# AXWAY SOFTWARE SA

## INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT

FOR THE

SOFTWARE AS A SERVICE (SAAS) SERVICES

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

Attestation and Compliance Services

# 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 SaaS ("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 SaaS 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.

Schellman & 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") SaaS ("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 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 SAAS

## 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 Business 2 Business integration (B2Bi) and Managed File Transfer (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 new experiences, innovate new services, and reach new markets.

## Description of Services Provided

*Syncplicity*

Syncplicity by Axway, a content services platform (CSP), is a cloud-native with cloud-scale Software-as-a-Service (SaaS) solution. Content services provide customers the control and agility to address their enterprise business needs. With Syncplicity, customers can centralize, manage, and protect their files, data, and content. Customers can add intelligence and engage in file sharing with people, places or things using APIs, application integration, or Axway pre-built integrations.

Syncplicity by Axway provides a secure, enterprise-grade file synchronization, sharing and collaboration platform that enables enterprises to build a digital workplace that integrates with their digital business. Syncplicity allows enterprises to use a hybrid approach to content services – with on-premises, private and public cloud storage options. Syncplicity also offers an advanced layer of global content protection with maximum visibility and security controls. Enterprises who leverage Axway solutions can add Syncplicity to their portfolio;
Syncplicity is pre-integrated with Axway MFT, B2Bi, API and the Amplify Platform.

*Amplify*

Amplify is an API platform which allows customers to centralize control, enforce IT policy, and scale at will. Amplify allows a flexible model with services hosted in the cloud connecting to private cloud and on-premises installations, meeting the varied data storage needs of each customer.

Axway's API platform includes the following areas to allow customers to experience faster integration within the platforms to fit all their business needs.

- API Management: Build and manage APIs;
- Application Integration: Rapidly connect and integrate applications with integration Platform-as-a-Service (iPaaS); and
- Runtime Services: Ready-to-run container environment. Elastic scalability, performance, and Ease-of-use.

## 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, SaaS 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. 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 SaaS 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 SaaS services are hosted within Amazon Web Services (AWS) Elastic Compute Cloud (EC2), referred to as the hosting service hereafter in this document, and consist 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 the hosting service 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 single-tenant or multi-tenant architecture that applies common, consistent management practices for customers. 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. Production systems operate utilizing a combination of the Microsoft Windows and Linux operating systems. Networking components, load balancers, web servers, and database servers are deployed utilizing redundant configurations.

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

| Primary Infrastructure | | | |
|---|---|---|---|
| **Production Systems** | **Business Function Description** | **Platform** | **Physical Location** |
| Active Directory (AD) | AD domains are utilized to control access to the production networks. | Windows | AWS |
| VPN appliance | Access to the production environment requiring external users to authenticate using multiple factors to the production network. | Palo Alto GlobalProtect | |
| Firewalls | Protects the network perimeter and segregates network security zones. | Palo Alto and CheckPoint | |
| Hosting service security groups | Cloud hosting security groups within the 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 | Relational Database Service RDS) supporting the enterprise SaaS services. | MongoDB and MySQL | |
| Servers and Virtual Machines | Production servers and virtual machines supporting the enterprise SaaS services. | Windows and Linux | |
| Bastion Host | A jump server allowing access to other production instances. | Linux | |

The following software is utilized in support of the delivery of the SaaS system:

- Zabbix – enterprise monitoring software utilized to monitor the availability and capacity levels (e.g., central processing unit (CPU) usage, network latency, disk space, etc.) of the production servers and databases.
- Elasticsearch, Logstash, and Kibana (ELK) stack – log analysis solution configured to log and consolidate security and access related events on the network domain and production servers.
- GitHub – source code management software utilized to control code versioning and security throughout the code development process.
- Rapid7 InsightVM – security scanning software utilized to conduct vulnerability scans of the production environment.
- Jira – automated ticketing system utilized for centrally managing and tracking production issues and change management activities.
- ServiceNow – SaaS help desk solution used for incident/problem management.
- Symantec – antivirus software running on production servers and installed on workstations.

## 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 production 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 production 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 will then access the hosting service console which is configured with a unique username, password, and two-factor authentication configurations. Once authenticated, access is restricted based upon predefined role-based access groups. The ability to configure security groups, provision and maintain production servers and databases, and access individuals' hosts is restricted to predefined role-based access groups. IAM groups are also utilized within the hosting service console which is provisioned using predefined user groups.

Back-end access into the production servers requires users to be on the production network and log onto a Linux based bastion host via secure shell (SSH) public and private key credentials. Only authorized individuals within the bastion host have authorized credentials and can access the Linux based production servers.

Access to and within the hosting service 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 or designated delegate 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 after their termination date. IT personnel will remove any 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 quarterly 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*

Axway maintains documented policies and procedures to help guide personnel in the change management process for both application releases and infrastructure changes. On a weekly basis, IT and development personnel meet to discuss and prioritize application releases and infrastructure changes. Both application releases and infrastructure changes are documented within an automated ticketing system and changes are tested by quality assurance (QA) personnel and approved by IT management prior to implementation. The environments used for changes, such as development and test, are logically and physically segregated from the production environment. In the event changes need to be rolled back, the change management software retains a history of source code that can be rolled back to prior versions of the software if necessary. Application source code resides within version control software and access to the version control software is restricted to authorized personnel.

Development personnel perform independent code reviews for application releases and infrastructure changes to verify that newly developed code satisfies the requested objective and is developed according to secure coding guidelines. Independent code reviews are systemically enforced by the version control software to prevent the same individual who initiated the pull request from merging the same code to the master branch without an independent review. The QA team performs testing for application releases and infrastructure changes, and senior management gives approval prior to implementation. The ability to implement those application releases and infrastructure changes is limited to authorized personnel.

*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 backups 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.

*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 SaaS 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 utilizes various monitoring tools to capture significant events and conditions related to the services provided, including the monitoring of network and server performance, server and device availability, network utilization, server capacity, backup job execution, and job processing. The tools are configured to send automated alerts to operations personnel in the event that predefined thresholds are exceeded. Significant events or conditions are documented within an incident ticket, investigated, and tracked to resolution.

Axway personnel maintain, monitor, store, and make available data for customers. Customers are responsible for the data that is entered and stored within the application; it is assumed that their information is confidential unless otherwise stated by the customer. Customers remain the sole and exclusive owner of their sync files. Customers are responsible for accessing their own data, and Axway personnel do not generate reports for distribution to their customers.

**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. | CC6.1.1 - CC.6.1.3 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 SaaS 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 SaaS at Axway.

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