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

Report on SAG Cloud GmbH's

ARIS 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 ARIS 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 100*A 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 ARIS 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 ARIS 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 ARIS 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 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 ARIS 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.

System Overview

ARIS Cloud:

ARIS Cloud is a full-scale Business Process Analysis-as-a-Service (BPAaaS) product. It powers collaborative process improvement projects around the globe. Customers can subscribe to ARIS Cloud to collaboratively design, analyze, share and improve processes on a subscription base without any participation barriers. ARIS Cloud is available in two editions: Advanced and Enterprise – each providing a feature set to fit customer's current project needs.

ARIS Cloud Advanced:

ARIS Cloud Advanced is built for immediate process transparency and improvement projects. Intuitive, ready-to-use, and best practice, ARIS Cloud Advanced is for designers and architects needing instant and out-of-the-box support for immediate BPA work.

ARIS Cloud Advanced supports organizations that are at the beginning of their BPA journey or need a Software-as-a-Service based BPA solution. Common to these organizations is an ad-hoc approach to these disciplines, performing design and blue printing activities on an as-needed basis. ARIS Cloud Advanced provides the necessary capabilities to perform BPA activities that typically arise in these situations. With a pre-configuration set-up for design/modeling, collaboration, and portal functionalities, the foundation for process description (e.g. blueprinting) are quickly created in the system. The centralized inventory becomes a reliable source of information with an easy and straightforward process to refine and maintain it.

ARIS Cloud Advanced is based on proven ARIS technology. ARIS Cloud Advanced supports two user types that address the individual needs of BPA project or program.

- ARIS Cloud Designer creates and manages content. They are typically architects that, for instance, need to create a process model and start the collaboration with users (e.g. from a business side);
- ARIS Cloud Viewer is for users who are assigned read access to the content in ARIS Cloud. They are allowed to take part in the collaboration but not change content.

The users can administrate their ARIS Cloud Advanced tenant (or project room) via ARIS Cloud Administration, a Java-based Download Client. With this client, customers can manage the ARIS databases and the ARIS configuration.

ARIS Cloud Enterprise:

ARIS Cloud Enterprise is the collaborative improvement environment that integrates everyone in strategizing, blueprinting, and transforming to a digital enterprise. ARIS Cloud Enterprise allows business and IT to collaborate for true end-to-end business and IT improvement, guided by the necessary governance. The results are tangible: Lower costs, better quality, higher throughput, faster reaction times and proactive error correction.

Components Relevant to ARIS Cloud Products

ARIS Core Features:

ARIS Architect / ARIS Designer:

- Create, analyze and manage the entire enterprise model. Do everything from devising your process strategy to planning information architectures, application landscapes and services.

ARIS Connect Viewer / ARIS Connect Designer:

- Improve processes using a social network;
- Engage anyone, anywhere, anytime;
- Design, publish and dashboard processes all with one tool.

Connect, communicate and collaborate on processes easily on a social network Stakeholders from anywhere, even while mobile, can work together on processes. Add MashZone to view KPIs on dashboards so you can easily see where to make improvements.

Extension Packs:

The extension pack makes it easier for non-ARIS experts to contribute their process knowledge to ARIS based on simplified fact sheets. In addition, the ARIS Extension Pack enables users to use additional features of ARIS such as ARIS for SAP or Enterprise Architecture content.

ARIS for SAP Solutions:

Accelerate the design, documentation and optimization of SAP processes. This extension pack for ARIS Architect & Designer provides a fast and efficient way to map processes and business concepts to your SAP environment. It's used to bridge the gap between business and IT across the entire SAP life cycle.

ARIS Business Strategy:

- Design strategy models to support management decisions;
- Plan and implement a balanced scorecard system;
- Define the scope of Six Sigma® projects.

This extension pack for ARIS Architect & Designer enables users to bridge the gap between strategy definition, performance management and organizational structures.

ARIS Simulation:

- Identify best practices in processes;
- See if new processes are executable;
- Uncover process weaknesses and bottlenecks.

This extension pack for ARIS Architect & Designer helps with improving processes. Users can identify process, modeling errors, and inefficiencies or weaknesses using a wide range of analysis options.

ARIS Process Governance:

- Design and implement governance processes;
- Automate ARIS administration tasks;
- Reduce your process change effort by 80 percent.

Increase process, quality, flexibility and traceability by defining policies, roles, and responsibilities with ARIS Process Governance, an extension pack for ARIS Architect & Designer. Users can establish enterprise-wide policies for BPM and automate governance processes using a model-driven approach.

Model-to-Execute:

- Create and sustain the best processes for your business;
- Govern business and IT collaboration with built-in workflows;
- Achieve Business Process Excellence via continuous process improvement.

Align the architecture and design with automated processes and IT applications so that structure follows strategy.

ARIS Enterprise Architecture:

ARIS Enterprise Architecture helps Businesses and IT development planners to document and analyze existing Enterprise Architecture assets in an easy-to-use fashion based on the ARIS methodology. This includes structured documentation of IT components, such as applications, data and technologies, which unifies IT standards across the organization. It creates the basis for future IT projects while aligning IT structures with corporate strategy, global projects, and business processes.

ARIS Aware:

KPI monitoring, data analytics, self-service analytics, data visualization, situational awareness, dash boarding, process monitoring, and process benchmarking.

AWS Infrastructure:

The Cloud infrastructure for ARIS Cloud Advanced and Enterprise is provided by Amazon Web Services (AWS) (an ISO 27001 certified third-party vendor).

ARIS Cloud Advanced:

The ARIS Cloud Advanced is deployed on the AWS public cloud using a multi-tenant concept where customers share central resources but are virtually segregated. This platform is available in three regions – United States,

Europe, and Asia-Pacific. Customers can select the best region to host their tenant in order to meet their connectivity needs.

ARIS Cloud Enterprise:

The Cloud Enterprise is deployed on AWS infrastructure using a single-tenant concept where customers dedicate resources encapsulated in an individual Virtual Private Cloud (VPC). Customer can select between at least 8 different regions for hosting their tenant depending on best connectivity. Standard regions include US (Oregon, Virginia, California), EU (Ireland, Frankfurt), AP (Sydney, Singapore), and South America (Sao Paulo). Customer tenant data is stored only in the Amazon environment.

Common Infrastructure Software:

Some or all of the following service components are provided by AWS to facilitate the delivery of Cloud services.

- **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 Directory Service:** AWS Directory Service is a managed service that is used to connect the Cloud end users with an existing on-premise Microsoft Active Directory at customer location.

  See https://aws.amazon.com/directoryservice/
- **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 Lambda:** AWS Lambda allows users to run code without provisioning or managing servers. See http://aws.amazon.com/lambda/
- **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 ARIS software and for notifications to the ARIS CSO Team related to the AWS Lambda configuration. See http://aws.amazon.com/ses/
- **Amazon Simple Queue Service (SQS):** Amazon Simple Queue Service is a fast, reliable, scalable, fully managed message queuing service. See http://aws.amazon.com/sqs/
- **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 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 and vulnerabilities scanning for the customer's environment. See http://www.trendmicro.com/aws/
- **Ossec Open Source HIDS SECurity:** Ossec is used for UNIX system activity monitoring (file integrity, log files, root check and processes). See http://www.ossec.net//
- **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:

- **Linux Operating System:** ARIS Cloud server instances are running Linux Operating system and are licensed through AWS on their EC2 service.
- **PostgreSQL Database:** PostgreSQL is an open source object-relational database system used to store and manage ARIS data. PostgreSQL utilization depends on the type of data or the size of installation.
- **Oracle Database:** Oracle is used as the Database Management System for ARIS Cloud. Oracle manages the ARIS database content depending on the size of installation.
- **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).
- **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 with the ARIS Cloud installation. Multi factor authentication is required to connect via a password and a private key in combination with the personal user is required.
- **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.

Organizational Structures:

ARIS Cloud Products are administrated and managed by Cloud Service Operations (CSO). Members of the CSO are located globally in Software AG offices in Germany, Bulgaria, USA, Australia and Malaysia. CSO is distributed in different time zones in order to provide “follow the sun” coverage for customer’s 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 ARIS Cloud service:

- **ARIS Research and Development (R&D):** RnD develops and releases new product versions twice per year. They participate in regular ARIS Cloud Steering Committee meetings and Cloud Service Incident Review Meetings. Product related customer incidents may be escalated to ARIS R&D through an iTrac ticket.
- **Logistics:** Logistics informs CSO about new ARIS Cloud Customers and creates the respective ARIS licenses. They provide the licenses and license updates to CSO. In the case of ARIS Cloud Advanced, Logistics also creates the tenant (project room) within the User Management Console.
- **Global Support ARIS:** Global Support is the single point of contact for ARIS Cloud Customers. All support incidents are initially managed by a Global Support Customer Support Representative (CSR). If support cannot solve an incident directly, the incident is escalated to either CSO for cloud platform related issues, or to R&D for product related issues.
- **ARIS Product Management:** Product Management prioritizes new features for ARIS Cloud. They interface between RnD, CSO, Marketing and Sales for ARIS 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.

All teams that influence the management of the ARIS Cloud platform are documented at the corporate level in an organizational chart, which is available for all employees through the company intranet. This organizational chart is maintained dynamically through Human Resources' SAP Master Data module.

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.

ARIS Cloud Advanced Onboarding:

For ARIS Cloud Advanced customers, Logistics creates a new project room in the selected regional multi-tenant system using the Manage Cloud Portal (MCP) of the ARIS cloud application. Logistics also loads the required customer licenses into the system. The customer receives an automated confirmation e-mail on completion which includes their access credentials.

ARIS Cloud Enterprise Onboarding:

For ARIS Cloud Enterprise, Customers are requested to complete a Connectivity and Deployment Questionnaire. The connectivity questionnaire asks the customer to provide required backend connectivity such as VPN tunnel data, LDAP-connection parameters, MS SharePoint information and SAP connectivity information.

Customer Support:

Standard Support for all cloud products includes 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, 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

All customer tenant data is contained in the Application (at runtime) and the database and file storage (at rest). Access to the technical AWS infrastructure is restricted to only authorized 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 ARIS Cloud tenant data, customer may 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 ARIS 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.

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.

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: ARIS Cloud Customers expect that **support services** are available at all times to safeguard the continuity of their business systems. To ensure full support of ARIS Cloud Products, 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.

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.