controls provide reasonable assurance that logical access to production systems and data files is restricted to authorized personnel.

Control Ref.	Control Description Provided by SAP	KPMG's Test Procedures	KPMG's Test Results
2.10_Ariba	Customer access to hosted applications requires a unique username and a password. The applications enforce an expiration date on the password of 90 days, and a password history to prevent the re-use of the last six passwords. Furthermore, the account is locked after five invalid password logon attempts.	Inspected password configurations on the Business Network to determine whether the application enforced expiration date of 90 days, password history to prevent re-use of the last six passwords, and account lockout after five invalid password logon attempts. Observed a system administrator attempt to re-use a previous password and input incorrect passwords on the Business Network to determine whether the application enforces password history to prevent re-use of the last six passwords and account lockout after five invalid password logon attempts. Observed a system administrator attempt to create a customer account on the Business Network to determine whether the system prevented the use of a non-unique username.	No exceptions noted.
2.11_Ariba	Customer access is segregated such that users may only view or access their own assigned data which is linked to their organizational and user ID.	Inspected database settings to determine whether users and data objects were associated with a unique identifier. Inspected the Cloud Services for SAP Ariba Solutions document to determine whether segregation of customer data was defined and documented. Observed a system administrator perform a successful and a failed attempt to view customer data to determine whether customer access was segregated such that users may only view or access their own assigned data which is linked to their organizational and user ID.	No exceptions noted.

Control Objective Ref.	Control Objective Description
UAM	Controls provide reasonable assurance that logical access to production systems and data files is restricted to authorized personnel.

Control Ref.	Control Description Provided by SAP	KPMG's Test Procedures	KPMG's Test Results
2.12_Ariba	SAP Business Network Supplier Mobile App is configured to authenticate users with a unique user account and enforce predefined password requirements.	Observed a user attempt to log-in to the SAP Business Network Supplier Mobile App to determine whether a password was required. Inspected the SAP Business Network Supplier Mobile App password configurations managed through Business Network to determine whether the application enforces expiration date of 90 days, password history to prevent re-use of the last six passwords, and account lockout after five invalid password login attempts. Inspected the authentication configuration for the SAP Business Network Supplier Mobile App to determine whether it was configured to authenticate via the Business Network environment.	No exceptions noted.

Control Objective Ref.	Control Objective Description
UAM	Controls provide reasonable assurance that logical access to production systems and data files is restricted to authorized personnel.

Control Ref.	Control Description Provided by SAP	KPMG's Test Procedures	KPMG's Test Results
UAM04a_Ariba	Production credentials are removed within seven business days after a user has been identified as a terminated employee or external worker. *This control was in place from October 1, 2022 to July 23, 2023.*	Inspected the Delete User Accounts Standard Operating Procedure to determine whether the requirements for de-provisioning terminated user access were defined and documented.	No exceptions noted.
		Inspected the configuration settings for the identification and replication of data for terminated employees or external workers to determine whether the relevant data needed to execute access revocations for terminated employees and external workers was transferred on a timely basis to SAP Global Active Directory.	Exception noted. The control is not suitably designed to remove access for terminated users as it does not include procedures to monitor that the job which updates the identity access management system processes termination data from the employee and external worker systems on a timely basis.
		Inspected the SAP Global Active Directory automated compare check job used to compare SAP Global Active Directory with SAP Ariba's Safeguard (Production Access) to determine whether it was configured to automatically identify terminated users and generate access removal tickets.	No exceptions noted.
		Inspected and compared the export of Safeguard users to the HR terminated users to determine whether any terminated users retained production access.	The design exception noted above related to the removal of access for terminated users impacted the completeness and accuracy of the data that was critical to the performance of this control attribute, and therefore KPMG was unable to test and conclude on the operating effectiveness of this control.

Control Objective Ref.	Control Objective Description		
UAM	Controls provide reasonable assurance that logical access to production systems and data files is restricted to authorized personnel.		
Control Ref.	**Control Description Provided by SAP**	**KPMG's Test Procedures**	**KPMG's Test Results**
		For a selection of terminated users, inspected access removal tickets to determine whether production access was removed within seven business days of their termination date.	The design exception noted above related to the removal of access for terminated users impacted the completeness and accuracy of the data that was critical to the performance of this control attribute, and therefore KPMG was unable to test and conclude on the operating effectiveness of this control. *Refer to Section V for management's response.*

Management's Evaluation:
SAP conducted a complete review of all employee and external worker terminations during the period October 1, 2022 to March 31, 2023 to (i) identify all of the instances where users had their access removed untimely, (ii) assess whether any of these users had access to Ariba's production environment, and (iii) if any of these users did have such access, whether they were removed timely within Ariba's production environment (seven business days or less), and (iv) if any of these users did have such access and were not removed timely within Ariba's production environment (>seven business days), whether they logged into Ariba's production environment post-termination.

SAP determined that, while there were terminated employees (no external worker) who maintained access to Ariba's production environment for longer than seven business days post-termination, none of these users logged into production post-termination date.

Additional Procedures Performed by KPMG over Management's Evaluation:
Inspected and reperformed aspects of management's analysis over employee and external worker terminations during the period October 1, 2022 to March 31, 2023 and determined that SAP management obtained a complete and accurate population of employee and external worker terminations. Further, we determined that SAP management performed a complete review over the users within these populations to identify those (i) whose access was removed untimely and (ii) who had access to Ariba's production environment, and to validate that these users did not login to Ariba's production environment post-termination date. No exceptions noted.

Control Objective Ref.	Control Objective Description
UAM	Controls provide reasonable assurance that logical access to production systems and data files is restricted to authorized personnel.

Control Ref.	Control Description Provided by SAP	KPMG's Test Procedures	KPMG's Test Results
UAM04b_Ariba	For employees who transfer between roles (i.e. organizational or cost center change), production credentials are deactivated within 30 business days, unless management confirms it is necessary for the employee to retain access. *The control was remediated as of July 24, 2023.*	October 1, 2022 - July 23, 2023 Inspected the SAP Ariba Cost Center Movers Procedure document to determine whether the requirements for reviewing and removing production access for transferred users were defined and documented.	No exceptions noted.
		Inspected the configuration settings for the identification and replication of data for employees who transfer between roles to determine whether the relevant data needed to execute access revocations for employees who transfer between roles was transferred on a timely basis to the SAP Global Active Directory.	Exception noted. The control is not suitably designed to deactivate access for employees who transfer between roles, as it does not include procedures to monitor that the job which updates the identity access management system processes job role change data from the employee system on a timely basis.
		Inspected SAP Global Active Directory automated compare check job used to compare SAP Global Active Directory with SAP Ariba's Safeguard (Production Access) to determine whether it was configured to automatically identify employees who transferred roles and generate access confirmation/modification tickets.	No exceptions noted.
		For a selection of transferred employees, inspected access removal tickets to determine whether manager approval was obtained for access retention, or production access was removed within 30 business days.	The design exception noted above related to the deactivation of access for employees who transfer between roles impacted the completeness and accuracy of the data that was critical to the performance of this control attribute, and therefore KPMG was unable to test and conclude on the operating effectiveness of this control.

Control Objective Ref.	Control Objective Description
UAM	Controls provide reasonable assurance that logical access to production systems and data files is restricted to authorized personnel.

Control Ref.	Control Description Provided by SAP	KPMG's Test Procedures	KPMG'sTest Results
			Refer to Section V for management's response.
		July 24, 2023 - September 30, 2023	
		Inspected the SAP Ariba Cost Center Movers Procedure document to determine whether the requirements for reviewing and removing production access for transferred users were defined and documented.	No exceptions noted.
		Inspected the configuration settings for the identification and replication of data for employees who transfer between roles to determine whether the relevant data needed to execute access revocations for employees who transfer between roles was transferred on a timely basis to the SAP Global Active Directory.	No exceptions noted.
		Inspected SAP Global Active Directory automated compare check job used to compare SAP Global Active Directory with SAP Ariba's Safeguard (Production Access) to determine whether it was configured to automatically identify employees who transferred roles and generate access confirmation/modification tickets.	No exceptions noted.
		For a selection of transferred employees, inspected access removal tickets to determine whether manager approval was obtained for access retention, or production access was removed within 30 business days.	No exceptions noted.
UAM11_Ariba	User Access Reviews are conducted quarterly for all production accounts. The results of the review are documented and deviations resolved timely.	For a selection of quarterly user access reviews, inspected user access review documentation to determine whether they were completed. For a selection of manager reviews, inspected user access review documentation to determine whether they were documented, and any deviations were resolved.	No exceptions noted.

Control Objective Ref.	Control Objective Description		
UAM	Controls provide reasonable assurance that logical access to production systems and data files is restricted to authorized personnel.		
Control Ref.	**Control Description Provided by SAP**	**KPMG's Test Procedures**	**KPMG's Test Results**
UAM04a_Internal_Leavers_Ariba	Production credentials for internal employees are removed within seven business days after a user has been identified as a terminated employee. *The control was implemented on July 24, 2023.*	Inspected the Delete User Accounts Standard Operating Procedure document to determine whether the requirements for reviewing and removing production access were defined and documented. Inspected the configuration settings for the identification and replication of data for terminated employees to determine whether the relevant data needed to execute access revocations for terminated employees was transferred on a timely basis to SAP Global Active Directory. Inspected the SAP Global Active Directory automated compare check job used to compare SAP Global Active Directory with SAP Ariba’s Safeguard (Production Access) to determine whether it was configured to automatically identify terminated employees and generate access removal tickets. Inspected and compared the export of Safeguard users to the HR terminated employees to determine whether any terminated employees retained production access. For a selection of terminated employees, inspected access removal tickets to determine whether production access was removed within seven business days of their termination date.	No exceptions noted.

Control Objective Ref.	Control Objective Description		
UAM	Controls provide reasonable assurance that logical access to production systems and data files is restricted to authorized personnel.		
Control Ref.	**Control Description Provided by SAP**	**KPMG's Test Procedures**	**KPMG's Test Results**
UAM04a_External_Leavers_Ariba	Production credentials for external workers are removed within seven business days after a user has been identified as a terminated external worker. *The control was implemented on July 24, 2023.*	Inspected the Delete User Accounts Standard Operating Procedure document to determine whether the requirements for reviewing and removing production access were defined and documented.	No exceptions noted.
		Inspected the configuration settings for the identification and replication of data for terminated external workers to determine whether the relevant data needed to execute access revocations for terminated external workers was transferred on a timely basis to SAP Global Active Directory.	The exception noted in AS_AMON05, where the control was not designed to monitor whether the job that processes external worker termination data from Fieldglass to IDM completes on a timely basis, impacted the completeness and accuracy of the data that was critical to the performance of this control, and therefore KPMG was unable to test and conclude on the operating effectiveness of this control. *Refer to Section V for management's response.*

Control Objective Ref.	Control Objective Description
UAM	Controls provide reasonable assurance that logical access to production systems and data files is restricted to authorized personnel.

Control Ref.	Control Description Provided by SAP	KPMG's Test Procedures	KPMG's Test Results
AS_AMON 4	On a daily basis, the 1AMProduct Support team reviews the IDM job sync logs and the error notification email alerts for any errors in the transfer of D/I-user account changes or terminations from Employee Central to IDM. The team validates that the user accounts are locked/disabled in IDM and the information is fed to downstream systems that are integrated directly with IDM. Errors are resolved in a timely manner. *The control was implemented on July 24, 2023.*	Inspected the job monitoring configuration that identifies errors related to the processing of D/I-user account changes or terminations from Employee Central to IDM to determine whether the configuration was designed to identify errors. Inspected the configuration that creates the email notification for errors to determine whether the configuration was designed to alert the 1AMProduct Support Team via email. Inspected the system logs for a selection of days to determine whether the job status was tracked as successful or if an error was identified in the transfer of D/I-user account changes or terminations from Employee Central to IDM. For any processing errors identified, inspected the corresponding failure email alert and any corrective actions taken by the 1AMProduct Support team to determine whether the error was communicated, investigated, and resolved.	No exceptions noted.
AS-AMON 5	On a daily basis, the 1AMProduct Support team reviews the IDM job sync logs and the error notification email alerts for any errors in the transfer of C-user terminations from Fieldglass to IDM. The team validates that the user accounts are locked/disabled in IDM and the information is fed to downstream systems that are integrated directly with IDM. Errors are resolved in a timely manner. *The control was implemented on July 24, 2023.*	Inspected the job monitoring configuration that identifies errors with the processing of C-user terminations for external workers from Fieldglass to IDM to determine whether the configuration was designed to identify errors.	Exception noted. The control was not suitably designed to monitor whether the job that processes system termination data from Fieldglass to IDM completes on a timely basis. *Refer to Section V for management's response.*
AS_AMON 6a	The 1AMProduct Support Team reconciles the HR IT lists of terminated users from EC to data in the IT-IDM system. Discrepancies are investigated and required changes to IDM data are input manually as needed. *The control was implemented on July 24, 2023.*	For a selection of days, inspected reconciliation documentation between HR IT lists for terminated users and IT-IDM lists to determine whether discrepancies were investigated and required changes to IDM data were input manually as needed.	No exceptions noted.

Control Objective Ref.	Control Objective Description
UAM	Controls provide reasonable assurance that logical access to production systems and data files is restricted to authorized personnel.

Control Ref.	Control Description Provided by SAP	KPMG's Test Procedures	KPMG's Test Results
AS_AMON 6b	The 1AMProduct Support Team reconciles the Fieldglass IT lists of terminated users to data in the IT-IDM system. Discrepancies are investigated and required changes to IDM data are input manually as needed. *The control was implemented on July 27, 2023.*	As noted in AS_AM0N5, the control was not suitably designed to monitor whether the job that processes system termination data from Fieldglass to IDM completes on a timely basis. As a result, a complete population of terminated users (external workers) was not able to be obtained to test the operating effectiveness of this control.	The exception noted in AS_AM0N5, where the control was not designed to monitor whether the job that processes external worker termination data from Fieldglass to IDM completes on a timely basis, impacted the completeness and accuracy of the data that was critical to the performance of this control, and therefore KPMG was unable to test and conclude on the operating effectiveness of this control. *Refer to Section V for management's response.*
AS_AMON 7	On a daily basis, the 1AMProduct Support Team monitors the IDM internal jobs for any errors or long-running scripts (>16 hours runtime). The team creates an IAM JIRA Defect ticket to prioritize and resolve any issues. *The control was implemented on July 24, 2023.*	Inspected the job monitoring configuration that identifies errors or long-runners with IDM jobs to determine whether errors or long-runners are identified. Inspected the configuration that creates the email notification for errors to determine whether the configuration was designed to alert the IAM Product Support Team via email. Inspected the system logs for a selection of days to determine whether the job status was tracked as successful or error was identified for any long-running scripts. For any error or long-running scripts, inspected follow-up activities to determine whether a JIRA ticket was opened, if required, or the team performed appropriate follow-up to resolve any issues.	No exceptions noted.

Control Objective Ref.	Control Objective Description
UAM	Controls provide reasonable assurance that logical access to production systems and data files is restricted to authorized personnel.

Control Ref.	Control Description Provided by SAP	KPMG's Test Procedures	KPMG's Test Results
HR05	External workers are required to have a worker end date field populated in Fieldglass which cannot be set to greater than 13 months from the account creation or extension date. Once the worker end date is reached, or if the Fieldglass account status is manually disabled, an automated workflow within Fieldglass will trigger the user account deactivation process.	Inspected the worker end date field configuration within Fieldglass to determine whether the end date cannot be set to greater than 13 months from the external worker account creation or extension date. Inspected the automated workflow configuration in Fieldglass that triggers the user account deactivation process to determine whether external workers with a worker end date in the past had their Fieldglass accounts automatically closed. Observed a system administrator attempt to set an external worker's validity to zero to determine whether a valid worker end date was required. Observed an external worker's work order within Fieldglass to determine whether their validity was less than or equal to 13 months. Inspected an external worker ID with a recently passed worker end date to determine whether the external worker's account was automatically disabled within Fieldglass.	No exceptions noted.
HR09	On a daily basis, an end of employment pending workflow report is run from SuccessMap End of Employment. If any pending workflows are identified upon manual review with retroactive effective dates an "Instant Access Removal" is populated in Employee Central to trigger access removal by IDM. *The control was implemented on July 17, 2023.*	For a selection of days, inspected the employment pending workflow manual review documentation to determine whether the review was completed, "Instant Access Removal" was populated for any users that required instant access removal and follow-up actions were completed.	No exceptions noted.

Control Objective Ref.	Control Objective Description
UAM	Controls provide reasonable assurance that logical access to production systems and data files is restricted to authorized personnel.

Control Ref.	Control Description Provided by SAP	KPMG's Test Procedures	KPMG's Test Results
UAM04_ Term_ Impact	A quarterly review of all terminated internal employees and external workers is completed. Any terminated individuals who are removed untimely are further assessed for post-termination login activity to the production environment. For any terminated individuals who are identified as having post-termination login activity to the production environment, their activity logs are reviewed for any inappropriate events. *The control was implemented on June 30, 2023.*	For a selection of quarterly reviews, inspected management's review performed over the terminated internal employees and external workers to determine whether reviews over the terminated internal employees and external workers were completed. For all terminated internal employees and external workers identified as being removed untimely in the selected quarterly reviews, inspected management's review of a production access listing and activity logs to determine whether any untimely terminated individuals had access to the production environment post-termination date, and, forthose identified, whether they had any inappropriate events in the production environment post-termination date. Based on the above test procedures, determined that no inappropriate events by terminated employees occurred during the period from April 1, 2023 through September 30, 2023.	No exceptions noted.

Control Objective Ref.	Control Objective Description
UAM	Controls provide reasonable assurance that logical access to production systems and data files is restricted to authorized personnel.

Control Ref.	Control Description Provided by SAP	KPMG's Test Procedures	KPMG's Test Results
UAM04_ Changers_ Impact	A quarterly review of all internal employee changers / transfers is completed. Any changers / transfers who are reviewed or removed untimely are further assessed for post-transfer login activity to the production environment. For any changers / transfers who are identified as having post-transfer login activity to the production environment, their activity logs are reviewed for any inappropriate events. *The control was implemented on September 15, 2023.*	For a selection of quarters, inspected management's reviews performed over the internal employee changers / transfers to determine whether the reviews over the internal employee changers/ transfers were completed and covered changers/transfers that occurred during the period from April 1, 2023 through September 30, 2023. For internal employee changers / transfers identified as being removed untimely in the selected quarterly reviews, inspected management's review of a production access listing and activity logs to determine whether any untimely removed internal employee changers / transfers had access to the production environment post-transfer date, and, for those identified, whether they had any inappropriate events in the production environment post-transfer date. Based on the above test procedures, determined that no inappropriate events by employee changers / transfers occurred during the period from April 1, 2023 through September 30, 2023.	No exceptions noted.

Control Objective Ref.	Control Objective Description
UAM	Controls provide reasonable assurance that logical access to production systems and data files is restricted to authorized personnel.

Control Ref.	Control Description Provided by SAP	KPMG's Test Procedures	KPMG's Test Results
UAM04_PIT	A point-in-time quarterly review of all active internal employees and external workers SAP IT Identity Management (IDM) accounts is completed. Active IDM accounts identified without an associated active HR (Employee Central/Fieldglass) record are further assessed for post-termination login activity to the production environment. For any employees and external workers who are identified as having post-termination login activity to the production environment, their activity logs are reviewed for inappropriate events. *The control was implemented on July 4, 2023.*	For a selection of quarters, inspected management's point-in-time review performed for all active internal employee and external worker IDM accounts compared against active HR (Employee Central/Fieldglass) listings to determine whether reviews over the internal employees and external workers were completed. For employees and external workers who were identified as having active IDM accounts without an associated active HR (Employee Central/Fieldglass) record, inspected management's review of a production access listing and activity logs to determine whether they had any inappropriate events in the production environment post-termination date. Based on the above test procedures, determined that no inappropriate events by terminated employees occurred as of July 4, 2023 and September 29, 2023.	No exceptions noted.

Section V

Other Information Provided by Management of SAP

Provided by KPMG LLP

Management's Response

Regarding the exceptions noted by KPMG during the examination period, SAP provided the following management's response:

SAP's Control	**BR03b** To help ensure the durability, the backup data is transmitted through encrypted communication channel to a remote site.
Applicable Control Objective	Backup and Restore: Controls provide reasonable assurance that computer systems are backed up to storage media and that procedures are employed to maintain the integrity of the storage media.
Exceptions noted	**<u>October 1, 2022 to October 22, 2022:</u>** The control was not designed appropriately to use an encrypted communication channel for the replication of full copies of production data.

Management's Response:

Encryption for HANA System Replication (HSR) between nodes was not enabled because, upon deployment, applications were unable to connect to HANA. The issue was remediated by October 23, 2022. There is no impact on security. HSR replication is always on private network and confidential data (i.e., PCI data) is encrypted at an application level, which results in encrypted confidential data in the replication stream.

SAP's Control	**UAM04a_Ariba** Production credentials are removed within seven business days after a user has been identified as a terminated employee or external worker. ***(The control was in place from October 1, 2022 through July 23, 2023)***
Applicable Control Objective	LIAM: Controls provide reasonable assurance that logical access to production systems and data files is restricted to authorized personnel.
Exception noted	The control is not suitably designed to remove access for terminated users as it does not include procedures to monitor that the job which updates the identity access management system processes termination data from the employee and external worker systems on a timely basis.
Additional Observations by Management	Management of SAP identified instances of delayed user terminations across the enterprise during the complete review of all terminations that indicated deficiencies in the operating effectiveness of control UAM04a_Ariba, as further described below: • During a batch upload of terminated internal employees, a key field in the employee termination record needed for mass termination recognition by SAP IT IDM was not updated. As such, SAP IT IDM did not identify these terminated users for access revocation and, consequently, the access was not revoked in a timely manner. The employee termination record was remediated as of July 13, 2023. • Additionally, SAP identified instances where an employee's termination was not processed timely in the employee system and, once processed, the date of the termination was backdated. This manifested in a gap between the backdated termination date and the date when removal of user access was triggered resulting in the 7-day timeframe for access revocation being exceeded and flagged in management's impact assessment. SAP has implemented as of July 17, 2023 controls to monitor for internal employee terminations that are not processed timely in the employee system that are backdated. When discrepancies, including termination backdating, are identified, control AS_AMON6a, implemented as of July 24, 2023, includes an attribute for the manual update to IT-IDM to resolve the discrepancies between EC and IT-IDM.

Management's Response for Exception Noted:
SAP conducted a complete review of all employee and external worker terminations during the period April 1, 2022 to March 31, 2023 to (i) identify all of the instances where users had their access removed untimely, (ii) assess whether any of these users had access to Ariba's production environment, and (iii) if any of these users did have such access, whether they logged into Ariba's production environment post-termination.

SAP determined that, while there were terminated employees (no external worker) who maintained access to Ariba's production environment for longer than seven business days post-termination, none of these users logged into production post-termination date.

For the period of April 1, 2023 to July 23, 2023 SAP management implemented the following controls to address the risks that changers/transfers and terminated users (employee and external workers) may have access beyond their termination date:

- UAM04_Term_Impact - to assess whether any terminated internal employees or external workers had inappropriate access to production post termination.

Based on the performance of these controls, management concluded that there is no indication of unauthorized access that affects customer data during the report period of April 1, 2023 through July 23,2023.

SAP management also implemented UAM04_PIT - which addresses whether all active IDM accounts were appropriate or had any inappropriate events as of July 4, 2023. Management concluded that none of the active IDM accounts had inappropriate events.

SAP's Control	**UAM04b_Ariba** For employees who transfer between roles (i.e., organizational or cost center change), production credentials are deactivated within thirty business days, unless management confirms it is necessary for the employee to retain access.
Applicable Control Objective	User and Access Management: Controls provide reasonable assurance that logical access to production systems and data files is restricted to authorized personnel.
Exceptions noted	The control is not suitably designed to modify access for employees that have transferred roles as it does not include procedures to monitor that the job which updates the identity access management system processes job change data from the HR systems on a timely basis.

Management's Response:

For the period of April 1, 2023 to July 23, 2023 SAP management implemented the following controls to address the risks that changers/transfers (internal employees) may have access beyond their job change date:

- UAM04_Changers_Impact - to assess whether any internal employee changers had inappropriate access to production post change date.

Management concluded that there is no indication of unauthorized access that affects customer data during the report period of April 1, 2023 through July 23,2023.

Additionally, for the period October 1, 2022 to July 23, 2023, SAP notes that delayed modifications of access for employees changing job roles would be identified by control UAM11_Ariba through the performance of the user access review. SAP also notes that the risks resulting from the deficiency in control UAM04b_Ariba related to employees changing job roles is further mitigated by 2.02_Ariba which requires production access to be approved by appropriate personnel, 2.03_Ariba which requires the access to GitHub administrators to be restricted to appropriate users, requires access for deployers to be restricted to appropriate users, and requires segregation of duties between developers and deployers, 2.08_Ariba which requires the access to the revision control tool (Perforce) to be restricted to appropriate users, and 5.09_Ariba which requires code changes to go review.

SAP management formalized monitoring activities and implemented alerting from SAP IT IDM during the period. As of July 24, 2023, management has established controls to address monitoring over the job which updated the identity access management system (IDM) and job change data from the employee system. Refer to the response in AS_AMON5, for further responses on monitoring controls and lookback controls established during the period.

SAP's Control	**AS_AM0N5** On a daily basis, the 1AMProduct Support team reviews the IDM job sync logs and the error notification email alerts for any errors in the transfer of C-user terminations from Fieldglass to IDM. The team validates that the user accounts are locked/disabled in IDM and the information is fed to downstream systems that are integrated directly with IDM. Errors are resolved in a timely manner. The control was implemented on July 24, 2023. **AS_AMON6b** The 1AMProduct Support Team reconciles the Fieldglass IT lists of terminated users to data in the IT-IDM system. Discrepancies are investigated and required changes to IDM data are input manually as needed. The control was implemented on July 27, 2023. **UAM04a_External_Leavers_Ariba** Production credentials for external workers are removed within seven business days after a user has been identified as a terminated external worker. The control was implemented on July 24, 2023.
Applicable Control Objective	UAM: Controls provide reasonable assurance that logical access to production systems and data files is restricted to authorized personnel.

Exceptions noted	**AS_AM0N5:** The control was not suitably designed to monitor whether the job that processes external worker termination data from Fieldglass to IDM completes on a timely basis. **AS_AM0N6b:** The exception noted in AS_AM0N5, where the control was not designed to monitor whether the job that processes external worker termination data from Fieldglass to IDM completes on a timely basis, impacted the completeness and accuracy of the data that was critical to the performance of this control, and therefore KPMG was unable to test and conclude on the operating effectiveness of this control. **UAM04a_External_Leavers_Ariba:** The exception noted in AS_AM0N5, where the control was not designed to monitor whether the job that processes external worker termination data from Fieldglass to IDM completes on a timely basis, impacted the completeness and accuracy of the data that was critical to the performance of this control, and therefore KPMG was unable to test and conclude on the operating effectiveness of this control.

Management's Response for Exception Noted:

Since identification of the UAM04a_Ariba deficiency related to delays in modification of access for employees and external workers related to leavers (terminations) and changers/transfers for employees, SAP management formalized monitoring activities and implemented alerting from SAP IT IDM during the period.

As of July 24, 2023 management has established the following controls to address monitoring over the job which updated the identity access management system (IDM) and job change data for employee terminations and employee changers/transfers:

- AS_AMON4 - Employee Central to SAP IT IDM Monitoring
- AS_AMON6a - Weekly reconciliation (3 times per week) of active users in EC and SAP IT IDM
- AS_AMON7 - SAP IT IDM Monitoring

The above listed controls were working effectively.

For external worker leavers (terminations), monitoring controls AS_AMON5 and AS_AMON6b were also implemented on July 24, 2023 and July 27, 2023 respectively with regards to termination data from external worker systems. AS_AMON5 contained a design deficiency as the control did not fully monitor for data transfer issues for external worker leavers (terminations) from Fieldglass to IDM. As a result, this impacted the completeness and accuracy of the data that was critical to the performance of the AS_AMON6b and UAM04a_External_Leavers_Ariba controls. As of November 2023, remediation actions were completed in establishing additional monitoring function as part of AS_AMON5.

SAP management also implemented the following controls to address the risks that changers/transfers and terminated users (employee and external workers) may have access beyond their job change date or termination date:

- UAM04_Term_Impact - to assess whether any terminated internal employees or external workers had inappropriate access to production post termination.
- UAM04_Changers_Iimpact - to assess whether any internal employee changers had inappropriate access to production post change date.

Management concluded that there is no indication of unauthorized access that affects customer data during the report period of April 1, 2023 through September 30, 2023.

SAP management also implemented UAM04_PIT - which addresses whether all active IDM accounts were appropriate or had any inappropriate events as of July 4, 2023 and September 29, 2023. Management concluded that none of the active IDM accounts had inappropriate events.