



AXWAY SOFTWARE SA

INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT

FOR THE MANAGED CLOUD SERVICES SYSTEM

FOR THE PERIOD OF OCTOBER 1, 2021, TO SEPTEMBER 30, 2022

Attestation and Compliance Services



Proprietary & Confidential

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

INDEPENDENT SERVICE AUDITOR'S REPORT

To Axway Software SA:

Scope

We have examined Axway Software SA's ("Axway") accompanying assertion titled "Assertion of Axway Service Organization Management" ("assertion") that the controls within Axway's Managed Cloud Services system ("system") were effective throughout the period October 1, 2021, to September 30, 2022, to provide reasonable assurance that Axway's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Axway uses a subservice organization for cloud hosting services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Axway, to achieve Axway's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

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

Our examination included:

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

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

Inherent Limitations

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

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

Opinion

In our opinion, management's assertion that the controls within Axway's Managed Cloud Services system were effective throughout the period October 1, 2021, through September 30, 2022, to provide reasonable assurance that Axway's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

 SCHEELMAN & COMPANY, LLC

Tampa, Florida
December 14, 2022

ASSERTION OF AXWAY SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Axway Software SA's ("Axway") Managed Cloud Services system ("system") throughout the period October 1, 2021, to September 30, 2022, to provide reasonable assurance that Axway's service commitments and system requirements relevant to security, availability, processing integrity, and confidentiality were achieved. Our description of the boundaries of the system is presented below and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period October 1, 2021, to September 31, 2022, to provide reasonable assurance that Axway's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Axway's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

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

We assert that the controls within the system were effective throughout the period October 1, 2021, to September 30, 2022, to provide reasonable assurance that Axway's service commitments and systems requirements were achieved based on the applicable trust services criteria.

DESCRIPTION OF THE BOUNDARIES OF THE MANAGED CLOUD SERVICES SYSTEM

Company Background

Axway Software SA (Axway) (Euronext: AXW.PA) enables enterprises to securely open everything by integrating and moving data across a complex world of new and old technologies. Axway's application program interface (API)-driven B2B integration and MFT software, refined over 20 years, complements Axway Amplify, an open API management platform that makes APIs easier to discover and reuse across multiple teams, vendors, and cloud environments. Axway has helped over 11,000 businesses unlock the full value of their existing digital ecosystems to create brilliant experiences, innovate new services, and reach new markets. Services offered include Managed Cloud Services (MCS) that provide enterprises the ability to assess, deploy, and configure solutions to help support their business and legacy infrastructure requirements. The MCS organization has cloud-specific service delivery teams located in Scottsdale, Arizona; Paris, France; Berlin, Germany; Bucharest, Romania; and Sofia, Bulgaria.

Description of Services Provided

The MCS environment consists of multiple Axway service offerings built around the AMPLIFY platform, including, but not limited to, cloud integration, API management, cloud business to business (B2B) managed services, cloud-based managed file transfer (MFT) services, and traceability and compliance in the cloud. MCS customers receive network and server infrastructure managed by Axway to the customers' on-premises systems or to partner cloud networks.

MCS offerings are organized into two distinct platform delivery models:

Private Cloud

The technical environment is dedicated to the customer and isolated from all other customers, but some elements remain common and shared with other customers (e.g., network access, firewall, virtualization, etc.). Axway is responsible for the technical architecture and its components, but the customer has the ability to customize the software solution and control the pace of patches and upgrades according to individual business needs.

Public Cloud

The public cloud platform is shared among multiple customers and made available to customers utilizing a pay-per-usage model. Axway manages the configurations and the set of software technologies. Customization of the environment is limited to configuration settings made specifically accessible to the customer by Axway. Axway regularly updates these platforms and delivers any enhancements to its customers. Maintenance is scheduled by Axway and will impact all customers on the shared service platform.

In both cloud platform models, licenses and technical infrastructure are owned by Axway and are made available to the customer in a subscription model. The customer has a right to use the services implemented and operated by Axway in accordance with its commitments.

System Boundaries

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

Principal Service Commitments and System Requirements

Axway has procedures in place to help ensure that customer security, availability, confidentiality, and processing integrity commitments are met. Axway's commitments to user entities are documented and communicated to customers in the cloud services and service level agreement (SLA) description made available on the Axway

support site. Standard security, availability, confidentiality, and processing integrity commitments include, but are not limited to, the following:

- Monitor systems and control processes for availability of services, including maintaining availability of the platform at a minimum of 99.5% up to 99.99% based on the subscribed service level;
- Manage technical incidents and problems, including informing the customer of technical issues related to the services delivered (e.g., functional or business errors, errors on the services or components developed, configured, modified, or deployed by the customer, etc.);
- Manage backups and restorations;
- Manage network and system access;
- Capacity and release management;
- Customer data disposal commitments are communicated via customer contracts during the onboarding process;
- Dispose of customer data upon request and per agreed upon specifications;
- Customer web portal for customer production and processing inquiries; and
- Monitor data uploaded by customers to ensure data processed through the system is valid and alert customers of any failures.

Axway establishes operational requirements that support the achievement of the aforementioned principal service commitments, relevant laws and regulations, and other system requirements. These include the services of dedicated development and operations, Managed Cloud Services, account management, and systems support personnel and other technologies to manage system security, availability, confidentiality, and processing integrity service requirements, and the necessary system change management procedures to support the requisite authorization, documentation, testing, and approval of system changes. Service level agreement reporting is utilized to outline and report on agreed upon service level performance internally and product management teams report on an ongoing basis and externally with customer personnel on a per request basis. Data backup schedules are preconfigured and executed according to documented policies and procedures.

Such requirements are communicated in Axway's system policies and procedures, system design documentation, and contracts with customers and related third parties. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired, trained, and managed. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation of the Managed Cloud Services.

In accordance with Axway's assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

Infrastructure

Production Environment

The Axway Cloud is hosted within Amazon Web Services (AWS) Elastic Compute Cloud (EC2) and consists of a multi-tier virtualized architecture comprised of web and database servers, and network monitoring and logging tools. Axway does not own or maintain any of the hardware located in the AWS data centers, and operates under a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure (i.e. physical infrastructure, geographical regions, availability zones, edge locations) and Axway is responsible for securing the platform deployment in AWS (i.e. customer data, applications, identity access management, operating system and security group configurations, network traffic, encryption).

Axway’s environment is based on a multi-tenant architecture that applies common, consistent management practices for customers. AWS’ availability zones allow for redundancy and provide a reliable, scalable, high availability platform. Axway’s infrastructure is spread across multiple availability zones. The Axway network operations team monitors the performance of infrastructure resources and will request additional resources if capacity is insufficient. Axway customers each have one or more tenants that their data is stored in. Tenants are spread across multiple availability zones.

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

Primary Infrastructure			
Production System	Business Function Description	Platform	Physical Location
Active Directory (AD)	AD domains are utilized to control access to the corporate and production networks.	Windows	AWS
VPN Appliance	Access to the production environment requiring external users to authenticate using multiple factors to the corporate network.	Palo Alto GlobalProtect	
Firewalls	Protects the network perimeter and segregates network security zones.	Palo Alto and CheckPoint	
AWS Security Groups	AWS security groups within the AWS Identity and Access Management (IAM) console with the ability to configure, control, and restrict inbound and outbound network traffic into the production infrastructure.	AWS EC2 VPC	
Database	AWS Relational Database Service (RDS) supporting the enterprise Managed Cloud Services.	Oracle 09G and MySQL	
Servers and Virtual Machines	Production servers and virtual machines supporting the enterprise Managed Cloud Services.	Windows and Linux	

Software

The following technologies are utilized by Axway as part of the delivery of the MCS environment:

- CA Privileged Access Manager (CAPAM) - the virtual appliance provides Axway the ability to centrally manage authentication to the MCS environment.
- Open Source Security (OSSEC) - a host-based intrusion detection system (HIDS) that performs anti-malware monitoring, log analysis, file integrity checking, policy monitoring, and real-time alerting on the Linux servers deployed in the MCS environment.
- Rapid7 InsightVM - a vulnerability management and policy management tool provided by the vendor, Rapid 7. Axway uses the tool to perform vulnerability scans and configuration checks (policy management) on all MCS hosts.
- Syslog - a standard computer message event collection agent deployed on all MCS Linux servers to gather data on security events and system activity.
- Splunk - a log and event management software which aggregates logs from OSSEC, Syslog, and other sources. Splunk is used as a central repository to monitor the logs, provide reporting capabilities on the data, and alert appropriate personnel in the event of an identified issue.
- ServiceNow - a SaaS help desk solution provided by the vendor ServiceNow. It is used for incident/problem management in the MCS environment.
- Icinga - a monitoring tool used for visibility and alerting regarding system and network performance.

People

Personnel involved in the operation and use of the system include the following:

- Executive management - responsible for overseeing company-wide activities, establishing goals, and overseeing objectives.
- Human resources (HR) - responsible for policies, practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisitions, employee retention, compensation, employee benefits, performance management, employee relations and training, and development).
- Customer support - responsible for customer implementation and support to clients.
- Information technology (IT) - responsible for managing corporate information systems and administering all user account access and permission levels for production and corporate systems.
- Information security and risk department - responsible for managing, monitoring, and supporting user entities' information and systems from unauthorized access and use while maintaining integrity.
- Production operations - responsible for managing, monitoring, and supporting user entities' systems from unauthorized changes while maintaining availability.

Procedures

Access, Authentication and Authorization

Axway uses Windows AD as their directory service controlling authentication and access to the corporate network. Minimum password controls and account lockout thresholds are in place and configured. Predefined security groups are in place to assign role-based access privileges and segregate access to data within the domain. Administrative access privileges within AD are restricted to user accounts accessible by authorized personnel.

For remote access to the corporate network, a VPN system is utilized. In order to access the VPN a user must have an Axway issued workstation. VPN authentication requires a user's AD credentials and are encrypted via Internet protocol security (IPsec) and TLS.

Once a user has an authenticated VPN session, the user would then need to separately authenticate to the privileged access manager (CAPAM), which is configured with unique a username, password, and two-factor authentication configurations. Once authenticated, access is restricted based upon predefined role-based access groups, the ability to configure AWS security groups, provision and maintain production servers and databases, and access individuals' hosts is restrained to predefined role-based access groups. AWS IAM groups are also utilized within the AWS console which is provisioned using predefined user groups.

Access to and within the AWS environment is logged via CloudTrail; logs are sent to the central logging aggregation systems for IT personnel to review on an ad hoc basis.

Access Requests and Access Revocation

The automated ticketing system is utilized to aid in tracking for user access requests. For new employee access, a ticket will be created to provision access by the employee's manager in which IT personnel will be responsible for assigning and maintaining access rights to the in-scope systems based off management requests. Prior to granting any individual access to the production environment, management personnel must formally approve access rights to the production environment. Upon notification of an employee termination, HR personnel provide the required departments a notification of termination to ensure that employees do not retain system access subsequent to their termination date. IT personnel will remove any corporate and production access for the terminated employee. Termination requests are documented using the ticketing system. In addition, to help ensure access privileges are authorized, members of the security team complete an audit of AD accounts on a monthly basis to verify that users with access to the production systems are current employees or approved personnel. If any individual is identified to have unauthorized access, the issue is remediated immediately.

Change Management

Documented standard build procedures are utilized for installation and maintenance of production servers and includes use of an access control system to control and restrict access to authorized users.

Axway has documented application change development maintenance policies and procedures to communicate management's expectations regarding the change control process to personnel to ensure unauthorized changes are not made to production application systems. These policies and procedures apply to changes to the enterprise Managed Cloud Services and convey the change control process including, as necessary, maintenance procedures, rollback procedures, assessing the impact of changes, test plan, assessing the impact of not implementing the change, and approvals. A change advisory board (CAB) meeting is held on a weekly basis to review and discuss changes within the pipeline to be implemented into the production environment.

Operations personnel maintain documented procedures to guide personnel in the routine maintenance procedures and configuration requirements for systems. In addition, change management personnel involved in the change management process maintain a continuous discussion channel to discuss upcoming changes prioritization, and approval of change requests. Any changes that may have an impact on the customer will be communicated internally to management and to customers prior to deployment.

Data Backup and Disaster Recovery

Backup procedures and data retention policies are in place to communicate replication and recovery processes to relevant personnel to ensure systems are replicated as required and securely stored in order to preserve the integrity of customer data files. Axway utilizes Amazon's EC2 to process data, which is stored in Amazon RDS, which are managed by AWS. RDS has built-in configurable database (DB) Snapshot functionality, which acts as a backup. Automated backup systems are in place to perform scheduled backups of production systems data at predefined times. Backups are monitored by the enterprise monitoring tool to ensure backups are successfully performed according to the predefined backup schedule. Logs of successful and failed backups are sent to the centralized logging tool when certain threshold are met and are reviewed by operations personnel on a continuous basis to ensure the continued operation of the backups. Axway has configured their DB Snapshots to be initiated daily. This allows Axway to complete a full restoration of the database from a backup if an issue ever arose that required a restore to be performed.

In addition to backup snapshots, production data is replicated between availability zones to provide fail-over redundancy. Axway is configured with multiple AWS regions and availability zones to permit the resumption of IT operations in the event of a disaster.

Disaster recovery activities include members of the operations team perform testing of the disaster recovery plan, which includes a tabletop of the procedures that would need to be performed if a restore would be required on an annual basis. Operations personnel will perform a restore of the backups to ensure the backup restoration process is working as intended. Once the exercise is completed, an assessment of the results is conducted and follow-up actions are assigned, as needed. Access to the production backup data is restricted to user accounts accessible through the AWS console, which includes authorized operations, IT, and security personnel. Additionally, vendors are evaluated on an annual basis to help ensure that vendors or business partners are in compliance and are able to fulfill their responsibilities in accordance with commitments.

Incident Response

Documented incident response policies and procedures for reporting security, availability, confidentiality, and processing integrity incidents are communicated to internal users via the company intranet site to provide guidance in identifying and reporting failures, incidents, concerns, and other complaints. Customers have the ability to call during business hours and/or submit a ticket or e-mail customer support and/or IT security group 24 hours a day in order to report system issues and/or incidents. The customer-facing website provides guidance should they need to contact Axway for troubleshooting issues.

Dedicated network operations center (NOC) personnel are available to respond to security incidents 24 hours a day. IT security personnel utilize the automated ticketing system to document security violations, responses, and resolution. Incidents requiring a change to the system follow the standard change control process. The tickets are posted and communicated internally, and the ticket is tracked and monitored until resolution. Once IT security

personnel are informed about a potential security incident, a security staff member will attempt to verify the claims in the ticket and validate whether the events meet the definition of a security incident.

System Monitoring

System monitoring policies are in place to communicate system availability expectations. Documented standard build procedures are utilized for the installation and maintenance of production server instances and network infrastructure. The AWS system is configured to utilize multiple availability zones to allow for automatic rerouting of data and services if one availability zone fails. Axway has implemented the following monitoring controls:

- The production servers are configured to log access related events and send logs to a centralized logging tool.
- Enterprise monitoring applications are configured to monitor the in-scope systems capacity levels and alert operations personnel when predefined thresholds have been met.
- A HIDS is utilized to analyze network events and report possible or actual network security breaches.
- A third-party assessment tool is utilized to perform network vulnerability scans of the production environment on a monthly basis. Remediation plans are monitored and tracked through resolution.
- AWS security groups are reviewed on at least an annual basis to ensure that only necessary connections are configured within the security groups.

File Processing

The system allows users to manage the data workflows. The workflows are used to automate a business set of processes that would normally be performed manually and repetitively. Customers work with Axway to establish the system of processing data; however, customers are responsible for ensuring data is accurately input into the system.

Key processing activities follow the standard change management process and undergo regression testing to help ensure data is processed accurately.

Monitoring applications are configured to monitor data uploaded by customers within the MCS to help ensure that the data processed through the system is valid. In the event the data processed does not function correctly, the monitoring applications are configured to alert the operations team to investigate and resolve the issue.

Data

Axway tracks service availability trends through tickets submitted through the automated ticketing system, and data is aggregated into a reporting tool. During monthly or quarterly meetings, the Axway customer success manager meets with customers and provides a set of the following reporting metrics:

- Service Quality Indicator Reports – mean time to (MTT) restore, MTT respond, and service availability for the last month and history for the past 12 months;
- Consumption or use of the service for the last month and history for the past 12 months; and
- Incident volume by priority and per day.

Significant Changes During the Period

There were no significant changes that are likely to affect report users' understanding of how the in-scope system is used to provide the services covered by this examination during the period.

Subservice Organizations

The cloud hosting services provided by the hosting service were not included within the scope of this examination.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at AWS, alone or in combination with controls at Axway, and the types of controls expected to be implemented at AWS to achieve Axway’s service commitments and system requirements based on the applicable trust services criteria.

Control Activity Expected to be Implemented by the Hosting Service	Applicable Trust Services Criteria
The hosting service is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its IaaS cloud hosting services where Axway’s systems reside.	CC6.1 – CC6.3, CC6.5 – CC6.6, CC7.2, PI1.2, PI1.4
The hosting service is responsible for implementing controls for restricting physical access to data centers, backup media storage, and other system components including firewalls, routers, and servers.	CC6.4 – CC6.5, CC7.2
The hosting service is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its IaaS cloud hosting services where Axway’s systems reside.	CC6.7
The hosting service is responsible for monitoring any configuration changes of the logical access controls system for the underlying network, virtualization management, and storage devices for its IaaS cloud hosting services where Axway’s systems reside.	CC7.1
The hosting service is responsible for ensuring environmental protection controls are in place to meet Axway’s availability commitments and requirements.	A1.2

Complementary Controls at User Entities

Complementary user entity controls are not required, or significant, to achieve the service commitments and system requirements based on the applicable trust services criteria.

Trust Services Criteria Not Applicable to the In-Scope System

The Trust Services criteria presented below are not applicable to the Managed Cloud Services system within the scope of this examination. As a result, an associated control is not required to be in place at the service organization for the omitted applicable trust services criterion. The following table presents the trust services criterion that is not applicable for the Managed Cloud Services system at Axway.

Criteria #	Reason for Omitted Criteria
C1.1	Axway does not make commitments with respect to retention of customer data.