



**SOC 3 – SOC (Service and Organization Controls) for
Service Organizations: Trust Services Criteria for
General Use Report**

**Report on SAG Cloud GmbH's
Alfabet Cloud Enterprise Edition System
Relevant to Security and Availability**

Throughout the Period of April 1, 2018 to September 30, 2018



Table of Contents

SECTION I	1
Independent Service Auditor’s Report To the Management of SAG Cloud GmbH	2
SECTION II	3
Management of SAG Cloud GmbH’s Assertion regarding its System.....	4
Management of SAG Cloud GmbH’s Description of its Alfabet Cloud Enterprise Edition System For the Period of April 1, 2018 to September 30, 2018	5

SECTION I

Independent Service Auditor's Report

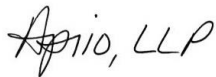
Independent Service Auditor's Report To the Management of SAG Cloud GmbH

We have examined the effectiveness of SAG Cloud GmbH's (also known as SAG) controls over the security and availability of the Alfabet Cloud Enterprise Edition System during the period of April 1, 2018 to September 30, 2018 based on the criteria for the security and availability set forth in the American Institute of Certified Public Accountants (AICPA) TSP Section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (2016). SAG's management is responsible for maintaining the effectiveness of these controls. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA and, accordingly, included (1) obtaining an understanding of the controls related to the security, confidentiality, and privacy of the IT Management Platform, (2) testing and evaluating the operating effectiveness of SAG's controls, and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of the nature and inherent limitations of controls, SAG's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent or detect and correct error or fraud, unauthorized access to systems and information, and failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes made to the system or controls, the failure to make needed changes to the system or controls or deterioration in the effectiveness of controls may alter the validity of such conclusions.

In our opinion, SAG maintained, in all material respects, effective controls over the security and availability of the Alfabet Cloud Enterprise Edition System throughout the period of April 1, 2018 to September 30, 2018 based on the AICPA Trust Services Security and Availability principles.



Atlanta, GA

October 31, 2018

SECTION II

Management Assertion and System Description

Management of SAG Cloud GmbH's Description of its Alfabet Cloud Enterprise Edition System for the period April 1, 2018 to September 30, 2018

SAG Cloud GmbH is responsible for designing, implementing, operating, and maintaining effective controls over the Alfabet Cloud Enterprise Edition System throughout the period April 1, 2018 to September 30, 2018, to provide reasonable assurance that SAG's service commitments and system requirements relevant to security and availability were achieved.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2018 to September 30, 2018, to provide reasonable assurance that SAG's service commitments and system requirements were achieved based on the Trust Services Principles and Criteria relevant to security and availability (applicable Trust Services Principles and Criteria) set forth in TSP Section 100A *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (2016). SAG's objectives for the system in applying the applicable Trust Services Principles and Criteria are embodied in its service commitments and system requirements relevant to the applicable Trust Services Principles and Criteria.

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 April 1, 2018 to September 30, 2018, to provide reasonable assurance that SAG's service commitments and system requirements were achieved based on the applicable Trust Services Principles and Criteria.

Signature: Michael Schuhmacher, Managing Director
Title: October 31, 2018

Signature: Gerd Schneider, Head of Cloud Security
Title: October 31, 2018

Description of SAG Cloud GmbH's Alfabet Cloud Enterprise Edition System for the Period of April 1, 2018 to September 30, 2018

Software AG Overview

Software AG helps organizations combine existing systems on premises and in the cloud into a single platform to optimize business and serve customers. With Software AG, Cloud offering can rapidly build and deploy digital business applications to exploit real-time market opportunities. Get maximum value from big data, make better decisions with streaming analytics, achieve more with the Internet of Things, and respond faster to shifting regulations and threats with intelligent governance, risk and compliance. Software AG helps organizations achieve their business objectives faster. The company's big data, integration, business process, IT planning, portfolio and architecture management technologies enables customers to drive operational efficiency, modernize their systems and optimize processes for smarter decisions and better service. Building on over 40 years of customer-centric innovation, Software AG is fueled by core product families such as Adabas-Natural, Alfabet, Apama, ARIS, Terracotta, and webMethods.

System Overview

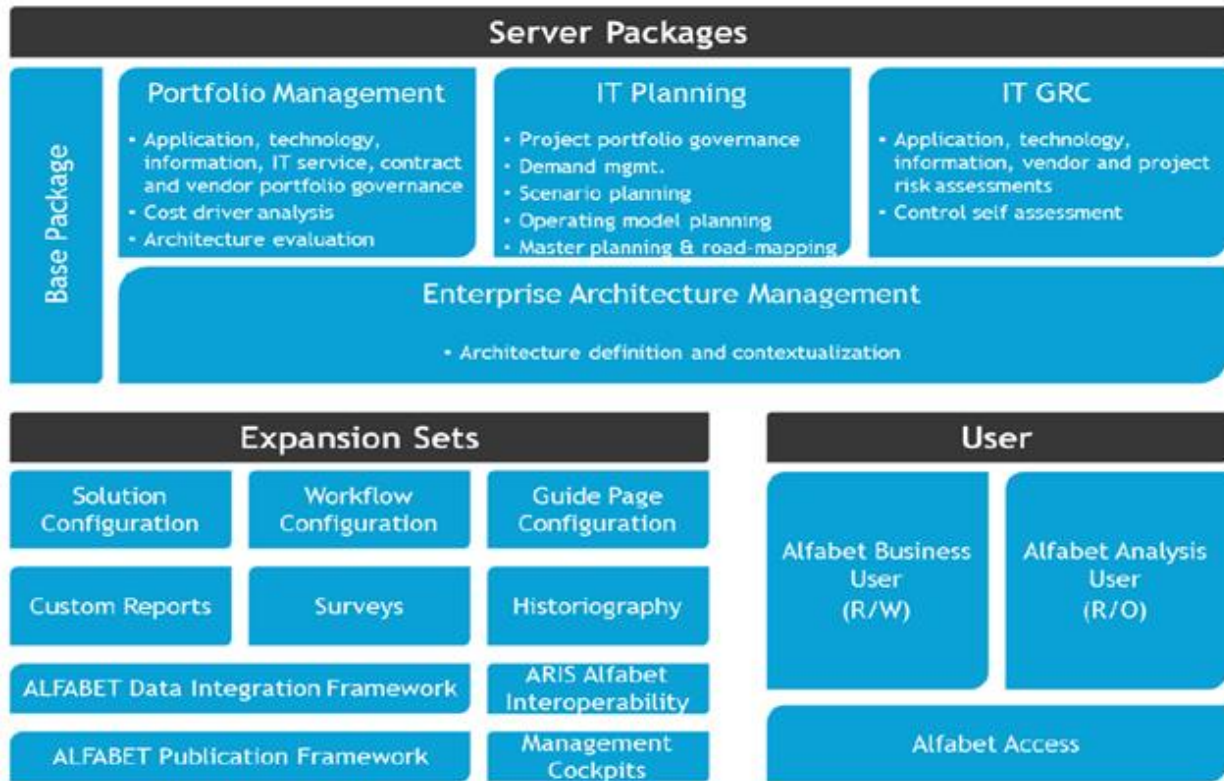
Alfabet helps organizations in making better IT investment decisions and reduce transformational risks by understanding the suitable parameters to make changes to their IT portfolio. It links the interdependent perspectives of IT, business, finance, and risk for “whole view” analysis of how IT can support business change. Enterprise architecture capabilities build the necessary foundation with an accurate, real-time picture of the IT landscape – including all applications and technologies, the inter-relationships between them, the information they exchange as well as the business capabilities and processes they support. Alfabet's portfolio management capabilities support independent decision-making for optimization of individual portfolios as well as portfolio-level strategy modelling to incorporate all portfolios into strategy formulation. Its collaborative planning platform enables all stakeholders to interface, communicate and consider multiple perspectives when making transformation decisions as well as prioritize project proposals based on alignment with business strategy. Alfabet is available as an on-premise or SaaS solution.

Benefits:

- Well-founded and sustainable decisions on IT transformation based on accurate, current and complete information on the IT landscape;
- IT structures aligned with business objectives and processes to ensure that IT transformation goes hand-in-hand with business transformation;
- Streamlined IT portfolios that increase Information Technology's agility in implementing business initiatives faster thus improving time to market for new business products;
- Lowered project, application and data risk to safeguard IT project investment, ensure business continuity, and increase compliance with regulatory requirements;
- Improved IT governance across federated environments through definition and enforcement of standard EA, IT planning and portfolio management processes.

Core Features:

With the Base Package, as pre-requisite for all other packages, organizations can implement individual packages in a stand-alone mode according to the organization’s needs.



Server packages follow a level-by-level build up approach. Please refer to the pre-requisites listed at the end of each server package description.

BASE PACKAGE:

The Base Package provides the necessary foundational infrastructure for using the Alfabet functional packages. It comprises features that are relevant and important to all of the functional packages, including user management functions, the workflow engine, monitors and assignments and other basic underlying functionality. The Base Package includes features that streamline data collection and navigation through the inventory such as:

- Web interface for quick access to the inventory;
- Simple editor screens for data entry;
- Wizard-driven interfaces for defining objects including infrastructure to perform input validation through configurable complex rules;
- Data collection templates using Microsoft Excel;
- Assignment of update responsibilities to named individuals;
- Display of sent assignments for keeping track of the progress on assignments;
- Display of all objects that a user is responsible for as well as all profiles defined for a user;

- Data-centric, hierarchical navigation of inventory content using explorers;
- Simple and hierarchical search facilities to retrieve objects;
- Automatically generated reports in flexible formats for the relevant objects in the inventory;
- Usage of Treemaps, Layered Diagrams, Matrix Diagrams, Kiviati Diagrams, Pivot Tables, Lane Diagrams, Geomaps, Portfolio Charts, Waterfall Charts, Multi-level Pie Charts, Area Charts, Circular Roadmaps and other visualizations showing object dependencies, relationships, rankings and KPIs. The Custom Reports; expansion set is a pre-requisite to configuration of these reports;
- Bookmarks for linking to a particular page view in the software;
- Glossaries including a full-text search across a glossary;
- Sending of web links to share information with peers and stakeholders.

Additionally, the Base Package provides functionality for collaboration, customer-specific configuration and administration.

- Monitors, workflows and streams support stakeholder collaboration;
- Configuration meets customers' specific needs;
- Administration functions support product implementation;
- Mandate support for federated enterprise architecture;
- Alfabet mobile portfolio manager.

Enterprise Architecture Management Package:

The Alfabet Enterprise Architecture Management (EAM) server package in Alfabet is used to describe complex IT systems in terms of their business, application, information and technical layers, and to develop standards for change. It helps enterprise architects align the IT landscape with the business to guide competitive transformation.

Includes the following BITM capabilities:

- Application Architecture Definition;
- Information Architecture Definition;
- Technology Architecture Definition;
- Business Process Definition;
- Technical Service Definition;
- Organization Definition.

IT Governance, Risk and Compliance Package:

The Alfabet IT Governance, Risk and Compliance (GRC) server package helps enterprises identify and assess threats and risk more effectively and achieve greater efficiencies in compliance control. It provides greater insight into risk exposure to be able to understand which, e.g., IT systems, technology components, or projects carry risk due to direct and indirect threats, what the implications of the risk are, and what kind of mitigation measures are needed. It also supports the processes necessary for compliance management: definition of control sets,

evaluation of objects for specific controls, reporting and auditing. In anchoring control processes and objectives into the IT architecture, organizations can better keep up with the on-going demands for controls assessment in the evolution of a corporation's IT landscape. Data retention policies for business data ensure data retention is compliant, cost-effective and supports information needs.

Includes the following BITM capabilities:

- Application Risk Management;
- Project Risk Management;
- Information Risk Management;
- Compliance Management;
- Threat Management.

Portfolio Management Basic Package:

This package provides the means to view the enterprise in the context of business capabilities as a common basis for evaluating how well IT is supporting the enterprise's business requirements. They enable evaluation and identification of which business capabilities are core and where improvement in one or the other of the portfolios is needed. Portfolio governance capabilities enable the organization to organize the information needed to optimize portfolios, improve agility, and set the pace for changes. Tightly integrated portfolios deliver impact analyses to reduce planning errors and improve synergies between the portfolios.

Includes the following BITM capabilities:

- Business Capability Management;
- Application Portfolio Governance;
- Information Portfolio Governance;
- Technology Portfolio Governance;
- Architecture Evaluation.

Portfolio Management Advanced Package:

The Portfolio Management Advanced package enables IT managers to use a portfolio approach to assess assets, returns and risks in the IT landscape in order to reduce operating expenditure. The contract management capability lets organizations associate contractual terms and conditions with related architecture elements to understand change implications in order to minimize planning risk and avoid unnecessary costs. Cost driver analysis helps organizations associate costs to architecture elements and aggregate costs for individual business services, processes, and domains to understand exactly where costs accrue. This enables organization in making rational decisions without the risk of losing IT support for business due to cost drivers.

Includes the following BITM capabilities:

- Contract & Vendor Management;
- Cost Driver Analysis;
- Opex Optimization.

Portfolio Management Complete Package:

The Portfolio Management Complete package includes “service product portfolio management” as an integrated portfolio management approach. In a portfolio management concept, the service product portfolio can be optimized for greater performance, standardization, and simplification which lead to a higher agility in delivering on business demand. Additionally, users can analyze the impact of changes to application and technology portfolios on IT services in terms of availability and SLA-conformity. Also, this will enable users to better understand the consuming and sponsoring parties of IT services. Further, users can coordinate the analysis and planning of changes to IT services with the projects delivering on those changes. Finally, this package includes Service Product Portfolio Management BITM capabilities.

IT Planning Basic Package:

The IT Planning Basic package supports the definition of the various dimensions of the business model of the enterprise including its market products, sales channels, customer segments, markets, and brands. For Business/IT Synchronization, Alfabet’s patented master planning functionality is a keystone in translating business strategy into IT tactics. This function shows the usage of applications supporting business operations, i.e. business processes and executing organizations. Business supports managed in the master plan allow the strategic planners to define and communicate the rollout plans of application assets through dedicated lifecycle definitions. Providing IT organizations with a clear overview of the relevant aspects of the IT landscape in order to understand how strategic decisions impact the IT’s tactics and direction over time. Using master planning, IT strategy planners can explore tactical options and ensure that flexibility in the IT architecture is accommodated. The master plan is a highly condensed representation of the strategic plan, easy to comprehend, and is a single point of reference. Therefore, it is an excellent medium for discussion at decision boards. Finally, IT Planning Basic is suitable for planning roll-outs of applications along organizational or business structures and for communicating such plans.

Includes the following BITM capabilities:

- Business Model Definition;
- Business IT Synchronization;
- Target Architecture Design;
- Road-mapping.

IT Planning Complete Package:

The IT Planning Advanced package transforms new services demands from operational business divisions into effective IT services by systematically capturing, assessing, and evaluating new IT demands with their underlying business motivation. Demand Management helps business analysts and IT identify the context and scope of each demand to be able to better understand the business need and potential architectural effect of its realization. This package helps in filtering the profusion of incoming demands into a manageable list that can be evaluated and translated into project proposals. The Project Portfolio Governance capability provides functionality for the definition, planning, assessment, and prioritization of project proposals and programs. Those capabilities are used to assign defined projects to programs and conduct architecture analysis, risk assessment, and validation of skill availability. The Project Portfolio Governance process in Alfabet informs decision-makers of the value, architecture alignment, and risk across a number of possible IT investment alternatives. The governance process is used to prioritize project proposals on the basis of strategic and technical alignment, resource priorities and risk.

Includes the following BITM capabilities:

- Demand Management;
- Project Portfolio Governance.

IT Planning Complete Package:

The IT Planning Complete package ensures that IT planning is performed and executed with full understanding of the enterprise's strategic and operational goals. The alignment of IT investments with business strategy is essential for revealing the actual value of IT services, enable informed decision-making and continuously improve service quality. Business Strategy Validation provides a framework for systematically deriving IT initiatives from business strategies. Operating Model Planning is the business foundation for enterprise transformation. This model is used to describe, evaluate and plan the company's business operating model and relate it to the IT architecture for planning the necessary changes to the enterprise landscape.

Includes the following BITM capabilities:

- Business Strategy Validation;
- Operating Model Planning;
- Scenario Management;
- Project & Release Design;
- Investment Optimization.

Expansion Sets:

Alfabet's expansion sets provide functionality for configuring solutions for organizations' individual needs and for greatly enhancing the user experience with products. The Base Package is a pre-requisite for using any of these expansion sets. Configuration of Alfabet with these expansion sets is conducted by specially trained solution designers in a networked development environment, i.e., networked non-production instance, or a local installation, i.e., non-networked presentation instance, as licensed by the customer. Changes to configurations are applied to the relevant production instance using the Alfabet Administrator application and a specifically created file comprising the configuration changes by the customer's administrative personnel.

- **Custom Reports:** Custom Reports expansion set enables customers to complement standard reports, diagrams, and analysis views available with Alfabet with customer-specific visualizations, diagrams and analysis views.
- **Alfabet Data Integration Framework (ADIF):** ADIF is a configurable mass update facility for high performance import, export and manipulation of large data volumes.
- **Guide Page Configuration:** With Guide Page Configuration, the user can create a look and feel matching corporate design or preferences, for example, the background and navigation tree. It allows definition of role-specific navigation through Alfabet as well as instructional text and shortcuts into the solution. This includes a configurable search for fast and targeted access to specific information. This expansion set is a configuration license. Customers can use guide pages without licensing this expansion set but cannot configure guide pages themselves without licensing this expansion set.

- **Solution Configuration:** Solution configuration enables the customer to own the configuration of the solution for its community of users based on the standard reports and object profiles defined for Alfabet.
- **Workflow Configuration:** Create and administrate automated workflow processes;
- **Survey Facility:** The Survey Facility enables run-time definition of auxiliary information and presentation models as well as auxiliary workflows for quick implementation of data gathering campaigns targeting the Alfabet stakeholder community. The facility provides an easily configurable survey procedure, a high level of automation, high data quality and reportable results on specific objects as well as the entire survey project. Data capture is governed using a proven process for efficiency and integrity.
- **Alfabet Publication Framework:** The Alfabet Publication Framework provides a framework for creating publications using user-defined templates for the format and desired content of the publication. Users define templates in Microsoft® Word® (.dot templates), determining text layout, creating static and dynamic fields, and formatting the document according to corporate standards or other publishing guidelines. Dynamic fields are filled with content from Alfabet such as the names of ICT objects, applications, domains and business processes as well as any standard or custom report related to an object. The template can hold a nested structure of separate documents on different objects. Once the template is configured by the solution designer, it is used by end users to create publications using the standard user interface.
- **Management Cockpits:** Alfabet's cockpits are a powerful medium for fast-path access to needed information. Using the Solution Configuration Expansion set they can be configured for a class of objects, such as a project or application and can contain different information sets for different user profiles in the user community. Individual user profiles and classes can, in turn also have several cockpits allowing the user to view information on an object according to different themes.
- **Historiography:** History tracking capability to document and track the history of changes made to objects in the IT architecture.
- **ARIS/Alfabet Interoperability:** The ARIS/Alfabet interoperability facility enables users to traverse both products to understand the relationships between business processes and their supporting applications as well as their enterprise context. This new capability ensures tighter business-IT collaboration on the whole range of business-IT management activities - from planning of business model changes to the implementation of IT-enabled business solutions.

User Types:

- **Alfabet Analysis User:** Users with the status of Analysis User access Alfabet for the sole purpose of viewing information relating to the enterprise architecture, IT planning and portfolio management activities the enterprise is engaging in. Information may be accessed through any of the functions available in Alfabet's base package and the functional packages the customer has licensed. This includes the use of dashboards, bookmarks or express views. A read-only user profile must be defined for the Analysis User. Analysis Users can attach notes to objects and notify the owners of objects as needed.
- **Alfabet Business User:** Alfabet Business Users are the main drivers of value-adding activities such as architecture landscape assessment and planning, master planning, strategy deduction, and capability management. The product functionality required to accomplish these tasks make up Alfabet's various server packages. Business Users have access to all of the functionality contained within the package(s) the customer

has licensed in a fully interactive mode. Permissions for Business Users to make changes to the information comprised in Alfabet are governed by the user and access rights set up in Alfabet.

- **Alfabet Access User:** Alfabet Access User licenses permit customers to use external solutions to capture information that is predominantly processed, stored and managed in Alfabet thereby replacing data management functionality natively provided in Alfabet with an alternative. Such information is typically fed into Alfabet using an integration solution, e.g., based on the Alfabet Data Integration Framework or web services communication. Any user with an external solution requires an Alfabet Access User license.

Components Relevant to Alfabet Cloud Enterprise Edition System

AWS Infrastructure:

Alfabet Cloud Enterprise's infrastructure is provided by Amazon Web Services (AWS), an ISO 27001 certified third-party vendor. Alfabet Cloud Enterprise's products are deployed as a public cloud, multi-tenant environment or a single tenant environment. It is hosted in the following regions – US, EU, AP, Brazil, Singapore, Japan, and Sydney – which gives the customers the ability to select the best region for their connectivity needs. The customer's environment can be hosted in the AWS region of their choice.

Sensitive data are stored only inside of Amazon environment. Only system documentation and the processes and procedures for management of the service are stored in the Software AG network. Access to this network is restricted by general Software AG policies (centralized domain control, limited access to servers and folders managed by central policies).

Physical access to Software AG's operations facilities is strictly controlled and monitored via Software AG's Physical Access Security Policy. Software AG has implemented a quality management system and is "ISO 9001:2015" certified for Global Support and Research & Development including supporting services (IT-Services, HR, Facility Management). Access to the AWS data center facilities as a subservice provider is managed by AWS.

Only the Alfabet Cloud Service Operations (CSO) has access to the environment via the Amazon Web Service console login. Two-factor authentication is implemented for these accounts and account activities are logged using AWS Cloud Trail services.

Monitoring Software

- **AWS Trusted Advisor:** AWS Trusted Advisor helps in provisioning resources by following best practices. AWS Trusted provides a general overview of all related AWS resources regarding Cost Optimizing, Performance, Security, and Fault Tolerance. See <https://aws.amazon.com/premiumsupport/trustedadvisor/>
- **AWS CloudTrail:** The AWS CloudTrail web service records AWS API calls and delivers log files. These log files are being stored in the S3 instance. See <http://aws.amazon.com/cloudtrail/>
- **AWS CloudWatch:** Amazon CloudWatch provides monitoring for AWS cloud resources. Respective log files are stored in the S3 instance. See <http://aws.amazon.com/cloudwatch/>
- **AWS Inspector:** Amazon Inspector is a security vulnerability assessment service that helps improve the security and compliance of your AWS resources. See <http://aws.amazon.com/inspector/>
- **Splunk:** Splunk Enterprise makes it simple to collect, analyze and real-time data. It is a Security Information and Event Management Software See http://www.splunk.com/en_us/products/splunk-enterprise.html

- **Trend Micro “Deep Security”:** Deep Security is an Infrastructure Protection tool that provides Intrusion Detection and Prevention, Virus scan and vulnerabilities scanning for the customer’s environment. See <http://www.trendmicro.com/aws/>

Operating Software

- **Windows Operating System:** Alfabet Cloud server instances are running Windows Operating system and are licensed through AWS on their EC2 service
- **MS SQL Database:** Microsoft SQL Server is a relational database management system developed by Microsoft and is licensed through AWS on their RDS service.
- **Labcase:** Labcase is a project management and document management system. Cloud Service Operations stores installation details such as licenses, contract or email templates in Labcase. Access to Labcase is restricted to authorized Cloud Operations users only.
- **KeePass:** KeePass is a free open source password manager which helps in managing passwords in a secure way. All passwords are kept in one database which is locked with one master key or a key file. The database is encrypted (AES and Twofish).
- **Password Depot Manager Server/Client:** Password Depot Enterprise Server lets the companies centrally manage, administer and share passwords, access data and documents. You decide down to the smallest detail what access rights a user is granted, what folders or entries s/he can view, or, for example, what kind of activities should be tracked.
- **Pivotal/Empower:** Pivotal/Empower is the support incident tool of Software AG. All incidents of Cloud customers are logged via Empower and worked on in Pivotal. The Cloud Support Manager or Cloud Support Expert checks support incidents for cloud specific properties and forwards them to Cloud Service Operations as required. The status of the incident is communicated via Empower to the customer.
- **iTrac (Jira):** iTrac is the CSO and R&D bug fix and change management ticketing system. Customer incidents can be escalated to iTrac from Pivotal by the Global Support team or directly entered as incidents are identified.
- **S3 Browser:** S3 Browser is a freeware Windows client for Amazon S3 and Amazon CloudFront. CSO uses the S3 Browser to download log files or backups. Access to respective S3 resources is restricted to a dedicated cloud service operations user role. See <http://s3browser.com/>
- **Putty:** Putty is an Open Source SSH and telnet client. It is used for remote log into the servers.
- **WinSCP:** WinSCP is an open source free SFTP client, FTP client, WebDAV client and SCP client for Windows. The main function of WinSCP, is file transfer between a local and a remote computer. Additionally, WinSCP offers scripting and basic file manager functionality.
- **Identity and Access Federation:** The SAML component is fully compliant with the OASIS Security Assertion Markup Language v2.0 specification. See <http://www.componentspace.com/SAMLv20.aspx>
- **UsingIT/Iwiki:**

Tool used for documentation of and communication amongst Alfabet CSO. It is based on the Alfabet software developed and implemented by the Alfabet CSO Team.

- **Duo Security:** Duo's Trusted Access platform secures your organization by verifying the identity of your users and the health of their devices before they connect to your applications. See <https://duo.com/>
- **JumpCloud:** JumpCloud's Directory-as-a-Service® centralizes and simplifies identity management. Give your users one set of credentials to securely access their systems, apps, networks, and file servers – regardless of platform, protocol, provider, or location.
See <https://jumpcloud.com>

Organizational Structures

Alfabet Cloud Enterprise is administrated and managed by the Cloud Service Operations Team (CSO). Members of the CSO are located in Software AG subsidiaries in Germany/Berlin. The CSO team is available 24/7 to provide follow the sun coverage for cloud product support needs and to offer maintenance windows outside of customer's standard business hours. The CSO interacts with several other Software AG teams in order to provide the Cloud service.

The ALFABET Cloud Operation Team interacts with three entities:

- **Research and Development:** RnD develops and releases new product versions on a half-year basis as well as patch releases on demand and hands them over to the CSO Team. The RnD process already includes a QA process that guarantees the security and stability of the product release.
- **Consulting Services:** Software AG Global Consulting Services (GCS) or Implementation partners will be involved in the planning of upgrading customer cloud environments to new product releases as part of the maintenance planning process conducted by the CSO or in configuration changes as part of Statements of Work.
- **Contract Management & Legal:** The CM&L Team is responsible for handover of a new contract to the CSO Team as a basis for delivering the service.

Procedures: All processes and procedures are regularly reviewed by CSO Management and relevant team members. A sample of recurring reviews is listed below.

- **Organizational Structure** - Including the assignment of roles and responsibilities and yearly review. Participants include the CSO team;
- **Contract Changes** – Monthly review is conducted in case of any amendments or service updates Participants include the CSO team, Product Management, Cloud Security, and Legal as necessary;
- **Monitoring Process** - Reviewed on a yearly basis by the CSO Management and the Monitoring experts;
- **Escalation Process** - Reviewed on a yearly basis by the CSO Management;
- **Access Control and Risk Logs** – Reviewed on a monthly basis by CSO Management.

Additionally, Software AG maintains procedures related to customer onboarding, customer service, and contract termination process as documented below.

Onboarding Customers: End-user registration and onboarding is normally done via integration to the customer's authoritative source of identity information, e.g., an LDAP or AD. Alfabet Cloud Enterprise also provides for an in-built user management function that is operated by explicitly authorized administrative individuals through the user profile configuration and assignment process.

Customer Support: Standard Support for all cloud products include a 24/7 access to the Customer web portal called Empower (<https://empower.softwareag.com>) where customers can search the Knowledge Center for articles, early warnings and technical whitepapers, access product documentation, and contact support through an eService interface. Within Empower, the customer can access all user guides, documentation, and application handbooks for the product, which are regularly updated with each release.

Through the eService portal, customers can create incidents (support requests classified by crisis, critical or standard) and monitor the status of existing requests.

Data: All customer tenant data is contained in the Cloud Product Service (at runtime) and the database and file storage (at rest). Access to the technical AWS infrastructure is restricted to only required team members using least privileges and all account activities are logged and monitored. Standard HTTPS encryption is used during transfer from the browser to the web server. All scoped data is stored in a secured Amazon Webservices (AWS) environment. It is transmitted through HTTPS with up-to-date encryption ciphers. Data-at-rest is protected using AWS S3 server-side encryption, AWS EBS volume encryption, and/or AWS RDS encryption.

The CSO personnel do not have access to scoped tenant data unless explicitly granted by customer. In case of a support incident, which requires access to the customer's Cloud Product tenant data, the customer can choose to grant access to the CSO to examine the issue by providing user credentials, function privileges and client license to access the data.

Control Environment:

Integrity and Ethical Values: Software AG's Corporate Security Officer is responsible for awareness and complying with security policies, procedures and standards. In addition, every Software AG employee is required to comply with the Company's Code of Business Conduct and Ethics. Cloud Service Unit Management ensures that all Cloud Service Unit employees complete periodic security and compliance training.

Management and Board of Directors: The Supervisory Board collaborates with the Software AG Management Board to fulfill its advisory role as required by law and by the company's articles of incorporation. The Supervisory Board advises the Management Board in aspects of running the company and supervises work performed by the Management Board. In doing so, the Supervisory Board is directly involved in all decision of key relevance to Software AG. The Management Board informs the Supervisory Board regularly, comprehensively and promptly regarding all important aspects of strategy, the status of strategy implementation, planning, business development, the risk situation and risk management, and compliance via oral and written reports. The Management Board is also available to the Supervisory Board in meetings for questions and discussions were any deviation from planned business development is explained in detail.

Assignment of Authority and Responsibility:

Key roles and responsibilities are assigned to individuals responsible for operating the Alfabet Cloud Enterprise products. Team members have both the skills and competencies to match their responsibilities and receive annual

training to maintain these skills. Team members whose responsibilities involve technical roles have external accreditation. Job descriptions are reviewed and revised as necessary on a yearly basis.

Talent Management Policies and Practices:

All CSO employees are required to regularly complete the Global Code of Business Conduct training, and receive performance reviews on an annual basis. The CSO team and the R&D team also complete an annual cloud security training course lead by the Cloud Security and Compliance Team.

Policies and procedures documents for significant processes, which include responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints, are published and available in the process documentation made available to all internal users via the documented incident process model. The CSO team reviews and updates Cloud Services procedural documentation on a semi-annual basis or as needed with product update.

Software AG Cloud Service Unit (CSU) Information Security Management**Program (ISMP)**

The Software AG CSU has designed, deployed and monitors their information security management system (ISMS) in accordance with the ISO 27001:2013 standard. CSU achieved certification for this standard effective December 27, 2017 and has deployed monitoring and surveillance audit program to maintain this certification through December 27, 2020. See also: [Cloud ISMS ISO/IEC 27001 certificate](#)

Software AG Business Continuity Management System

Software AG has designed, deployed and maintains an ISO 22301 based Business Continuity Management System (BCMS) for the CSU business unit (as well as several other aspects of the Software AG enterprise.) Software AG achieved certification for this standard effective December 15, 2016 and has deployed monitoring and surveillance audit program to maintain this certification through December 15, 2019. See also: [IS 22301 Business Continuity Management System Certificate](#)

Risk Assessment:**Risk Analysis and Risk Management:**

An organizational and information technology risk analysis is performed to enable the Cloud Service Unit (CSU) to establish information technology systems and organizations that provide the security that is required by law and is proportionate to risks. The analysis makes it possible to identify the security flaws of IT systems, as well as entities of implemented controls that are ineffective. Therefore, A mandatory information technology and organizational risk analysis is carried out for CSU IT systems and CSU Organization at least annually.

A risk assessment is further performed in cases where an enhanced or priority new system, system component or application is deployed, the major version of an existing system or application is changed, or wherever appropriate due to negative external or internal effects.

Controlled Activities:

System Account Management: Only authorized Software AG Support teams such as R&D, Global Cloud Support, and Cloud Service Operations (CSO) members have access to the Amazon Web Service console and the infrastructure of the Cloud service. AWS access is controlled through a Central Account Management policy where

users are assigned roles depending on the requirements of their position. The administrators can only access the AWS console using multi-factor-authentication. Within AWS, these roles are governed by a shared Trust Policy, an AWS document in which a definition of roles and responsibilities of all parties are documented. All activity within AWS is logged and monitored by AWS CloudTrail.

Data Backup and Recovery Management: An automated backup process is established and is reviewed periodically. The snapshot procedure is a backup of the system including the operating system and program setup excluding the database and log files. The snapshot is provided after any change to the environment, the first snapshot contains all initial setups. After finishing a maintenance window, a snapshot will be provided. The snapshots are stored for a period of 30 days or until completion of user acceptance test.

Incident Management: After a support incident is created, it is assigned to a Cloud product Customer Service Representative (CSR). The CSR initially troubleshoots the issue and if they cannot resolve it, they will determine whether the incident is related to the standard a specific Cloud product or to a Cloud specific topic. If it is related to a Cloud specific topic, the CSR will ask via Pivotal for CSO support. CSO will try to fix the issue or escalate to a product specific Cloud R&D team for support. In both cases, the Global Support team will be updated via Pivotal. If R&D has to be involved in an incident, an iTrac issue is created and all details to the incident are exchanged via iTrac between Global Support or CSO and R&D. iTrac (Jira) is the ticketing system used for all development and production changes for products and cloud environments.

Change Management: Software AG Cloud Products are updated on a semi-annual basis. The supporting teams have processes in place to ensure a smooth upgrade with minimal customer impact. The development and operations teams for the Cloud products incorporate a rigorous change management process, which mitigates the risk of unscheduled downtime due to unexpected results from a change in the production.

System Monitoring: AWS maintains responsibility for monitoring the AWS infrastructure used by Software AG, while the Software AG Security Team is responsible for monitoring activity and usage within the boundary of Software AG's cloud environment through the use of audit logs, logging analysis and alerting tools, and data visualization tools. All logs of system activity are stored for at least 90 days. These data points from system components and endpoints allow CSO to monitor system performance, potential security threats and vulnerabilities, resource utilization, and detection of unusual system activity. The CSO team receives alerts when the log data triggers certain performance metrics (such as an EC2 instance is not responding), a capacity warning or a latency issue. Depending on the severity of the alert, the responsible team member will review and make the necessary remediation.

System Security Testing: Software AG Cloud Products have a rigorous software design and development processes. R&D follows industry standards such as OpenSAMM for Software Development Lifecycle Management. R&D performs design review to verify the built-in security features and to identify any missing security features. Third-party component scans are performed to identify any vulnerable components in use. In addition, manual penetration tests, log analysis, session mismanagement, platform specific attacks, etc., are performed on all the interfaces provided by the application. For all the Cloud hosted products, network penetration testing is performed, along with port scanning and security configuration audits on network devices.

In addition to the regular anti-virus and vulnerability scans performed by CSO on the Cloud environments, the R&D Security Team conducts web application vulnerability testing on a yearly basis. Any vulnerability noted is

incorporated into the risk assessment process. A yearly Network Penetration Test and a pre-release cycle Network Penetration Test is performed as part of the development life cycle as well.

Penetration Test: Penetration Testing is executed on a yearly basis in a model cloud environment based on OWASP community best practices. The Cloud Products Test Manager is responsible to define the test scenario in agreement with the R&D department four weeks prior to the test and to plan the test run in agreement with AWS services.

In addition, Cloud Security and Compliance engages with an external security testing company to perform a penetration test for Cloud products.

Information and Communication Systems

Communication Systems:

- The Alfabet Web Application connects directly to the Alfabet database. The Alfabet Server is only required to set up Alfabet Web services or run batch-processing tools if required. Other Alfabet Tools connect directly to the Alfabet database. The Alfabet Web Application, Alfabet Server and other Alfabet tools are deployed on an AWS EC2 instance (for details see section infrastructure on EC2).

Documentation and Communication:

- Documentation is conducted in using IT (see 'Software' section for more). Only members of CSO have access to the Alfabet Enterprise Cloud relevant data.
- For communication with the customer regarding maintenance windows activities Software AG's support portal Empower (see 'Software' section for more) is used.

Alfabet CSO has a team calendar functionality in Outlook where all events - like maintenance windows - are scheduled for the different Cloud customers

Monitoring Controls: Based on ISO 27001, CSO maintains and improve the security controls monitoring processes through verification, monitoring and assessing performance of controls against organizational policies and objectives, and reporting the results to management for review.