SAP Fieldglass

Independent Service Auditor's SOC 3 Report For the SAP Fieldglass Solution System

For the Period of

October 1, 2017, to September 30, 2018

Attestation and Compliance Services

schellman
Quality, above all.

Independent Service Auditor's Report

To SAP America, Inc.:

Scope

We have examined SAP America, Inc.'s ("SAP Fieldglass") accompanying assertion titled "Assertion of SAP Fieldglass Service Organization Management" ("assertion") that the controls within the SAP Fieldglass Solution system ("system") were effective throughout the period October 1, 2017, to September 30, 2018, to provide reasonable assurance that SAP Fieldglass' service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in the 2016 TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Principles and Criteria).*

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

Service Organization's Responsibilities

SAP Fieldglass is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that SAP Fieldglass' service commitments and system requirements were achieved. SAP Fieldglass has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, SAP Fieldglass is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

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

Our examination included:

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

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

Inherent Limitations

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

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

Opinion

In our opinion, management's assertion that the controls within the SAP Fieldglass Solution system were effective throughout the period October 1, 2017, to September 30, 2018, to provide reasonable assurance that SAP Fieldglass' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

SCHELLMAN & COMPANY, LLC

Tampa, Florida
October 29, 2018

Assertion of SAP Fieldglass Service Organization Management

We are responsible for designing, implementing, operating, and maintaining effective controls within SAP America, Inc.'s ("SAP Fieldglass") Fieldglass Solution system ("system") throughout the period October 1, 2017, to September 30, 2018, to provide reasonable assurance that SAP Fieldglass' service commitments and system requirements relevant to security, availability, processing integrity, confidentiality, and privacy were achieved. Our description of the boundaries of the system is presented below and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period October 1, 2017, to September 30, 2018, to provide reasonable assurance that SAP Fieldglass' service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in the 2016 TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Principles and Criteria).* SAP Fieldglass' objectives for the system in applying the applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

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

We assert that the controls within the system were effective throughout the period October 1, 2017, to September 30, 2018, to provide reasonable assurance that SAP Fieldglass' service commitments and systems requirements were achieved based on the applicable trust services criteria.

System Description of the SAP Fieldglass Solution System

Company Background

SAP America, Inc. (SAP Fieldglass) provides a cloud-based Vendor Management System (VMS) that enables organizations to procure, manage, and optimize their global external workforces, including contingent labor, freelancers, independent contractors, private talent pools, and services managed through Statements of Work (SOWs).

Headquartered in Chicago, Illinois, SAP Fieldglass has additional offices across the United States and in the United Kingdom, Australia, and India to serve its global customer base. SAP Fieldglass serves firms in more than 180 countries, and the solution is used in 21 languages by more than 85,000 staffing and service suppliers and more than nineteen million users.

SAP Fieldglass was founded in 1999 by Jai Shekhawat, an industry pioneer and recipient of the Ernst & Young Midwest Entrepreneur of the Year and Peter Yessne Staffing Innovator awards. Under his direction, SAP Fieldglass has been recognized by well-respected award programs including the American Business Awards, Illinois Technology Association CityLIGHTS Awards and CODiE Awards. For more information, visit www.fieldglass.com.

Description of Services Provided

SAP Fieldglass helps organizations achieve total workforce visibility, maximize cost savings, improve worker quality, and enforce compliance. The enterprise platform offers a secure, private marketplace for a company and its chosen suppliers.

Companies use SAP Fieldglass to manage:

- Contingent labor across technology, healthcare/clinical, professional, creative, skilled trade, and other specialized areas
- SOW-based projects and services
- Independent contractors and freelancers
- Specialized talent pools, such as retirees and alumni

The SAP Fieldglass platform may be used to perform a wide variety of functions that include, but are not limited to, the following:

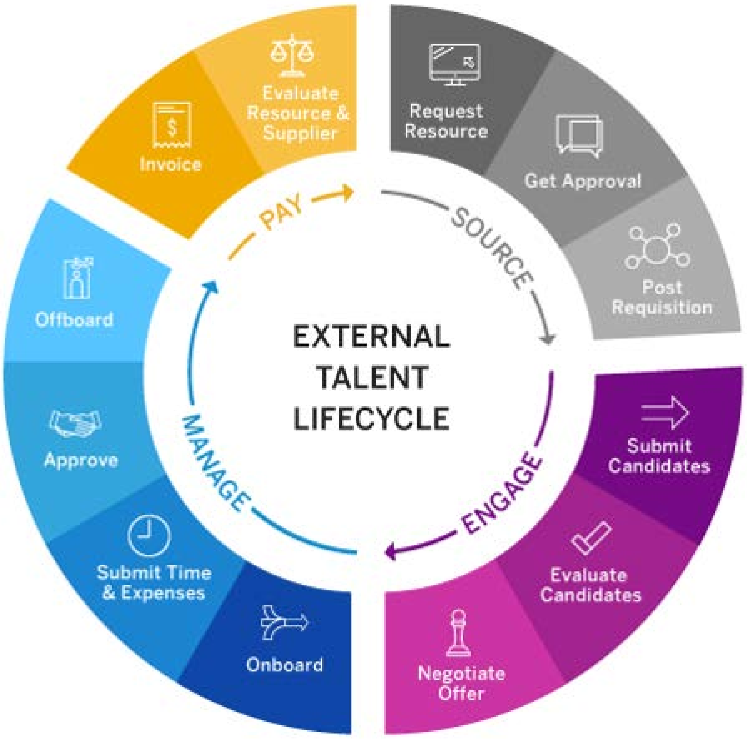
- Create, search, and archive requirements
- Generate preferred vendor lists
- Review resumes and rank candidates
- Schedule interviews
- Streamline on- and off-boarding processes
- Track and evaluate vendor and worker performance
- Create approval chains based on user profiles mapped to business rules
- Assign corporate authorization levels
- Produce detailed real-time reports
- Standardize job titles and pay according to a rate card
- Manage time and expense reports

- Automate invoicing, taxation, and discounts
- Customize alerts and notifications

SAP Fieldglass Contingent

SAP Fieldglass' external workforce management module automates the entire process of procuring and managing flexible labor, from requisition all the way through invoice and payment. It enables organizations to find, source and manage workers, enforce compliance, gain access to real-time data to better forecast costs, measure performance and plan for different types of labor needed in different scenarios. The platform supports any program model including those managed in-house, through one or more Managed Service Providers (MSPs) on- or off-site.

The diagram below illustrates the SAP Fieldglass Contingent process.

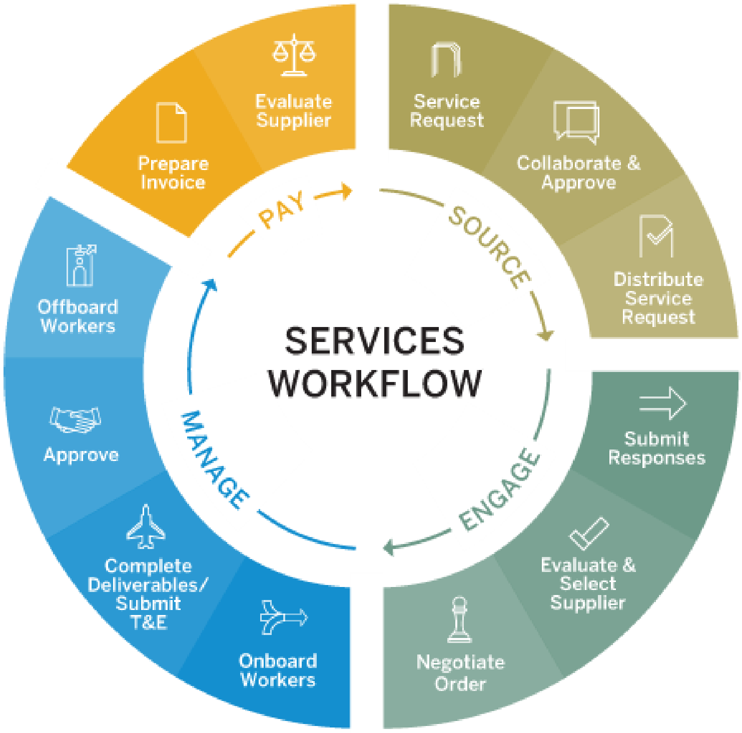


SAP Fieldglass Services Procurement

The SAP Fieldglass Services Procurement module streamlines the process of engaging third-party service providers. It automates sourcing, contracting, purchasing, tracking, invoicing, and payment for each project. SAP Fieldglass Services Procurement can accommodate any type of SOW, including unit-based, team-based, fixed-fee or Service Level Agreement (SLA)-based milestones.

[Intentionally Blank]

The diagram below illustrates the SAP Fieldglass Services process.



Benefits of Using SAP Fieldglass

Customers utilizing the SAP Fieldglass platform can:

- Drive users to the most appropriate engagement type for a given role or project
- Increase cost savings by bidding external services to preferred suppliers
- Control spend by enforcing the use of preferred suppliers and pre-defined rate cards
- Ensure the proper on- and off-boarding of external workers and service providers
- Increase the quality of the work and service being delivered by tracking vendor and worker performance, and level of effort
- Increase accuracy of time sheets and invoices
- Uncover critical insights with robust analytics and reporting to drive program improvements

Customer requests for services are initiated and authorized by user entities by directly contacting SAP Fieldglass. Customer requests are recorded and tracked by SAP Fieldglass through resolution and are managed according to established contracted services and related SLAs.

System Boundaries

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

Infrastructure and Software

The SAP Fieldglass application resides on physical servers and virtual machines. Production equipment is located in data centers operated by SAP SE (SAP Corporate) in Rot, Germany, Cyxtera Data Centers, Inc. (Cyxtera) in Elk Grove, Illinois, and ServerCentral, Inc. (ServerCentral) in San Jose, California, and Amsterdam, Netherlands. The application is built on a J2EE architecture utilizing an n-tier approach. The application has a presentation layer for user interaction and rendering pages, a business layer for business rules and required validations, a service layer for delegation of persistence and workflow per business rules, and a persistence layer for persisting to the database.

The SAP Fieldglass Solution system is hosted in highly available infrastructure environments. Within the United States and Germany, SAP Fieldglass designs, deploys, manages, and is the owner of the production infrastructure from the cage in, including the hardware, devices, and software. Within the ServerCentral-operated facility within the European Union (EU), ServerCentral manages the firewalls and configures the rules as requested by SAP Fieldglass. Additionally, ServerCentral manages the physical infrastructure; however, they are not provided with logical access to systems. Regardless of location, the hosting data center facilities provide Internet, heating, ventilation, air conditioning (HVAC), fire detection and suppression equipment, power, and physical security.

Components within the facilities are redundant, including firewalls, switches, network connectivity, database clusters, and content management appliances. Power is brought to the buildings through two entry point locations. This power is delivered to multiple power management modules that interconnect multiple battery storage systems and multiple generators. Infrastructure components have redundant power supplies and systems have multiple paths with infrastructure components spilt on a backplane.

SAP Fieldglass utilizes two redundant firewall pairs from two different vendors. The first firewall manages perimeter access. The second firewall manages inter-virtual local area network (VLAN) communications. Web servers are configured in a load balanced farm running Microsoft Windows operating systems and database servers are clustered in active-active mode.

Remote access is restricted to personnel via encrypted virtual private network (VPN) connections while access to the production environment is restricted to personnel already authenticated via remote desktop protocol (RDP) and two-factor authentication. VPN and RDP communication sessions are encrypted via various encryption protocols. To protect data in transit, transport layer security (TLS) encryption is utilized for web communication sessions.

The in-scope infrastructure consists of multiple applications, operating system platforms and databases, as shown in the table below:

Primary Infrastructure			
Production System	**Business Function Description**	**Operating System Platform**	**Physical Location**
SAP Fieldglass Application	Provides contingent workforce management solutions.	Microsoft Windows	Elk Grove, IL, San Jose, CA, Amsterdam, Netherlands, and/or Rot, Germany
Active Directory	Used to manage user accounts, application access, and authentication requirements.	Microsoft Windows	Elk Grove, IL, San Jose, CA, Amsterdam, Netherlands, and/or Rot, Germany
Firewalls/ Switches	Used to filter and route traffic.	Cisco / FortiGate	Elk Grove, IL, San Jose, CA, Amsterdam, Netherlands, and/or Rot, Germany
Virtual Hypervisor	Runs virtual machines for the execution of the operating system.	VMWare vCenter	Elk Grove, IL, San Jose, CA, Amsterdam, Netherlands, and/or Rot, Germany

Primary Infrastructure			
Production System	**Business Function Description**	**Operating System Platform**	**Physical Location**
Servers	Used for virtual application delivery.	Microsoft Windows	Elk Grove, IL, San Jose, CA, Amsterdam, Netherlands, and/or Rot, Germany
Databases	Used to store, retrieve, and manage data input into the system.	Microsoft Windows	Elk Grove, IL, San Jose, CA, Amsterdam, Netherlands, and/or Rot, Germany

People

The personnel supporting the SAP Fieldglass Solution system include, but are not limited to, the following:

- Executive management – responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives.
- Human resources (HR) – responsible for establishing policies, standards, and processes for recruitment, employee record-keeping, organizational design and development, and performance and behavior management.
- Systems administrators – responsible for functions such as patch management, antivirus/anti-malware administration, monitoring services, issue escalation and troubleshooting, and backup procedures.
- Virtualization system engineers – responsible for managing the virtualization environment under which the system operates.
- Network engineers – responsible for managing the network infrastructure.
- Developers – responsible for systems development and maintenance for in-house developed software.
- Quality assurance (QA) personnel – responsible for rigorously testing updates to the software before deployment to the production environment.

Procedures

Access Authentication and Authorization

Access to system information, including confidential data, is protected by authentication and authorization mechanisms. User authentication is required to access the production networks, including the application and database server operating systems, the databases, and the application. The information security policy outlines the formalized process for access provisioning, administration, and management.

Systems administration personnel are responsible for assigning and maintaining access rights to the production environment. In order to access the application or database server operating systems, users first authenticate to the network domain. Access to application and database server operating systems is governed by the primary domain controller's policy. In order to access the production databases, users must authenticate to the database after they have authenticated to the database server.

The network domain is configured to enforce password requirements based on predefined standards. Predefined groups are utilized to assign role-based access to the network domain. Administrative access privileges to the network domain, application and database server operating systems, and databases are restricted to authorized personnel.

Access Requests and Access Revocation

An automated provisioning process is in place for new hires. After the requested onboarding documentation is completed (nondisclosure agreement, background check, etc.), the candidate information is entered into a portal, in which the information is subsequently converted to an Excel spreadsheet and an automated script is run to create system access. A complex password is automatically assigned, and the user account remains in a disabled state until activated. When the HR department triggers an employee or contractor offboarding, automated tasks are sent to recipients for offboarding tasks including the creation of a checklist and subsequent termination of access. Systems administrators revoke system access privileges assigned to terminated employees as a component of the employee termination process. Escalations are sent to recipient's managers and the security team when off-boarding tasks are not completed within expected timeframes. This escalation helps ensure employees and contractors do not retain system access subsequent to their termination date.

Change Management

Application Changes

Internal personnel or customers can request a change via e-mail or verbal communication. Once a change request has been submitted, it is logged into a ticketing system. Change management personnel populate key fields, including the change request description, change type, priority, and target release. Changes are ultimately bundled into releases based on the following classifications:

- Major releases – major changes in functionality
- Minor releases – minor changes in functionality
- Service packs – small urgent changes

Releases follow a defined methodology for successful implementation, including the use of a change management system, detailed documentation to be completed, and testing to be performed pre- and post-deployment. However, major releases are subject to more stringent processes, including the completion of functional requirements that are required to be approved by project stakeholders, the documentation of detailed test plans and weekly test metrics prior to implementation, static code profiling to ensure secure coding standards are being adhered to, and penetration testing the application to help ensure vulnerabilities are addressed prior to implementation.

Development personnel execute unit test plans created by the QA team for major releases prior to releasing the software to QA for formal testing. QA personnel perform a vulnerability scan of the application for major releases to help ensure vulnerabilities are addressed prior to implementation, as well as regression and functional testing of major releases. Releases are implemented during scheduled maintenance windows. QA personnel perform post-deployment testing of change releases.

Formal quality gate meetings are conducted by the SAP Fieldglass release management team to ensure key performance indicators (KPIs), product requirements, and corporate requirements are being met throughout the SDLC. Results are reviewed in a final decision gate meeting between SAP and the SAP Fieldglass release management team prior to deployment to the production environment.

Releases require an application digest to be generated to help ensure production code changes are authorized. This is performed before a release is deployed to production (to validate the state of the production environment) and after implementation (to validate that the certified code was deployed without modification). Additionally, application source code is escrowed within ten business days for releases. QA management performs a post-deployment escrow audit of change releases to help ensure that changes are escrowed within the specified timeframes.

Release management meetings are held on a weekly basis to discuss current and upcoming projects. In addition, the ability to implement changes into the production environment is restricted to authorized personnel.

Version Control Software

Version control software is utilized to manage versions of source code. The software allows development personnel to check-out different versions of the code for editing. Once users are ready to update the code repository, they check-in the version. The version control software assigns a different version number to each iteration and allows users to rollback code to previous versions when necessary. In addition, the software is configured to restrict code changes from being checked in without an associated change request. The ability to lock and unlock code within the version control software is restricted to authorized personnel.

Separation of Environments

Development and testing activities are performed in distinct environments that are physically and logically separate from production in order to ensure that changes made within the test environment do not affect changes in the production environment.

Infrastructure Changes

Internal personnel can request a change by opening a change request ticket in the IT ticketing system. The change request tickets include the ticket status, request details, risk, if applicable, and approval details. Once a change request has been submitted, a technician selects a change request template, and the change is logged in a ticketing system. Any enabled tasks within the ticket are assigned to specific technicians, which subsequently receive an e-mail notification with details of the task and related change request.

Change requests require approval from IT management prior to the initiation of change management activities. Once approved, the assigned technician will perform the associated task in a sequenced process and document the results in a work log within the change request. Once required tasks have been completed, the request is marked as resolved.

System Software Changes

Patching is the process of installing a piece of software designed to fix problems and/or update a system. This includes fixing security vulnerabilities and other bugs and improving the usability or performance of a system. The patching process helps protect systems from vulnerabilities, such as viruses and/or malicious code. A patch management application is utilized to monitor, distribute, and apply patches to production servers. Scans of the production environments are performed on a monthly basis to identify security patches. A process for testing patches is in place – this process is formalized in regard to the production environment with documented approvals from QA personnel.

Patches are deployed during the scheduled maintenance windows to minimize the impact on the production environment. The ability to implement patches is restricted to authorized personnel via domain administration privileges.

Data Backup and Disaster Recovery

Production databases are backed up via an automated system – transaction logs are replicated between data center sites every 15 minutes and full database backups to local disk occur daily. At the conclusion of the full daily backup, the production database backups are replicated to the secondary data center, which is geographically separate from the primary data center. The automated backup and replication system is configured to notify systems administration personnel regarding the failure of relevant jobs, in which the cause is subsequently investigated. Additionally, restoration testing is completed on a monthly basis to help ensure data can be restored. The ability to retrieve production database backups from the off-site storage facilities is restricted to authorized personnel.

A disaster recovery plan is in place and the disaster recovery procedures are tested on an annual basis to help ensure that the contractually agreed upon recovery time and the recovery point objective from the time the disaster is officially declared by SAP Fieldglass senior management can be met.

Incident Response

The security team is designated to lead security incident investigations. Defined processes assign roles and responsibilities, address the reporting, classification, and handling of incidents, identify learning requirements from incidents, and the process for collection and retention of evidence. In addition, incidents are documented within a security incident report and are escalated, monitored, and reviewed as necessary. Incidents requiring a change to the system follow the standard change control process.

System Monitoring

The security team has configured security events to be logged according to internal prioritization. These security events consist of activities identified by the firewall and intrusion detection system (IDS). Events that are logged are sent to a centralized monitoring tool. The monitoring tool analyzes the log results and alerts security personnel via onscreen alerts in the event suspicious or unauthorized activities are identified. Upon receipt of the alerts, security personnel review the alerts to determine if any additional action should be taken.

An IDS is utilized to analyze network traffic for possible or actual network security breaches and is monitored by systems administration personnel. In the event that a potential or actual security breach is encountered, security personnel work to identify the cause and remediate the breach as soon as possible.

An enterprise monitoring system is utilized to monitor the health and availability of the production environment. In the event that a monitored component falls out of the predefined monitoring thresholds, the enterprise monitoring application is configured to notify systems administration personnel via e-mail alerts. Once notified, systems administration personnel review the alerts and investigate the cause. Additionally, monthly performance metrics reports are generated for review by information technology (IT) management personnel to evaluate system performance and capacity requirements/needs.

Windows production servers and workstations are protected by antivirus software, which is configured to update virus signature definitions on a daily basis. The antivirus software is configured to scan files upon access or modification.

SAP Fieldglass utilizes a vendor for help desk support during non-business hours and for customers that use other languages. This vendor is required to adhere to SAP Fieldglass’ policies and procedures, including the privacy policy.

Data

The SAP Fieldglass application holds information such as job posting details, SOW details and related contractual clauses, rate card information, worker bill and pay rates, time sheet data, and invoices. The application, by design, does not require data that would require breach notifications, if compromised. If customers choose to store sensitive data, that may include Personally Identifiable Information (PII), custom fields may be defined that can be encrypted with advanced encryption standard (AES) 256-bit encryption. These fields can also be optionally masked from view while entering and viewing the fields in the application. Data can be delivered to users in various formats including the user interface, subscription-based reporting, job seeker resumes e-mailed to users, and e-mail approval requests. In addition, a native mobile application (iPhone/Android) is available for download that can be used to complete approval work items. SAP Fieldglass does not transmit personal information by mail or other physical means.

Data within the SAP Fieldglass application may be imported or exported via web services including simple object access protocol (SOAP) or representational state transfer (REST), SAP Fieldglass Integrator, hypertext transfer protocol secure (HTTPS), or secure file transfer protocol (SFTP)/file transfer protocol secure (FTPS) protocols. HTTPS transactions may be imported or exported either via the user interface or using SAP Fieldglass Integrator. SAP Fieldglass Integrator, which is a light-weight Java-based integration tool, can be used to integrate SAP Fieldglass with third-party applications, such as enterprise resource planning (ERP) solutions. Additionally, many pre-built connectors are available for applications that include, but are not limited to, the following: PeopleSoft, Ariba, SAP, Oracle, SiteMinder, JD Edwards, Kronos, GEAC, Niku/Clarity, ADEO, Cyborg, and various legacy applications. SAP Fieldglass has developed various application programming interfaces (APIs) to facilitate integration to other enterprise applications and has architected both the SAP Fieldglass application and SAP Fieldglass Integrator to integrate to those applications.

The data within the SAP Fieldglass application is generated and uploaded by SAP Fieldglass’ customers. Each customer is responsible for the accuracy and timeliness of data entered within the application and additionally has their own administrators which manage their users and data. Customer data stored within the system is considered confidential.

Subservice Organizations

The data center hosting services provided by SAP Corporate, Cyxtera, and ServerCentral, and the managed network and infrastructure services for the production systems hosted within their European data centers provided by ServerCentral were not included within the scope of this examination. The following table presents the applicable Trust Services criteria that are intended to be met by controls at SAP Corporate, Cyxtera, and ServerCentral, alone or in combination with controls at SAP Fieldglass, and the types of controls expected to be implemented at SAP Corporate, Cyxtera, and ServerCentral to meet those criteria.

Control Activity Expected to be Implemented by SAP Corporate, Cyxtera, and ServerCentral	Applicable Trust Services Criteria
SAP Corporate, Cyxtera, and ServerCentral are responsible for ensuring controls are implemented to restrict physical access to facilities housing the system to authorized personnel.	CC5.5 PNC6
ServerCentral is responsible for configuring the firewall rules for their systems hosted within the EU as requested by SAP Fieldglass to block unauthorized inbound network traffic from the Internet.	CC5.6
ServerCentral is responsible for configuring and monitoring the IDS as requested by SAP Fieldglass and for alerting SAP Fieldglass of possible or actual security breaches for their systems hosted within the EU.	CC5.6
SAP Corporate, Cyxtera, and ServerCentral are responsible for ensuring controls are implemented to design, develop, implement, operate, maintain, and monitor environmental protections.	A1.2 PI1.1

SAP Fieldglass has not delegated any responsibility of the personal information life cycle to SAP Corporate, Cyxtera, or ServerCentral.

Statement of Privacy Practices

Within the SAP Fieldglass Solution system, SAP Fieldglass provides services to user entities in the capacity of a data processor. SAP Fieldglass serves in the function of a processor in cases where it processes personal data only as instructed by user entities (data controllers) in order to fulfill the requirements of an agreement associated to the provisioning of the services.

User entities are responsible for providing their privacy notice to individuals. SAP Fieldglass communicates the privacy practices to user entities in the Statement of Privacy Practices. Therefore, the description does not address the (a)(i)(11) criteria in Section 2. The Statement of Privacy Practices includes the following, and is included below:

At SAP Fieldglass, we are committed to protecting your privacy. Please read the following policy to understand how your personal information will be treated as you make use of the SAP Fieldglass cloud service. Please note that your organization will be notified of updates to this policy within the release notes for each major release to our cloud service, and that provisions of this policy may be supplemented or superseded by company-specific contractual terms (the details of which can be obtained from your organization).

The SAP Fieldglass cloud service may contain links to other websites. SAP Fieldglass is not responsible for the privacy practices or the content of such other websites. The privacy policies applicable to such other websites may differ substantially from this privacy policy so we advise you to read them before using those websites. SAP Fieldglass will not be liable for any use of those websites.

Consent

Your organization is responsible for your enrollment into the cloud service and is solely responsible for obtaining your consent. If you decide to opt out of having your personal information within the cloud service after providing your consent, you must contact your organization's administrator. The action of opting out will prevent you from using the cloud service we provide. Your personal information is a requirement and removal of your personal information will result in termination of your user account (i.e., termination of your ability to use the SAP Fieldglass cloud service).

Information Collected

- Information about your transactions with us, our affiliates, or nonaffiliated third-party users of the SAP Fieldglass cloud service
- Information about you as required or permitted by law
- Your name and other contact details when you request support by phone or e-mail us, or establish a user account for the cloud service
- Information about you when you apply for a job or contract with us (for example, your name and contact details, information about your working history and relevant records checks)
- Information we receive from our customers and other third-party users of the cloud service

Information Processed

Your organization determines what information is processed by the cloud service. SAP Fieldglass only requires your name and e-mail address; however, your organization may choose to use additional information. Each organization's administrator is responsible for the accuracy of the data within our cloud service.

SAP Fieldglass processes the personal information necessary to provide services and information to its customers, for its business operations and to comply with the law. Depending on the circumstances, SAP Fieldglass may also use personal information about you to:

- Accurately identify you
- Protect and administer your records and accounts
- Help us notify you of product enhancements and changes to products
- Save you time when you apply for additional products and services
- Comply with certain laws and regulations
- Collect information about the usage of our services
- Respond to your requests for information about our services

Data Analytics, Benchmarking, and Disclosing Personal Information

We may share with our partners and customers non-identifying statistical information regarding you, your customers, your suppliers, sales, traffic patterns and site usage.

The SAP Fieldglass cloud service may also allow you or your organization to share information about you (including personal data) with other users of the cloud service. You or your organization can use the functionality within the cloud service to determine which information you want to share.

In addition to the foregoing, for the purposes described in this policy, SAP Fieldglass may disclose personal information:

- To any of our related companies;
- To anyone to whom our assets or business (or any part of it) is transferred or offered to be transferred;
- As stated in our contracts with your organization;
- Where you or your organization have otherwise consented; or
- As otherwise required or authorized by law .

Cookies, Browser Information, and IP Address Tracking

The SAP Fieldglass website uses cookies for site administration purposes and they do not store your personal information. The cookies are used to identify you to our cloud service. If for any reason, you wish not to take advantage of cookies, you may have your browser not accept them, although this may disable or render unusable some of the features of the cloud service.

The SAP Fieldglass website uses cookies to record your preferences within the cloud service and they do not store your personal information. SAP Fieldglass stores the browser versions of the users who access the cloud service. This data is collected to ensure browser compatibility of the cloud service as it goes through its development and maintenance processes.

SAP Fieldglass' website may also detect and use your IP address or domain name for internal traffic monitoring and capacity purposes or to otherwise administer the cloud service. The patterns of usage of visitors to the website may be tracked for the purposes of providing improved service and content based on aggregate or statistical review of user site traffic patterns.

Data Retention

SAP Fieldglass retains personal information for the time necessary to fulfil the purposes identified in this privacy policy, as authorized by your organization (including as stated in our contracts with your organization), or as required by law or regulation. Thereafter, except in the event of a governmental or legal audit, retention requirement, investigation or pending litigation, SAP Fieldglass will (or enable your organization to) delete personal information stored on servers hosting the cloud service.

Information Security

We restrict access to personal information about you to those who need to have that information to provide the cloud service to you. If we use other companies to provide the cloud service to you, we require that they keep the information we share with them safe and secure.

We have physical, logical, and technical safeguards in place that comply with industry standards and legal requirements to process personal information about you from unauthorized access, alteration, and destruction.

Details of our security program can be found at http://www.fieldglass.com/solutions/security

Compliance

SAP Fieldglass takes significant efforts to comply with its respective obligations under applicable data privacy laws and regulations and we are committed to continually protecting your right to privacy as it currently applies, and evolves, in all applicable jurisdictions.

When entering into a business agreement for use of the SAP Fieldglass cloud service, SAP Fieldglass may enter into appropriate contractual clauses, including, without limitation, a data processing agreement that incorporates the standard contractual clauses where the transfer of personal information may occur by an SAP Fieldglass customer located in the European Economic Area to a country outside of the European Economic Area.

If you have any specific questions or concerns about our privacy program, please feel free to reach out to your organization or directly to SAP Fieldglass at the following email address: fieldglass_privacy@sap.com.

Complaints

Any issues, questions, or complaints that you have regarding the access, correction and/or handling of your information must be addressed with your organization's administrator of the SAP Fieldglass cloud service.

Further Information

If you would like further information about our privacy policies or practices, please contact our SAP Fieldglass Privacy Officer:

E-mail: fieldglass_privacy@sap.com
111 North Canal Street
Suite 600
Chicago, Illinois, 60606
United States