Cloud Services for SAP Ariba® Solutions

January 2021

Table of Contents

Chapter 1 – Introduction

The Security Vision of SAP Ariba Solutions

Today's cloud technologies power levels of innovation, agility, and efficiency that no other approach can provide. That's why companies are moving to the cloud faster than ever, with the majority already capitalizing on cloud solutions or making active plans to adopt them. Yet security, privacy, performance, and availability concerns cause many organizations to perform their due diligence before using a cloud solution. For example, cyberattacks pose a serious and growing threat and may cause a devastating data breach that can damage a customer's reputation.

By choosing partners you can depend on, you reap the rewards with less risk. SAP Ariba solutions deliver an unparalleled, world-class security strategy uniquely designed to safeguard your digital transformation – enabling you to build secure, run secure, and stay secure in the cloud.

This document covers the cloud services for SAP Ariba solutions, and our model is based on the following principals:

- Building "security in" with guided security investments that mitigate risks, strengthen defense, and reduce vulnerabilities
- Building a high availability architecture with redundant sites in data governance zones
- Creating business continuity plans with data privacy
- Supporting risk governance and certifications

Chapter 2 – Cloud Architecture of SAP Ariba Solutions

Why Use the Cloud?

Companies of all sizes share the same challenge: How to meet the growing demands of their business while effectively managing costs and quick time to value. By providing a combination of low startup costs, few IT resources required for startup and maintenance, rapid deployment, ease of use, and increasingly robust functionality, cloud services are successfully meeting this challenge.

Technical Details of Cloud Services for SAP Ariba Solutions

The cloud service for SAP Ariba solutions is a true SaaS model-IV solution.

Cloud services are deployed to multiple data centers throughout the world. The data centers are geographically located in regional pairs. Data is replicated between the regional pairs so that data remains in the region of deployment.

An SaaS IV system is scalable to an arbitrarily 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. As a result, scaling resources does not require any rearchitecting of the applications, so changes and fixes can be rolled out to thousands of tenants as easily as for a single tenant.

SAP Ariba solutions are powered by high-performance servers and utilize a network infrastructure designed for scalability, reliability, and security. SAP Ariba solutions implement an n-tier network architecture that physically segments Web, application, and data tiers. The communication protocols used between the systems are TCP/IP-based. The Cloud Engineering Services team constantly monitors and maintains all systems. Redundant load balancing and security firewall devices are inserted between each tier of SAP Ariba solutions.

The following description provides a detailed overview of the path of a request from an SAP Ariba solutions customer to an SAP Ariba solutions service:

1. The customer connects through a browser to the appropriate Internet URL address.
2. The user request passes through perimeter routers and the first level of firewalls, and the connection is terminated by a redundant set of load balancers.
3. The load balancers use a round-robin and source-IP/cookie-based SSL persistence to determine which Web server should be connected, and then reissues another connection to it.
4. The Web server accepts the request and identifies which application node to send the request based on the URL and a round-robin protocol. The Web server initiates another connection to the application node, which traverses through a second layer of firewalls.
5. The application servers accept the request, process application-level security and authorization checks, interpret the request, and determine if data interaction is required.
6. If data interaction is required, the application servers issue requests through a third layer of firewalls to the database servers or the file servers.
7. The database servers and file servers return the requested data back to the application server layer, which generates the required response.

8. Application servers send the response back to the Web server layer, which returns the response to the original requester.

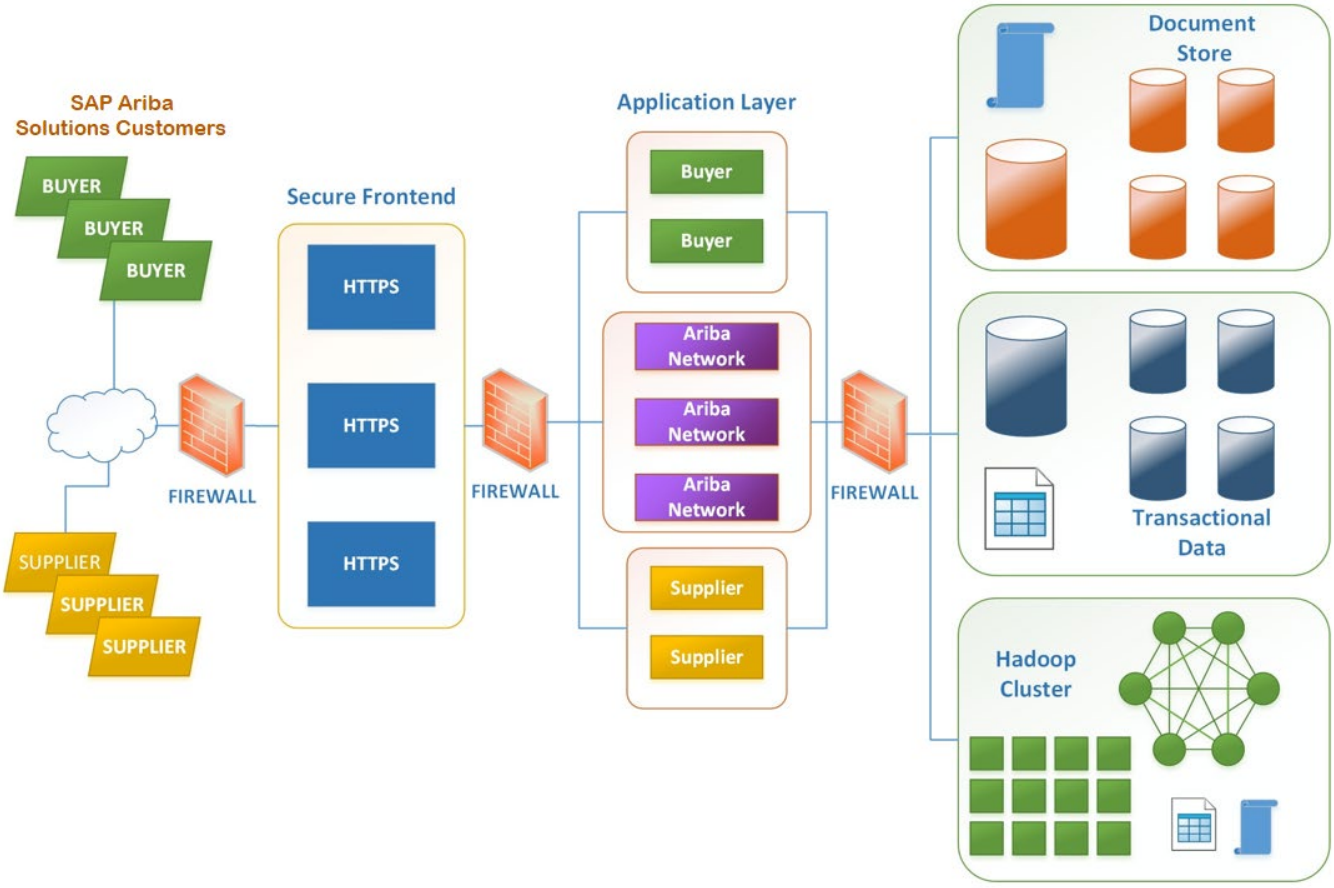


Figure 1: High-Level SAP Ariba Solutions Infrastructure Architecture

Internet Connections

SAP Ariba solutions maintain diverse redundant connections to the Internet through top-tier carriers. These are configured using BGP (Border Gateway Protocol) for redundancy. BGP is used to achieve 100% network uptime, providing redundancy for IP networks.

Switches and Routers

SAP Ariba solutions use cutting-edge technology and industry-standard equipment for ensuring optimum network connection performance. They deliver enterprise-class versatility, integration, and power to SAP Ariba solutions. Together, these routers provide the required support for Internet and intranet access with firewall security.

Routers are the primary networking components in SAP Ariba solutions. 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.

Load Balancers

SAP Ariba solutions' load balancers control traffic and guarantee optimal utilization of the Web servers. Although it is not considered a security component, the load balancers provide access control functionality to 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.

The load balancers are used as SSL-termination end points for TLS 1.2 initiated sessions.

Firewalls

SAP Ariba solutions employ next-generation firewall appliances that deliver strong security and performance and create almost no network performance impact. The solutions enforce secure access between an internal network and Internet, extranet, or intranet links.

SAP Ariba solutions use cutting-edge technology and industry-standard equipment to control the traffic to and from the Internet, between the corporate intranet of SAP Ariba solutions and the cloud solutions, and between the cloud solutions' servers. The firewall servers are configured for high-availability configuration setup.

Specifically, firewall servers are used in each level of data communication within SAP Ariba solutions:

- Between the Internet and Web servers
- Between the Web servers and the application servers
- Between the application servers and the database servers

These firewall appliances allow the Cloud Engineering Services team to rigorously protect SAP Ariba solutions from unauthorized access, providing full firewall security protection.

Additionally, SAP Ariba solutions use Citrix Workspace software to protect customer data from unauthorized corporate SAP Ariba solutions users, allowing only cloud engineering services personnel access for limited periods of time.

Application System Topology

All major application services developed and hosted by SAP Ariba solutions consist of three basic software layers:

- Secure front end and HTML rendering layer: This layer renders application objects and data in HTML/XML templates for display in client browsers.
- Application layer: The application logic layer is coded primarily in Java. This layer handles client requests using the core business application logic and interacts with the persistence layer to persist data and retrieve data from the underlying database.
- Storage and persistence layer: The persistence layer interacts with the underlying document store and relational database to manage the object-to-relational mapping. The persistence layer stores and retrieves application data. SAP Ariba solutions use the SAP HANA database software and management utilities.

SAP Ariba solutions offer a Java-based, N-tiered service that leverages open standards and intranet and Internet technology to deliver a broad range of functionality. SAP Ariba solutions were built using open standards such as Java, XML, HTTPS, HTML, and Java Database Connectivity (JDBC) to enable support for a variety of computing platforms.

Client Tier and Customer Access

SAP Ariba solutions are thin client solutions. Cloud solution customers (users) access the solution through a browser and use HTML and JavaScript for presentation. The client browser communicates with the Web server tier using HTTPS over any connection to the Internet. SAP Ariba solutions support various browsers on Windows and Mac platforms. The login page indicates the browsers supported. For the most up-to-date list of compatible browser version, please visit the SAP Help Portal site.

Web Server–Secure Front End

The Web server passes (or "proxies") requests from client browsers to the SAP Ariba solutions application server tier using HTTPS. The Web server also serves static content such as images to the browsers. The Web server uses a proxy plug-in from the application server vendor to communicate with the application server tier.
SAP Ariba solutions support multiple Web servers, communicating with the application server tier. Client requests can be load-balanced across multiple Web servers as desired.

Application Server Application Layer

Applications for SAP Ariba solutions are deployed on multiprocessor servers that utilize Red Hat operating systems and Apache Tomcat as the application server software. Each server can support multiple application nodes as determined by load testing and performance optimization. Application servers for SAP Ariba solutions are configured with redundancy in mind, allowing them to handle increased system loads if one or more servers go offline.

The collaborative business commerce services of SAP Ariba solutions consist of multithreaded Java 2 Enterprise Edition (J2EE) modules that run as servlets within a J2EE application server environment. The cloud solutions leverage features of the J2EE application servers such as the HTTPS server, thread pools, and session management. SAP Ariba solutions use threads within the J2EE application server to provide a pool of shared services for handling client requests and a pool of persistent database connections that use native JDBC drivers for database interaction.

Storage Tier – Database and Document

SAP Ariba solutions use standard relational database technology for object persistence, transaction management, and query processing. SAP Ariba solutions persist object state to the underlying relational database and rely on the database for managing transactional concurrency. SAP Ariba solutions submit standard JDBC transactions to the database and do not consider a change as persistent until the database replies with a successful commit message. SAP Ariba solutions do not use two-phase commit or mid-tier transaction management technology – transactions are managed by the underlying relational database.

SAP Ariba solutions store attachments on a file store, and some documents are stored in the database to provide robustness and consistency with how other documents are stored. Only documents and attachments from the SAP Ariba Contract solution and the SAP Ariba Sourcing solution are stored in the database. All other cloud solutions store documents and attachments within a document storage system.

Chapter 3 – Security Mechanisms and Procedures

Today's threats are more sophisticated and more targeted than ever before. SAP Ariba solutions deploy a defense-in-depth approach to protect information assets. This well-known best-practice security strategy layers security controls to better ensure that no single point of failure exists that might enable an attacker to gain unauthorized access if one control is exploited. A defense-in-depth approach typically includes both perimeter protection (such as firewall and intrusion detection systems) and end-point protection (such as application whitelisting and disk encryption). This section provides an overview of the security model of SAP Ariba solutions.

SAP Ariba solutions recognize that security is a critical component of effective electronic commerce architecture and takes necessary security measures to protect any information passed between buyers and suppliers. SAP Ariba solutions implement security using a variety of hardware, software, and procedural best practices, detailed below.

Physical Security

Only certified representatives of SAP Ariba solutions have access to the solutions' computers within the data centers. These data centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, biometrics access control, and other measures to prevent equipment and data center facilities from being compromised.

Operating Systems Security

Operating systems, when installed through default means and with default settings, are typically not secure and often include superfluous applications and services that not are not necessary. SAP Ariba solutions have standardized operating systems' installations based on best practices. The solutions' servers are configured with just the applications and services required to run the server as designed. Services not required are disabled and binary files not required for operation are removed, which reduces the total number of vulnerabilities a system may have.

The standardized installation process of SAP Ariba solutions also ensures that all servers of the same type are configured the same, 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 comply with security standards. SAP Ariba solutions use this configuration process to "harden" the operating system prior to implementing additional controls as detailed below.

Web Servers and Web Tier

SAP Ariba solutions' Web tier utilizes Web servers in conjunction with F5 load-balancers to provide perimeter security for all SAP Ariba solutions in the cloud. F5 provides TLS termination (SSL) and enables support for modern strong encryption, including elliptic curve ciphers and 256-bit encryption. Connectivity between F5 and the Web servers are also protected with a TLS connection behind F5's Internet perimeter.

Web servers are deployed in a highly-available and fault-tolerant cluster deployment. As is typical for cloud solutions, F5 balances the user load across the available servers in the Web-server cluster. The Web servers then distribute these requests across the available application servers.

Intrusion Detection System

SAP Ariba solutions use both network-based and host-based intrusion detection. This technology provides logging and alert capabilities to assist in the detection of malicious acts and misuse. An automated script generates a daily intrusion detection report. An on-call production operations engineer reviews the intrusion detection report on potential security breaches for possible incidents daily. Any potential incidents are subsequently addressed and resolved, then reviewed by production operations management.

SAP Ariba employs an intrusion protection systems (IPS) to detect and prevent identified threats at our data centers. The IPS devices have intrusion detection system (IDS) mode enabled and are configured in Symmetric mode to protect against Distributed Denial-of-Service (DDoS) attacks. The IPS configuration implemented has performed consistent with best practices recommendations provided by the vendor.

SAP Ariba solutions conduct periodic security reviews and vulnerability assessments. Results are analyzed and followed up by the information security department.

Security Incident and Event Management (SIEM)

SAP Ariba solutions implements a dedicated appliance to provide security analytics and to meet compliance requirements with SIEM in production environments. A SIEM is classified as a “security information and event management” utility. This is a collection of hardware and software processes that ingest information from logs, net flow, and additional security services as needed. The sensors are deployed throughout the network to collect logs and monitor network traffic. This provides the five essential security capabilities – behavioral monitoring, SIEM, intrusion detection, asset discovery, and vulnerability assessment – for complete visibility.

The SIEM server aggregates and correlates information that the sensors gather and provides single-pane-of-glass management, reporting, and administration.

Incident Response

SAP Ariba solutions have developed a computer security incident response team. Following policies and procedures, this team responds to suspected security incidents to mitigate risks and damage. The team conducts response and forensic analysis of systems and network traffic. This information can be used to assist with prosecution if a security breach is detected and the offender caught.

Corporate Network Security for SAP Ariba Solutions

A firewall separates the corporate network of SAP Ariba solutions from the solutions’ cloud infrastructure. Therefore, unauthorized SAP employees cannot access the cloud solutions’ data from the corporate network infrastructure. Access is limited to specific roles or functions within the Cloud Engineering Services team. Additionally, access is managed on an “exception” basis whereby personnel need clearance to be authorized. Access is time-limited, after which time reauthentication is required.

End-to-End Encryption

Encryption is an important part of the solutions’ data protection strategy. Our end-to-end encryption commitment uses both encryption-at-rest and encryption-in-transit to keep our customer data safe and secure as it flows from the customer into the cloud environment of SAP Ariba solutions. Customer data is secured as it transits the Internet, crosses internal system boundaries, and is stored in the cloud.

Encryption in Transit

The security goal of encryption in transit is to create a secure communication channel between two processes or people to protect the confidentiality and integrity of the information being exchanged. Although rare, attempts to attack channel security typically implement a man-in-the-middle (MITM) position between the two parties that are communicating to eavesdrop on or intercept the communication.

For an attacker to achieve a man-in-the-middle position, they must impersonate the client to the server and impersonate the server to the client. For this reason, it is very important to authenticate the parties that are attempting to communicate securely. Typically, the server asserts its identity using a Web server certificate that the client trusts. Sometimes, the client will implement a certificate that the server trusts to authenticate itself to the server; other times, client authentication is performed through the Web application login functionality. Obviously, it is important that the login credentials are not passed to an imposter.

The Internet-facing services from SAP Ariba solutions have earned an A+ security rating by Qualys SSL Labs. This is a testament of the hardened security settings that SAP Ariba has deployed to assure that the strongest levels of security are implemented when customers are connecting to SAP Ariba solutions and transmitting data.

With our Encryption Between Tiers (and Services) Project, we intend to encrypt the communication within our infrastructure in keeping with a “zero trust” security philosophy. Of course, this does not mean that we do not trust our people. Instead, we assume that login credentials and internal networks can and will be compromised. Our security architecture is designed to impede an attacker’s ability to leap from system to system, collect credentials and keys, and eavesdrop or impersonate other systems.

By requiring mutual authentication and encryption for services that exchange sensitive data with other services in our environment, we are applying a “least privilege” security tenant. Each system or service only needs to talk to a few other specific systems or services. The encryption between the Web tier and the application tier is just the first step in the right direction. This lays the foundation for how the security-sensitive microservices will intercommunicate in the Cobalt platform.

Encryption at Rest

The security goal of encryption at rest is to provide access control by permitting only the authorized users or processes to view or alter the unencrypted data. Thus, it protects the integrity and confidentiality of the data. Unauthorized users or processes will see ciphertext. Ciphertext looks like random data and has no discernible patterns or meaning.

SAP Ariba solutions apply encryption-at-rest solutions at different layers to mitigate different types of threats pertaining to unauthorized access. These include:

- Storage-layer encryption, also known as transparent disk encryption, is implemented through self-encrypting disks. All content of a disk drive is encrypted and tied to a specific physical system. If a disk drive is removed and connected to another system, the data will not be able to be read.
- Database-layer encryption, also known as transparent database encryption, is enabled on our SAP HANA database. The full database is encrypted, and all writes of data to storage are encrypted before write.
- Application-layer encryption is used to assure that data is encrypted before it is inserted into the database. Therefore, the application performs the access control and policy enforcement duties. If the database administrator directly queries the database, all that will be returned are records that contain ciphertext.
- Key management services (KMS) provide a secure infrastructure for managing encryption keys and other types’ secrets. The KMS of SAP Ariba solutions is backed by a FIPS-140-2–compliant

hardware security module (HSM) for additional security. The KMS is integrated into operational procurement, strategic procurement, and Ariba Network.

SAP Ariba solutions have standardized on 256-bit AES encryption, using Java Cryptography Extension (JCE). The solutions support both shared-service and tenant-specific encryption keys. The solutions generate tenant-specific keys and manage them on behalf of the client. Having a tenant-specific key means that our customer's data is further isolated from compromise. In the worst-case scenario of a key compromise, this means that only the customer using that key is impacted. These keys are stored in the aforementioned key management service, backed by a hardware security module.

Customer user passwords are one-way hashed using SHA256 and salted with random data.

Citrix Workspace User Authentication and Authorization

SAP Ariba solutions use Citrix Workspace to transparently verify the identity of SAP Ariba solutions corporate users at the firewall and permit or deny access from the corporate network to any TCP/IP-based application in production.

Chapter 4 – Cloud Operations of SAP Ariba Solutions

SAP Ariba solutions have an internal security policy and various processes and procedures that are outlined in documents that are managed, updated, and adhered to by the cloud engineering services team. These documents include descriptions of processes to follow for database recovery, database extracts, and other systems maintenance tasks.

High Availability and Reliability

SAP Ariba solutions recognize that customers need the highest-possible availability and reliability. To that end, the solutions' infrastructure is scalable and redundant at all tiers. To provide high availability and reliability, SAP Ariba solutions have extensive error handling and failover capabilities. This section describes the main features of the solutions' failover and recovery plans. To ensure the highest availability, SAP uses best practices for the following:

- Redundant systems
- Maintenance and systems backup
- Proactive customer notification of unplanned downtime
- International support coverage

Redundant Systems

SAP Ariba solutions maintain redundant copies of all critical software subsystems. When a failure occurs, failover is triggered automatically to prevent disruption of service. Similarly, the solutions' hardware infrastructure is implemented with automatic failover mechanisms as well. To establish connection redundancy, SAP Ariba solutions are connected to the Internet via two different ISPs running through physically separate conduits to the upstream provider.

In the event of any hardware failure, Cloud Engineering Services personnel are automatically notified so that the failed equipment can be analyzed and repaired, as well as to prevent any recurrence of the problem in the future. If, for some reason, automatic hardware failover does not complete successfully, data integrity will still be intact due to redundancy.

In addition to redundancy on the hardware and software levels, SAP Ariba solutions benefit from the triple-redundant power systems utilized by our datacenters. These power systems consist of redundant connections to power utilities, backup power supplies, and diesel generators that can run for extended periods without refueling. For fire protection and suppression, inert gas and dry pipe sprinkler systems are utilized to protect the equipment and prevent inadvertent water damage.

Maintenance and System Backup

SAP Ariba solutions perform preventive maintenance on a scheduled basis. Maintenance intervals are reserved for low-use times, such as weekends and off-peak hours. All data in the system is maintained during these intervals and processing resumes as soon as the maintenance is completed.

SAP Ariba solutions utilize replication technologies to mirror data between the data centers in a region (regional data centers). These technologies protect against data loss due to a catastrophic event affecting a single site. SAP makes several backup copies of customer data to ensure that no data loss occurs.

SAP Ariba solutions perform regularly scheduled backups of stored data. These backups do not interrupt the normal operation of the cloud solutions. Backup data includes user information, projects, and the library.

When backups are taken, they are encrypted and stored on disk.

Database Backup

- Data is stored in databases on high-availability storage disk-based systems in the primary data center.
- Data replication to the secondary data center happens in near-real time (a few seconds normally).
- Database transaction logs are written simultaneously to redundant volumes on the high-availability storage systems in each data center. The log volumes are physically separated from one another as well as from the database data volumes.
- Database transaction logs are copied from database volumes to backup storage volumes at each data center.
- Database copy-on-write snapshot disk backups are completed twice per day at each data center. Database transaction logs are saved to disk for the point in time of each database disk backup.
- Database physical disk backups are completed once per week in each data center and copied to physically separate disks from the database data and transaction log volumes. Database transaction logs are saved to disk from the point in time of each database disk backup.
- Full database backup copies are written to dedicated storage backup volumes.

File Data Backup

- Discrete files are stored on high-availability network–attached storage devices in the primary data center and replicated to the secondary data center in near-real time (a few seconds normally).
- Copy-on-write snapshot disk backups are completed four times per day at each data center.

Process Integrity

- Validations are performed for all to-disk backup processes, including failure alerts and log reviews.
- Full restore tests to running databases are done every year to ensure the integrity of the backup process.
- All these processes and procedures are audited twice annually by PricewaterhouseCoopers (PwC) against the ISAE 3402 standard.

Disaster Recovery

SAP Ariba solutions are deployed in regional data center pairs so, in the event of a failover, the data will remain within region. Failover from one site to another has a design goal for its recovery time objective (RTO) to not exceed four hours. The design goal for the recovery point objective (RPO) is five minutes.

Disaster recovery options are included for all cloud services for SAP Ariba solutions. In the event of a failover to the secondary data center, no customer changes are required, as all URLs that customers use to reach the applications will continue to work. SAP will notify customers through e-mail in the event of unplanned downtime.

Internally, SAP Ariba solutions use a documented system recovery plan that outlines the approach and steps for recovering the applications. This document defines roles and responsibilities in the event of disaster:

- Cloud engineering services personnel maintain the hardware remotely
- SAP Ariba solutions maintains the application software
- Processes are in place to keep database and storage subsystems synchronized between primary and secondary data centers
- The failover processes for all infrastructure elements are automated

- If the primary data center incurs a catastrophic event, SAP will declare the primary data center "down" and the Cloud Engineering Services team will initiate the process to switch to the secondary data center and restart the applications at the secondary data center
- Once the switch is complete, the secondary data center becomes the primary data center and vice versa

SAP tests power outage backup scenarios and the disaster recovery plan on a periodic basis to ensure it is up-to-date, successful, and effective.

Chapter 5 – User Security Blueprint of the Cloud Solutions

Application Security

Application security governs end-user access to the online services and information on cloud solutions from SAP Ariba solutions. The cloud solutions use unique user IDs and passwords as the primary means of user authentication and access control.

IDs and passwords are case-sensitive. Customers can set up single-sign on (SSO) with their own authentication store (such as an identity provider) and define users with passwords that are stored hashed using SHA-2(256) after being converted to Base64 and salted with random data. Passwords used for authentication with SSO are stored within a customer's identity provider and adhere to the password rules enforced by the identity provider in use. For users who are to be authenticated by the SAP Ariba solutions applications (such as users not authenticated through an identity provider as part of corporate authentication), SAP enforces the use of strong passwords for all passwords stored within the applications.

All passwords stored within SAP Ariba solutions must adhere to the following rules:

- Passwords must be between 12 and 32 characters long
- Passwords are case-sensitive and can include Latin characters, special characters, and numerals
- Passwords must include at least one lowercase letter, one uppercase letter, one numeral, and one special character
- There must be at least one numeral between the first and last characters of the password

Access Control

Access to data and functionality within modules for SAP Ariba solutions is based on groups that determine which features of the service a user can see and work with, and what data the user can access. Groups allow customers to manage access control in a way that reflects their organizational structures and the roles of users within those structures.

SAP Ariba solutions provide a single point of integration and administration for users and user profiles, organizations, and groups and group memberships. This common data is shared and synchronized across modules automatically. The user and group objects can be managed from a customer administration portal or populated from a variety of sources, such as corporate systems and flat files, using predefined integration methods. For example, the user object can be populated from an external HR system. SAP Ariba solutions provide capabilities to perform batch upload from the user interface, either through Web page–based interactive file upload, or through automated (scripted/scheduled) HTTPS push of data from HR and ERP systems or using the SAP Ariba Cloud Integration Gateway solution.

Separation of Customer Data

The software's data model keeps customers' data separated. Customer data is isolated through realms. Each individual customer is assigned a distinct realm to identify and store their data. Realms are isolated from each other to prevent a customer realm from being able to see or access data from another customer realm.

Cookies

The SAP Ariba solutions applications utilize secure session cookies to maintain users' sessions after they're logged in. Once a browser initiates a secure connection to a server via HTTPS, a secure session cookie is used; this ensures that the cookie is encrypted when transmitting from the Web browser to the Web server.

A session cookie (or temporary cookie) exists only for the duration of the visit to the Web site. Session cookies are used to maintain session context, ensuring that page changes and data selections are retained as the user navigates from page to page. When a user initiates a session in any cloud solution from SAP Ariba solutions, the solution sends a session ID in the form of a session cookie. The session ID is transmitted back and forth between the browser and the server. HTTPS cookies are based on industry standards and provide a more secure method of session management rather than URL-based and form-based session management, which are prone to session hacking. SAP Ariba solutions never use cookies for marketing purposes; SAP Ariba solutions utilize cookies only to maintain session for its applications

For more information on how SAP Ariba solutions use cookies, please reference the privacy statement.

Session Timeout

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, then their work will be saved, and they will be logged out of the system.

Session IP-Range Validation

To guard against session hijacking, SAP Ariba solutions perform IP range checks. During a single user session, if the requesting IP address changes significantly (by more than a class B range - /16), then the session is terminated, and the user is required to log in again.

Object State

SAP Ariba solutions modules automatically persist object state to the underlying relational database as users work. When a user performs a significant action (for example, adding an item to an order, performing an approval, and so on), the application tier is aware of the change and automatically saves the relevant object state to the database. This provides transparent persistence of the user's work without the user having to “save” or “submit” changes to avoid losing work in the event of failure or session timeout. This in turn means that the loss of any connections between the tiers or failure of one of the tiers will not leave data in an inconsistent state.

Although object data is cached in the middle tier for performance, the official record is stored in the database to avoid any potential data loss or corruption. This means that recovery for SAP Ariba solutions modules is implicit and automatic. When the modules start, they retrieve the state of the various business objects from the underlying database as needed for user sessions. If a module fails, there is no special application recovery process other than restarting the module. The module will automatically connect to the database on restart; once users log in and commence working, all required business object data will be retrieved from the database.

Chapter 6 – System Administration

E-Mail

SAP Ariba solutions use Simple Mail Service Protocol (SMTP) over Transport Layer Security (TLS) as the default to send e-mail if the destination mail server supports it. Otherwise, it is standard SMTP.

SAP Ariba solutions provide configurable templates for text and HTML e-mails. E-mails are sent to the appropriate users for significant events in the application, such as approval requests or supplier invitations. The generated e-mails contain links or buttons that, when clicked, direct the e-mail recipient to the associated module for them to perform an action or review.

SAP Ariba solutions use sender policy framework records for their domain to prevent spammers from sending messages with forged “from” addresses. Customers can refer to the SPF record to determine if a message comes from an authorized SAP Ariba solutions mail server.

Audit Trails

SAP Ariba solutions provide a variety of audit trail mechanisms within the modules, depending on the nature of the objects being managed. As users complete their tasks, create new versions of their documents, perform approvals, and so on, the audit details are recorded as part of the transaction. This transaction record then becomes available for query through the user interface. In short, the audit trails are recorded across the applications suite for all user initiated and background activities.

Common Data

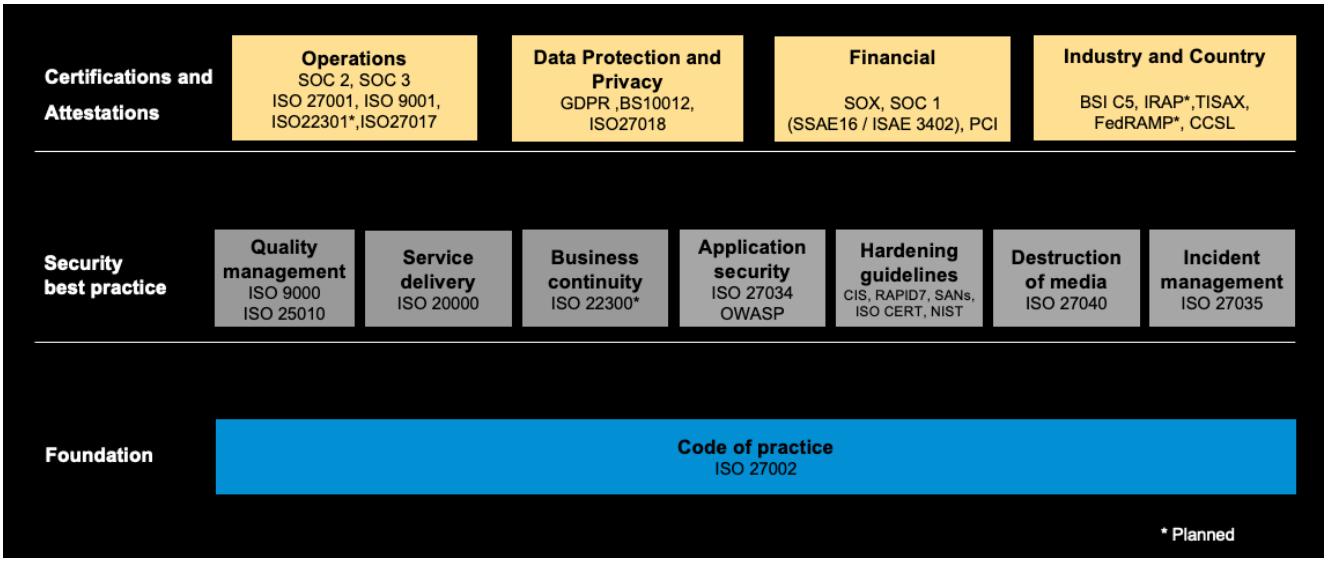
SAP Ariba solutions provide a single point of administration for common data shared among SAP Ariba solutions modules. This common data includes users and user profiles, organizations, groups and group memberships, currencies, exchange rates, and commodity codes. The solution administrator provides a full user interface for managing these common objects. In addition, these common objects can be populated from flat files.

Time Synchronization

SAP Ariba solutions use industry-standard Network Time Protocol (NTP) distributed by RedHat to perform time synchronization throughout the data center. NTP implementation ensures accurate time stamps on transactions and audit logs. There are at least two NTP servers in each data center. They are configured as peers to ensure both servers are synchronized with one another and serve consistent time to clients within the data center. NTP servers reference external stratum-2 NTP servers to synchronize their time. Stratum-2 NTP servers are automatically selected from a pool of North American servers that participate in pool.ntp.org. Customer administrators can select the preferred time zone in the application and no other configurations are required from the customer end.

Chapter 7 – Assurances and Certifications

SAP Ariba solutions demonstrate the information security assurances by complying with industry-recognized standards and regulations. Compliance with the standards are measured through either annual or semiannual audits. Current attestation reports and certificates can be made available upon request. The following figures explain the regulations and standards that SAP Ariba solutions comply with, are in the process of certifying, or are attesting this compliance.



List of Abbreviations and Acronyms

Acronym	Description	Certification Number
AT	Acceptance Test	AT 101
BDSG	Bundesdatenschutzgesetz (German Federal Data Protection Act)	
BS	British Standards	
BSI	Bundesamt fuer Sicherheit in der Informationstechnik (German Federal Office for Information Security)	BSI C5
CIS	Center of Internet Security	
EC	Employee Central	EC GDPR
EU	European Union	EU Directive 95/46
GDPR	General Data Protection Rights	
IRAP	Information Security Registered Assessors Program	
ISAE	International Standard for Assurance Engagements	ISAE 3000
ISO	International Standard Organization	22301, 27001, 9001, 9000, 20000, 22300, 27034, 27040, 27035, 27002
ISO CERT	International Standard Organization Certified	
NIST	National Institute of Standards and Technology	
OWASP	Open Web Application Security Project	
PCI	Payment Card Industry	
SAN	Storage Area Network	
SOC	System and Organization Controls	SOC 1, SOC 2, SOC 3
SOX	Sarbannes-Oxley	
SSAE	Statements on Standards for Attestation Engagements	SSAE16

Figure 2: Certifications and Assurances of SAP Ariba Solutions

Chapter 8 – Data Centers

Cloud services from SAP Ariba solutions are deployed to multiple data centers throughout the world. The data centers are geographically located in regional redundant pairs, in compliance with local and regional data residency regulations. Data is replicated between the two regional data centers, so that data remains within the region of deployment. The data centers within each region are geographically separated to minimize the impact of a single regional event causing a disruption in both data centers simultaneously.

Ariba Network runs globally and is housed in the United States data centers. It requires certain specific transactional data to be shared.

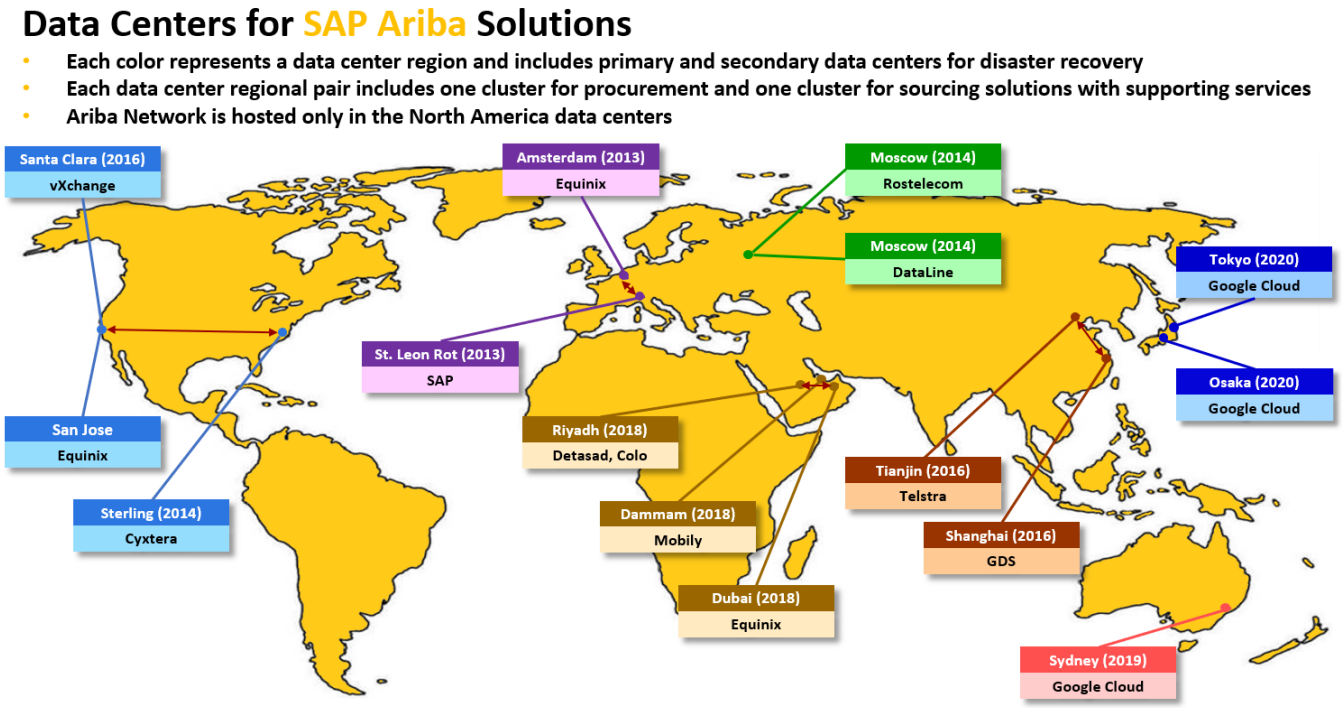


Figure 3: Data Centers for SAP Ariba Solutions

United States Data Centers

Equinix Data Center – San Jose, California

The SAP Ariba solutions system is co-located within the Equinix San Jose California facility. SAP is responsible for maintaining the software and hardware components of the system. SAP Ariba solutions use Cogent and Internap networks as an Internet service provider (ISP) for connectivity to the Internet.

The Equinix Data Center in San Jose, California, is a SSAE16 SOC-1 Type II–compliant facility. While the Cloud Engineering Services manages the solutions' hardware and software, the data center provides standard "remote-hands" service (reboot boxes and more) as needed. Equinix, Inc. operates International Business Exchange(IBX) data centers offering businesses a place to reliably run their operations and

securely exchange critical information. With locations in over 35 strategic markets across North America, Europe, and Asia-Pacific, Equinix enables customers to rapidly deploy data center operations worldwide. Customers can rely on the same state-of-the-art infrastructure, support, and experience of Equinix at any IBX center locations across the globe. For more information, please visit http://www.equinix.com.

Cyxtera (DC4) Data Center – Sterling, Virginia

The SAP Ariba solutions systems are housed in a private suite within the Cyxtera data center facility at Sterling, Virginia. Cloud operations are responsible for maintaining the software and hardware components of the system. Connectivity is provided through dedicated diverse path connections with tier-1 carriers (Cogent, CenturyLink, and Verizon). Fully redundant network infrastructure ensures 100% availability.

Cyxtera: While the operations of SAP Ariba solutions manages the solutions' hardware and software, the data center provides standard "remote-hands"service (reboot boxes and more) as needed. Cyxtera provides both logical and physical security. Cyxtera provides customers with dedicated access to the Cyxtera tier-1 IP backbone. The data center complies with U.S.-EU Safe Harbor, PCI Security Council standards, ISO, ISAE 3402, SSAE16, and HIPAA standards. For more information visit: http://www.cyxtera.com/data-center-services/data-center-locations

European Union Data Centers

Equinix Data Center – Amsterdam, Netherlands

The SAP Ariba solutions are housed in a private suite within an Equinix tier-4 facility in Amsterdam, the Netherlands. Cloud operations are responsible for maintaining the software and hardware components of the system. SAP Ariba solutions use a redundant pair of dedicated fiber interconnects for external connectivity to tier-1 carriers. In addition, a separate fully independent line via a diverse physical path provides redundancy.

The solutions' infrastructure is hosted in the latest Equinix Data Center in Amsterdam, (AM5) an ISO 27001– and PCI-compliant facility. Equinix provides standard "remote-hands" service (reboot boxes and more) as needed. Equinix is a global leading provider of premium carrier-neutral data centers, operating facilities in city locations across Europe. The group's data centers provide secure and highly connected environments for the IT and telecoms equipment that powers the digital economy. Its data centers enable environments in which the separate networks that make up the Internet meet and where bandwidth intensive applications, content, and information are hosted. For more information visit: https://www.equinix.co.uk/locations/europe-colocation/europe-data-centers/

SAP Data Center – St. Leon Rot, Germany

The SAP Ariba solutions systems are housed in a private suite within SAP's data center facility at St. Leon Rot, close to the SAP Walldorf campus. Cloud operations are responsible for maintaining the software and hardware components of the system. Connectivity is provided through dedicated diverse path connections to the DEC-IX hubs at Frankfurt (x2) with tier-1 carriers providing the external connectivity at each of the separate sites respectively. Fully redundant network infrastructure ensures 100% availability.

The SAP Ariba solutions infrastructure is hosted in the SAP-dedicated data center in St. Leon Rot. The data structure infrastructure team from SAP provides standard "remote-hands"services (reboot boxes and more) as needed.

SAP Group AG: SAP is one of the largest software and cloud providers in the world. The tier-4 data center at St. Leon Rot is dedicated to supporting the SAP suite of software and cloud applications, providing high availability, highly redundant, and secure facilities to host a variety of SAP applications. Local on-site support and third-party vendor presence, combined with highly available power, cooling, and network infrastructure make the data center in St. Leon Rot an excellent choice for housing any business-critical environment. For more information visit: https://www.sap.com/index.html

Russian Federation Data Centers

Rostelecom Data Center (Moscow, Russia)

The SAP Ariba solutions systems are housed in a private suite within a Rostelecom data center in Moscow, Russia. Cloud operations are responsible for maintaining the software and hardware components of the system. SAP Ariba solutions use a redundant pair of dedicated fiber interconnects for external connectivity to tier-1 carriers. In addition, a separate fully independent line via a diverse physical path provides redundancy.

Rostelecom: This is a tier-3 data center and a ISO 27001– and PCI DSS 3.0–compliant, carrier neutral facility. It provides high availability, highly redundant and secure facilities to host a variety of SAP applications. There is local on-site support and third-party vendor presence, combined with highly available power, cooling and network infrastructure. For more information please visit: https://rtk-dc.ru/en/

DataLine Data Center – Moscow

The SAP Ariba solutions systems are housed in a private suite within a DataLine data center in Moscow, Russia. Cloud operations are responsible for maintaining the software and hardware components of the system. SAP Ariba solutions use a redundant pair of dedicated fiber interconnects for external connectivity to tier-1 carriers

DataLine: This is a tier-3 data center and a ISO 27001– and PCI DSS 3.0–compliant, carrier-neutral facility. It provides high availability, highly redundant and secure facilities to host a variety of SAP applications. There is local on-site support and third-party vendor presence, combined with highly available power, cooling and network infrastructure. For more information visit: http://www.dtln.ru/en

China Data Centers

GDS Shanghai Waigaoqiao Data Center – Shanghai

The SAP Ariba solutions systems are housed in a private suite within a GDS Shanghai Waigaoqiao data center in Shanghai, China. The cloud operations of SAP Ariba solutions are responsible for maintaining the software and hardware components of the system. SAP Ariba uses a redundant pair of dedicated fiber interconnects for external connectivity. GDS is a tier-3 data center with ISO 27001 and BS 25999 certifications. GDS is also the proud recipient of the first Information Security Service Qualification Certification (Category of Disaster Recovery) in China.
Advanced data center design, high technical specifications and robust operating procedures make GDS the partner of choice for Internet and enterprise leaders. For more information visit: http://en.gds-services.com/

Telstra Tianjin-Beijing Data Center – Tianjin

The SAP Ariba solutions systems are housed in a private suite within a Telstra Tianjin-Beijing data center in Tianjin, China. The cloud operations of SAP Ariba solutions are responsible for maintaining the software and hardware components of the system. SAP Ariba solutions use a redundant pair of dedicated fiber interconnects for external connectivity.

Telstra is a tier-3 data center that complies with global security and quality standards including ISO 9001, ISO 27001, and PCI DSS. The facility provides customers with world-class colocation, connectivity, and managed services backed by 24x7 expert, multilingual customer service and on-site remote-hands support. For more information visit: https://www.t-pbs.com.cn/tianjin-dc/?lang=en

Middle East Data Centers

Equinix Dubai Data Center – United Arab Emirates

The SAP Ariba solutions systems are housed in a private suite within an Equinix data center in Dubai, United Arab Emirates. The cloud operations of SAP Ariba solutions are responsible for maintaining the software and hardware components of the system. SAP Ariba solutions use a redundant pair of dedicated fiber interconnects for external connectivity.

Equinix is a tier-3 data center that complies with global security and quality standards including ISO 9001, ISO 27001, and PCI DSS. The facility provides customers with world-class colocation, connectivity, and managed services backed by 24x7 expert, multilingual customer service and on-site remote hands support. For more information visit: https://www.equinix.co.uk/www/locations/europe-colocation/europe-data-centers/

Detasad Riyadh Data Center – Kingdom of Saudi Arabia

The SAP Ariba solutions systems are housed in a private suite within a Detasad data center in Riyadh, Kingdom of Saudi Arabia. The cloud operations of SAP Ariba solutions are responsible for maintaining the software and hardware components of the system. SAP Ariba solutions use a redundant pair of dedicated fiber interconnects for external connectivity.

Detasad is a tier-3 data center that complies with global security and quality standards including ISO 9001, ISO 27001, and PCI DSS. The facility provides customers with world-class colocation, connectivity, and managed services backed by 24x7 expert, multilingual customer service and on-site remote-hands support. For more information visit: https://www.detasad.com.sa/?page_id=2059

Mobily Dammam Data Center – Kingdom of Saudi Arabia

The SAP Ariba solutions systems are housed in a private suite within a Mobily data center in Dammam, Kingdom of Saudi Arabia. The cloud operations of SAP Ariba solutions are responsible for maintaining the software and hardware components of the system. SAP Ariba solutions use a redundant pair of dedicated fiber interconnects for external connectivity.

Mobily is a tier-3 and tier-4 data center that complies with global security and quality standards including ISO 9001, ISO 27001, and PCI DSS. The facility provides customers with world-class colocation, connectivity, and managed services

backed by 24x7 expert, multilingual customer service and on-site remote-hands support.

For more information visit: https://www.mobily.com.sa/portalu/wps/portal/business/services/it-services/hosting-and-cloud/co-location-service

Australia and New Zealand Data Centers

Google Cloud Sydney Data Centers – Sydney, Australia

The SAP Ariba solutions systems are housed in public cloud at multiple data centers in Sydney, Australia; Google maintains three zones in its Sydney region. The cloud operations of SAP Ariba solutions are responsible for maintaining the software components of the system.

Google Cloud is an MTCS tier-3 cloud service provider that complies with global security and quality standards including ISO 27001, ISO 27012, and ISO 27018. Google Cloud provides customers with world-class colocation, connectivity, and managed services backed by 24x7 expert, multilingual customer service and on-site remote-hands support. For more information visit: https://cloud.google.com/about/locations/sydney

Japan Data Centers

Google Cloud Japan Data Centers – Tokyo and Osaka, Japan

The SAP Ariba solutions systems are housed in public cloud at multiple data centers in Tokyo and Osaka; Google maintains three zones in both its Tokyo and Osaka regions. The cloud operations of SAP Ariba solutions are responsible for maintaining the software components of the system.

Google Cloud is an MTCS tier-3 cloud service provider that complies with global security and quality standards including ISO 27001, ISO 27012, and ISO 27018. Google Cloud provides customers with world-class colocation, connectivity, and managed services backed by 24x7 expert, multilingual customer service and on-site remote-hands support. For more information visit: https://cloud.google.com/about/locations