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

Report on SAG Cloud GmbH's

webMethods Integration Cloud System

Relevant to Security and Availability

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

Table of Contents

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 WebMethods Integration Cloud 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 WebMethods Integration Cloud System throughout the period of April 1, 2018 to September 30, 2018 based on the AICPA Trust Services Security and Availability principles.

Aprio, LLP

Atlanta, GA

October 31, 2018

SECTION II

Management Assertion and System Description

Management of SAG Cloud GmbH’s Description of its WebMethods Integration Cloud 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 webMethods Integration Cloud 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 availabilitywere 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*. 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 WebMethods Integration Cloud 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.

webMethods Integration Cloud System Overview

webMethods Integration Cloud is Software AG's Integration Platform as a Service (iPaaS) offering. It enables organizations to quickly and easily integrate Software-as-a-Service (SaaS) applications such as Salesforce and Success Factors. Additionally, it also facilitates a secure and reliable way to integrate SaaS applications with organization's on-premises hosted ERP, CRM and warehouse applications such as SAP systems and Oracle e-business suite. webMethods Integration Cloud includes the following features:

- Seamless integration of SaaS applications;
- Secure and reliable integration with on-premises hosted applications;
- User Interface supporting guided development for faster development and deployment;
- Sophisticated orchestration using easy-to-use graphical design language;
- Connectivity to many popular SaaS applications;
- Web Services with a SOAP connector;
- FTP servers for file transfers with a FTP/FTPS connector;
- Support for full development life cycle with stages;
- Multi-tenant architecture which scales elastically based on demand.

webMethods Integration Cloud provides a way to eliminate integration silos that arise when adding new cloud-based applications to your SaaS environment. Customers can seamlessly integrate applications hosted in public or private clouds, as well as applications hosted on premise. With webMethods Integration Cloud, organizations can standardize a single integration technology.

wMIC Core Features:

- **User Interface:** webMethods Integration Cloud's user interface is built for business users and citizen developers. The user interface supports guided development and wizards to help users create integrations. The user interface runs on all latest browsers and on the tablets.

- **Sophisticated Service Orchestration:** webMethods Integration Cloud's graphical user interface provides easy to use graphical design language to build complex integrations involving multiple applications and other integrations. This graphical design language is easy enough to use by non-integration specialists/non-IT professionals.
- **Application Connectors:** webMethods Integration Cloud provides connectivity to many SaaS applications, some of which are Salesforce CRM, ServiceNow, StrikeIron, Amazon SQS, Amazon S3, Microsoft Dynamics CRM and SuccessFactors HCM.

  In addition, webMethods Integration Cloud provides the FTP/FTPS connector for connection to FTP servers for file transfers, and the SOAP connector to consume and communicate with Web Services.

  webMethods Integration Cloud allows users to define multiple accounts to connect to these applications and define operations over these applications, which can be used in Integrations.
- **Mapping, Transformation & Enrichment:** Mapping, transformation, and enrichment are the core strengths of the webMethods Integration platform and now these capabilities are available to cloud users as well. Mapping and transformation capability can be utilized by simple drag-and-drop user interface, which a citizen developer can easily use.
- **Integration Agent:** webMethods Integration Cloud enables organizations to integrate their applications with those of their partners, as well as their own on-premises applications by providing a lightweight agent.
- **Stages and Development Lifecycle:** webMethods Integration Cloud allows organizations to manage their development lifecycle by providing multiple environments one for each stage in their development lifecycle. Up to three such environments called Stages can be created, i.e., Default, Test, and Live. Integrations and their referred assets, like operations, can be promoted from one stage to another enabling the organizations to implement rigorous software development life-cycle process in the cloud.

The Integration Cloud will provide the customers with stages on which versions of the integrations will work. There will always be one stage called "Default". In cases where customers are not entitled to more stages, the whole staging management process will be performed in the default stage.

Promotions from one stage to another includes a strong Change Management process, which mitigates the risk of unscheduled outages during the migration to the production environment and thereafter. A series of tests and approvals have to be passed before moving from one stage to the next. Any tests or steps that fail during a pre-production stage require a root-cause-analysis of the issue, a fix, and a retest before a passing mark and approval to move to the next stage can be received.

Components Relevant to webMethods Integration Cloud System

- **AWS Infrastructure:** webMethods Integration Cloud's infrastructure is provided by Amazon Web Services (AWS), an ISO 27001 certified third-party vendor. webMethods Integration Cloud is deployed as a public cloud, multi-tenant concept where customers share central resources but are virtually segregated. Customers can purchase either Integration Cloud Basic, Advanced or Enterprise levels which grant additional dedicated virtual Integration Server instances to the tenant. The webMethods platform is available in two regions – United States and Europe. Customers can select the best region to host their tenant in order to meet their connectivity needs.

- **AWS VPC:** A Virtual Private Cloud (VPC) service instance from AWS secures the customer's service installation against intrusion. Amazon VPC (Virtual Private Cloud) is used to provide a private, isolated section of the AWS Cloud where AWS resources are launched in a defined virtual network. See http://aws.amazon.com/vpc/

- **AWS EC2:** Amazon EC2 provides resizable compute capacity in the cloud. EC2 (Elastic Cloud Compute) is the virtual computing environment with the Operating System. It is used for the deployment of the Cloud software and workloads of web application, application server and additional Cloud components. See http://aws.amazon.com/ec2/

- **AWS S3:** Amazon S3 (Simple Storage Service) provides a fully redundant data storage infrastructure. The AWS S3 instance is used to securely store all log information, for example the event monitoring and application log information etc. See http://aws.amazon.com/s3/

- **AWS ROUTE 53:** Amazon Route 53 is a highly available and scalable Domain Name System (DNS) web service, which is used for accelerated content delivery of the Cloud to remotely located users by setting up a dedicated domain name for the customer. See http://aws.amazon.com/route53/

- **AWS Relational Database Service (RDS):** Amazon RDS (Relational Database Service) is used to set up, operate, and scale a SQL Server database in the cloud. It provides cost-efficient and resizable capacity while managing time-consuming database administration tasks. See https://aws.amazon.com/rds/

- **AWS Identity & Access Management:** AWS Identity and Access Management (IAM) is used to securely control access to AWS services and resources for dedicated members of the Operations team including the AWS Directory Services in which they are entitled. See https://aws.amazon.com/iam/

- **AWS Key Management Service (KMS):** AWS Key Management Service is a managed service that enables users to create and control the encryption keys used to encrypt data, and uses Hardware Security Modules to protect the security of keys. AWS Key Management Service is integrated with several other AWS services to help in protecting the data stored with these services. AWS Key Management Service is also integrated with AWS CloudTrail to provide users with logs of all key usage to help meet users' regulatory and compliance needs. See http://aws.amazon.com/kms/

- **AWS Config:** AWS Config is a fully managed service that provides users with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance. See http://aws.amazon.com/config/

- **AWS Simple Email Service (SES):** Amazon SES (Simple Email Service) is a highly scalable and cost-effective bulk and transactional email-sending service for the cloud. It is used to configure the SMTP service related to the webMethods Integrations Cloud software and for notifications to the CSO Team related to the AWS Lambda configuration. See http://aws.amazon.com/ses/

- **AWS Simple Notification Service (SNS):** Amazon Simple Notification Service is a fast, flexible, fully managed push notification service that allow users to send individual messages or to fan-out messages to large numbers of recipients. Amazon SNS makes it simple and cost effective to send push notifications to mobile device users, email recipients or even send messages to other distributed services. See http://aws.amazon.com/sns/

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/
- **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/
- **Zabbix:** Zabbix is used for performance, and availability monitoring of customer's Cloud Service components and resources. See http://www.zabbix.com/
- **Graylog:** Graylog is used for log management and analysis of customer's Cloud infrastructure components and resources. See https://www.graylog.org/

Operating Software:

- **webMethods Integration Server:** webMethods Integration Server is a run-time server that provides built-in services. The Integration Server provides a platform to develop, deploy, and execute services or integrations from webMethods Integration Cloud.
- **webMethods CloudStreams:** CloudSteams is a multi-component product that enables customers to develop and govern integration flows between software as a service (SaaS) providers such as Salesforce.com and on-premise applications such as CRM and ERP.
- **Universal Messaging:** Universal Messaging is fast, reliable, scalable, and flexible Java message-oriented middleware (MOM) that provides messaging functionality. Universal Messaging serves as the intermediary that routes data from webMethods Integration Cloud to on-premise and vice versa.
- **Agileapps Platform:** The Agileapps Platform is a database (MySQL 5.5.34-1) in the cloud that doubles as a PaaS (Platform as a Service). This enables customers to get a high-powered database including a suite of pre-built application templates, so customers can run, customize, and build enterprise apps "in the cloud"--applications that are driven by workflow processes and data policies and that support collaboration.
- **Memcached:** Memcached is a third-party caching mechanism used by the platform to cache the Application Data and other required elements, which improves performance by minimizing the user response time to the server.
- **Linux Operating System:** webMethods Integration Cloud server instances are running Linux Operating systems called CentOS 6.6 final and CentOS 7.x and are licensed through AWS on their EC2 service.

- **MySQL Database:** The product is running MySQL databases on the AWS RDS instances. MySQL Server Version 5.5.xx (Community Edition or Community Enterprise Edition). Learn more details at https://dev.mysql.com/downloads/mysql/5.5.html
- **Labcase:** Labcase is a project management and document management system. Cloud service operations stores all policies and important documents, as well as information for daily procedures in it. Access to Labcase is restricted to authorized Cloud Operation 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).
- **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. 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. Putty 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.
- **SAML:** The SAML component is fully compliant with the OASIS Security Assertion Markup Language v2.0 specification. See http://www.componentspace.com/SAMLv20.aspx

Organizational Structures

webMethods Integration Cloud is administrated and managed by the Cloud Service Operations Team (CSO). Members of the CSO team are located in Software AG subsidiaries in Germany, Bulgaria, Malaysia and the USA. The CSO team is distributed in different time zones in order to provide follow the sun coverage for cloud product support needs and to offer maintenance windows outside of customer's standard business hours.

The Cloud Service Operations team interacts with several other Software AG teams in order to provide the webMethods Integration Cloud service.

- **webMethods Research and Development:** R&D develops and releases new product versions on a 3 months basis. R&D is also responsible for the setup of new customers of the webMethods Integration Cloud. Once the new customer setup is complete, R&D will hand over the webMethods Integration Cloud to CSO. If an incident occurs in the environment that cannot be resolved by CSO, R&D may be asked to assist to resolve the issue.
- **Logistics:** Logistics informs CSO about new webMethods Integration Cloud customers and sends the customer their initial welcome e-mail with links for tenant creation.

- **Global Support:** Global Support is the single point of contact for webMethods Integration Cloud customers to report support incidents. Depending on the incident and whether it can be resolved directly by Global Support, the incident may be routed to CSO or R&D.
- **webMethods Product Management:** Product Management evaluates new features for webMethods Integration Cloud. They interface between R&D, Marketing and Sales for webMethods Integration Cloud topics.
- **Cloud Security & Compliance:** The Software AG Cloud Information Security & Compliance team is responsible for establishing security standards and policies to guarantee secure and compliant cloud service operations of Software AG's cloud offerings.

Procedures

All processes and procedures are regularly reviewed by CSO Management and relevant team members. Samples of recurring reviews are 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:

After a webMethods Integration Cloud opportunity is successfully closed, the Direct Sales team provides the customer contract to the Contract Admins. Then a Contract Admin creates a new contract in SAP and provides the contract information and customer license files to the Logistics team and CSO team. Customers are also provided with the counter-signed Cloud Services Agreement (also known as the Master Service Agreement) which includes a security and availability exhibit, the SLAs, and product specifications for their reference.

Customer Support:

Standard Support for all cloud products include 24/7 access to Customers' 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, customers 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

Customer tenant data is stored only inside the Amazon environment. Physical access to the AWS data centers is strictly controlled and audited according to their ISO 27001 and SOC 2 controls. Only the Cloud Service Operations (CSO) has access to the AWS hosted environment via either the Amazon Web Service console using two-factor authentication or direct SSH access to the OS-level of hosted resources using individual key-pairs. All AWS access attempts and activities within the hosted environments are logged using AWS Cloud Trail services. All customer tenant data is contained in the Platform (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 with updated ciphers are used during transfer from the browser to the web server. Data-at-rest is protected using AWS S3 server-side encryption, AWS EBS volume encryption, and/or AWS RDS encryption.

CSO personnel do not have access to customer tenant data unless explicitly granted by customer. In case of a support incident, which requires access to the customer's tenant data, the customer can choose to grant access to CSO to examine the issue by providing user credentials, function privileges and client license to access the data. Software AG customers retain control and ownership of their 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 deviations from planned business development are explained in detail.

Assignment of Authority and Responsibility: Key roles and responsibilities are assigned to individuals responsible for operating the webMethods Integration 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 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.

Control 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: webMethods customers expect that support services are available at all times to safeguard the continuity of their business systems. To ensure full support of the webMethods Integration Cloud, a Business Continuity and Disaster Recovery (BC/DR) policy for Software AG Global Support (and supporting functions) according to ISO 23001 standards has been enacted.

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

The CSU Cloud Information Security Policy is based on the implement an Information Security Management System (ISMS) that complies with 27001:2013 Standard. The policy demonstrates the direction and commitment of the management to information security in order to protect CSUs managed own information assets, customer information assets and those provided by third parties (internal and external suppliers).

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.