

# Axway Managed Cloud

---

## Axway Managed Cloud Description

---

September 5, 2024



## 1. OVERVIEW OF AXWAY MANAGED CLOUD.

**1.1. Introduction.** This Axway Managed Cloud Description is intended to set forth the components and features of the “Axway Managed Cloud” and the services that Axway provides in relation to the Axway Managed Cloud which are provided by Axway to Customer in accordance with the terms specified herein. Capitalized terms not otherwise defined herein are set forth in Exhibit A “Definitions” hereto.

**1.2. Axway Managed Cloud.** The “Axway Managed Cloud” refers to Axway’s deployment offering in which Axway provides subscription access to Axway software Products via an Axway provided single tenant virtual cloud Environment (“Single Tenant”) or multi-tenant public cloud Environment (“Multi-Tenant”), as specified in the Subscription Order Form.

**1.3. Axway Managed Cloud Stack.** The Axway Managed Cloud operates on four distinct “Implementation Layers” which collectively comprise what is referred to as the “Axway Managed Cloud Stack”. Different services are included and available for purchase for each Implementation Layer, those Implementation Layers are as follows:

- **Hosting Layer:** Layer consisting of the infrastructure and related technical elements (e.g., server, network, database, operating system, middleware).
- **Application Layer:** Layer where Products and Axway monitoring, supervision and security management tools are installed and running.
- **Solution Layer:** Layer consisting of specific technical and business configurations for the business and operational requirements of Customer.
- **Data Layer:** Layer consisting of managed data that is processed by the Axway Managed Cloud.

### 1.4. Axway Managed Cloud Stack Management Activities

- **Private SaaS.** For all Axway Managed Cloud subscriptions, Axway provides Customer’s solution as private SaaS (software-as-a-service) and manages the Run Activities of the Platform (consisting of the Hosting Layer and the Application Layer) while the Customer is responsible for the Solution Layer and Data Layer.
- **Managed Services.** If Managed Services are purchased by Customer, Axway manages the Run Activities of all four (4) layers of the Axway Managed Cloud Stack (Hosting Layer, Application Layer, Solution Layer, and Data Layer). All implementation and modification of Customer flows and other configurations on the Solution Layer of the Axway Managed Cloud **must** be performed by Axway, these activities are performed as BSR Services or as Professional Services (see Section 4) delivered on a project basis under a dedicated SOW and are provided at additional cost through the purchase of BSR Service hours/Service Unit Points.

**1.5. Axway and Customer Responsibilities.** The specific responsibilities of Axway and Customer in relation to the Axway Managed Cloud are summarized in Exhibit B, “Axway and Customer Responsibilities”.

**1.6. Exclusions.** For clarification and the avoidance of doubt, this Axway Managed Cloud Description does not govern or describe any other Axway Products or services (i.e., perpetually licensed products, “SaaS”, or “Customer Managed” subscriptions) other than the Axway Managed Cloud and related services thereto.

## 2. AXWAY MANAGED CLOUD PARAMETERS AND OPTIONS

**2.1. IaaS Hosting Partner.** The applicable Hosting Services Partner (HSP) for Customer’s Axway Managed Cloud subscription will be set forth in the Subscription Order Form. Additional information on Customer’s Hosting Services Partner in relation to the Axway Managed Cloud can be provided upon request. Axway reserves the right to change



hosting service providers from time to time upon advanced written notice to Customer, provided such change does not materially degrade Customer's Axway Managed Cloud subscription.

**2.2. HSP Data Centers.** Axway Managed Cloud offers several different HSP data center regions. If specified in the applicable Subscription Order Form, Customer's Environments will be configured in the specified HSP data center region ("Defined HSP Region"). In addition, if purchased by Customer, Axway may establish a Disaster Recovery Environment in a separate HSP region from the Defined HSP Region.

**2.3. Use and Usage Metrics.**

**2.3.1 Usage Metrics.** Customer is entitled to Production Environment use up to the applicable Usage Metrics set forth in the applicable Subscription Order Form. Usage Metrics are defined by the sum of usage across all Production Environments, therefore, purchasing additional Production Environments does not increase Customer's total Usage Metrics entitlement. Non-Production Environments may not be used for Production purposes, except in the event of a Disaster, the Disaster Recovery Environment may be used for Production purposes. In the event the Disaster Recovery Environment is used for Production purposes, usage in the Disaster Recovery Environment will be measured in the calculation of Usage Metrics.

**2.3.2 Excess Use.** If rates for Excess Use of a certain Usage Metric are specified in the applicable Subscription Order Form, Customer may exceed its entitlements for those Usage Metrics, subject to Customer's consent for Axway to monitor Customer's usage for those Usage Metrics and Customer agreeing to execute an additional order form and promptly pay any additional fees for any Excess Use ("Excess Use Fees"). Excess Use Fees will be charged at the applicable rates set forth in the applicable Subscription Order Form. Axway reserves the right to suspend Customer's Axway Managed Cloud service for failure to pay any Excess Use Fees. Failure to pay Excess Use Fees shall be deemed a material breach of the Agreement.

**2.3.3 Reporting.** Monthly reports will be made available for Customer access on the Axway Platform or may be provided directly to Customer upon request. Monthly reports include, but are not limited to, any Usage Metrics for which Excess Use Fees may be charged and the capacity provided to Customer.

**2.3.4 Increasing Usage Metrics.** If Customer wishes to increase its Usage Metrics, an additional Subscription Order Form may be entered into between the parties to increase Customer's entitlements. If Customer has purchased Managed Services, any purchase of increased Usage Metrics also requires Customer to also pay additional fees for Managed Services (up to the new level of Usage Metrics purchased).

**2.4 Environments.** The Environments described below are included or available to Customer as part of Customer's Axway Managed Cloud subscription unless otherwise set forth in the Subscription Order Form.

**2.4.1 Included Environments.** By default, the following Environments are included in an Axway Managed Cloud subscription (collectively, "Included Subscription Environments"):

- One (1) Production Environment in the Defined HSP Region
- Non-Production Environments
  - For SLA Level "Platinum" and "Gold", two (2) Non-Production Environments in the same Defined HSP Region as the Production Environment
  - For SLA level "Silver", one (1) Non-Production Environment in the same Defined HSP Region as the Production Environment

**2.4.2 Additional Environments.** In addition to the Included Subscription Environments, the following additional Environments may be purchased by Customer pursuant to a Subscription Order Form:

- Additional Production Environments
- Additional Non-Production Environments including Disaster Recovery Environments in a separate HSP region or Pre-Production Environments.



## 2.5. Environment Sizing

**2.5.1. Production Environments.** The following sizing and usage parameters shall be applicable to Customer's Production Environments:

- The sizing of Customer's primary Production Environment will be determined by Axway based on the Usage Metric entitlements of Customer's Axway Managed Cloud. The sizing of any additional Production Environments will be equivalent to the primary Production Environment.
- Excess Use by up to twenty percent (20%) is supported without any upsizing requirement or downtime, however, any additional Excess Use may require resizing of the Production Environment, which may require downtime and/or additional fees.
- The maximum supported peak processing load per hour for Production Environments is one percent (1%) of the contracted Usage Metrics per month. Peak processing greater than one percent (1%) in any hour may be achieved but is neither advised nor guaranteed.

**2.5.2. Non-Production Environments.** Non-Production Environments are provided as a single node deployment with a maximum processing capacity of no more than twenty percent (20%) of the applicable Usage Metrics.

**2.5.3. Pre-Production Environments.** Pre-Production Environments are sized equivalent to the Production Environments.

**2.5.4. Disaster Recovery Environments.** Disaster Recovery Environments are sized equivalent to the Production Environments.

## 2.6. Deployment Architectures.

**2.6.1. General.** The specific deployment architecture will be determined by Axway on a per customer and per Environment basis based on the applicable Usage Metrics, SLA Level, and other selected options and requirements of Customer's specific Axway Managed Cloud subscription. The deployment architecture may be modified from time to time by Axway.

**2.6.2. Deployment Architecture and SLAs.** For SLA Levels Platinum and Gold, the Axway Managed Cloud deployment will be distributed across at least two (2) "Availability Zones" within the Defined HSP Region to meet the Platform Availability SLA, however active data processing may, in Axway's discretion, be limited to a single Availability Zone at any given time. In addition, any redundant or replicated Environments may be deployed as needed to meet the Platform Availability SLA.

## 2.7. Customer Network Connectivity.

**2.7.1. Customer Network Connectivity Types.** Axway supports virtual private network (VPN) and available Customer Network Connectivity Types for the applicable HSP provider as the Customer Network Connectivity Type. Other Customer Network Connectivity Types may be mutually agreed between Axway and Customer at additional cost to Customer.

**2.7.2. Connection to Customer Network.** Connections to one or more Customer networks will be established by the Customer Network Connectivity Type. By default, unless otherwise agreed by the parties, Axway will establish one (1) redundant connection using VPN. Details regarding technical network connectivity may need to be provided and agreed upon between Axway and Customer before Customer's dedicated VPC is able to be provisioned by Axway.

## 2.8. Storage Encryption at Rest.

**2.8.1.** If possible given Customer's security constraints, Axway will encrypt the disk storage in the Hosting Layer using services offered by the HSP to perform encryption and will manage the keys which are stored securely at the HSP.



2.8.2. "Storage Encryption at Rest" is limited to coverage of Customer's virtual cloud Environment and the data stored on disks in the virtual cloud Environment and specifically does not include: (a) Environments external to the HSP or Axway, (b) the HSP network between the internet and the Axway virtual cloud Environment. Unless approved in writing by Axway, all data in motion must be restricted by Customer to secure protocols.

## 2.9. Security Services – Standard

2.9.1. **Security Services – Standard.** Includes the following security services for Customer's Environments hosted by Axway's Hosting Service Provider:

- **General Security.** Internal and external security protection and monitoring for Instances, storage types, networks and databases.
- **IAM (Identity Access Management).** Management of roles and access privileges for Customer users and Axway employees.
- **IDS (Intrusion Detection System) services.** System monitoring of network traffic for suspicious activity and policy breaching and alerts when such activity occurs.
- **Certificate Management services.** Deploying, updating, and monitoring expiring certificates.
- **DDOS (Distributed Denial of Service) protection.** Network equipment and protections designed to mitigate the effects of DDOS attacks.
- **Firewall rules services.** Limited solely to firewall rules established during initial implementation of Customer's Environments. After implementation in Production, any additional firewall rules are subject to additional fees.

2.10. **Other Optional/Selectable Entitlements.** If purchased by Customer as set forth in Customer's Subscription Order Form, Customer's entitlements may also include the following option(s):

2.10.1. **Application Log Forwarding (ALF) Service.** If purchased, Customer is entitled to forwarding of application log events.

- Limited solely to application log events from Customer's Production and Non-Production VPC Environments, specifically excludes any security log events.
- Axway will push application log events to Customer's repository. Customer is not permitted to pull the application log events from the Axway Managed Cloud.
- Axway will store application log events according to the retention period specified for each application which the Application Log Forwarding Service is applicable.
- Forwarding of application log events is limited solely to 100KBps.

2.10.2. **Anti-Virus Scanning.** If purchased, Customer's Environments provided by Axway hereunder will be scanned for viruses up to the number of Messages per Month specified in the Subscription Schedule. For clarification and the avoidance of doubt, Anti-Virus Scanning does not include Environments external to the Environments provided by Axway hereunder or the internet between the applicable hosting service provider and the Environments provided hereunder.

2.10.3. **Partner IP Address Whitelisting.** If purchased, Partner IP addresses provided by Customer will be configured specifically into the Customer Environment to allow incoming data connections originating only from those addresses. Customer is entitled to up to 950 addresses.

2.10.4. **Security Services – Advanced.** If purchased, Customer is entitled to the following additional security services for Customer's Environments hosted by Axway's hosting service provider ("HSP"):

- **CVSS (Common Vulnerability Scoring System) score.** Industry standard assessment of Customer's Environment for security vulnerabilities. Limited to high (score 7.0 – 8.9) and critical (score 9.0 – 10.0) severities only.

- **Monthly report on internal and external scanning.**

**2.10.5. Security Services – Premium.** If purchased, Customer is entitled to the following additional security services for Customer’s Environments hosted by Axway’s hosting service provider (“HSP”):

- **Reports provided on internal and external scanning monthly and upon request of Customer.**
- **CVSS score for all severities.**
- **Monthly operating system policy compliance report.** Report of scanning of operating system to ensure compliance with Center for Internet Security (“CIS”) hardening benchmarks.
- **Health report.** Historical trend analysis of security events in Customer’s Environment.
- **Threat detection services.** Monitoring and protection services for threats for Production Environments only, workloads, and data.
- **Quarterly security situational awareness reporting.** Overview report of threats and vulnerabilities. Includes security information and event management (SIEM) report from SIEM software that aggregates and analyzes activity across all Customer Environments and applies analytics to detect threats and discover trends.

**2.10.6. Penetration Testing Services.** Axway will perform the Penetration Testing Service Option specified on Customer’s Subscription Order Form on Customer’s Non-Production Environments, the “Penetration Testing Services Options” are as follows:

- **Network Testing Service (“NTS”).** Entitles Customer to the following:
  - Automated scanning of Non-Production Environment(s).
  - Testing of common external network security vulnerabilities in Customer’s Non-Production Environment(s).
  - Manual triage of identified vulnerabilities.
  - Detailed report.
  - Limited to up to two-hundred fifty (250) IP addresses and endpoints.
  - Customer may request one (1) NTS retest in writing no more than ninety (90) calendar days following the delivery of the initial detailed report.
- **Dynamic Application Security Testing (“DAST”).** Entitles Customer to the following:
  - All services identified for NTS.
  - In-depth testing which includes automated scanning and manual test cases to identify vulnerabilities pertaining to authentication and session management, access control and information leakage.
- **Comprehensive Penetration Test.** Entitles Customer to the following:
  - All services identified for NTS and DAST.
  - Testing performed to mimic a hacker who can use exploits on any open attack surface in Customer’s Environments to initiate an attack.
  - Testing on up to five (5) User Application Roles.
  - Testing on up to three (3) Business Application Logic Flows to assess business logic flaws, logic limits and application controls.

**2.11. Data Rejection.** Subject to agreement by Axway, Customer (or Axway on Customer’s request) may set up rules to block or reject certain exchanges (for example: quota violation, security rules, or anti-virus) (“Rejection Rules”). The rejection or blocking of an exchange on account of such Rejection Rule will not be treated as an error by Axway nor will Axway’s support team manage specific alerts or creation of tickets for the Rejection Rules. The rejection or blocking of the exchange will only be visible through the logs provided by Axway



Managed Cloud. If Customer requests information on these rejections or blockings, Axway may, subject to an additional fee, retrieve information and create specific alerts with respect to the Rejection Rule.

### 3. AXWAY MANAGED CLOUD MANAGEMENT.

#### 3.1. Platform Monitoring

**3.1.1. Automated Platform Monitoring.** Axway provides automated monitoring of the Axway Managed Cloud to monitor issues that may affect SLAs or have potential to affect the operation of the Axway Managed Cloud. Should an error occur, automated altering mechanisms will alert Axway to address them promptly. Axway regularly evaluates the automated monitoring process to enable continuous improvement of the automated monitoring employed.

**3.1.2. Manual Platform Monitoring.** Axway performs regular inspection of the Platform (including automated monitoring employed thereby) in accordance with operational checklists based on the Customer's Managed Services Level and Customer's Usage Metrics, and regularly updates such checklists upon changes to Customer's Axway Managed Cloud subscription or upon new releases of the underlying software. Any faults detected in the monitoring process will trigger a ticket in the incident management process.

#### 3.2. Maintenance and Upgrades

**3.2.1. General.** To maintain integrity of the Axway Managed Cloud, Axway performs regular maintenance for the following:

- **Production Environments.** Axway will perform regular maintenance on Customer's Production Environment(s) during Customer's Regular Maintenance Window. When possible, maintenance that requires downtime will be undertaken during the Regular Maintenance Window. Additional preventive maintenance will be scheduled with the Customer at least 2 weeks in advance. Production Environment maintenance is applied to Production Environments only after successful application on the corresponding Non-Production Environments.
- **Non-Production Environments.** Axway will perform maintenance on Customer's Non-Production Environment(s) during Customer's regular Non-Production maintenance window.
- **Hosting Layer Maintenance.** Axway performs maintenance on the Hosting Layer primarily to apply security updates to operating systems and Infrastructure management tools. All Hosting Layer maintenance will be performed during the Regular Maintenance Window.
- **Application Layer Maintenance.** Application Layer maintenance will be performed, on an as needed basis, if there is an identified application or security issue for which a fix is available. Patches and Service Packs may also be applied during the Regular Maintenance Window. For issues with an "Impact Classification" of "Critical", Axway and Customer will agree on a schedule for applying needed maintenance.
- **Security, Monitoring, and Complementary Tools.** Notwithstanding anything to the contrary, any products, tools, components, and/or agents that require continuous or regular updates may be updated at any time without notice (e.g., anti-virus software, anti-malware solutions, endpoint detection and response systems, monitoring systems, etc.). Such updates will not require system downtime or adversely affect the features, performance, accessibility, or user interface of the subscribed services.

#### 3.2.2. Application Layer Upgrades.

- The Application Layer of Axway Managed Cloud is implemented using the applicable Product for the Axway Managed Cloud subscription. A subscription to Axway Managed Cloud entitles Customers to



all “Supported” Versions, Updates, Service Packs, and Patches (as those terms are defined in Axway’s Product Life Cycle Policy) (collectively “Releases”) to the underlying Axway software product.

- Axway will use reasonable efforts to plan the implementation of any new Releases of the underlying Axway software product in the Application Layer pursuant to an agreed upon schedule between Axway and the Customer.
- For Production Environments, Axway will suggest multiple dates (at least 2 options) for implementing a new Release in the Production Environment. Upgrade of the Non-Production Environments will be performed on the agreed Production upgrade date.
- Axway will not implement a new Release without Customer approval, except in the case of new Versions or Updates during the last six (6) months before the end-of-support (EOS) date for the applicable Product, the Customer will be required to accept one of the suggested dates to implement the Version or Update. In this case, if Customer does not agree to implement the new Version or Update at one of the suggested dates before EOS date, any availability issue or incident caused by the failure to implement the new Version or Update will not be covered under the applicable SLAs.
- Axway will notify the Customer about end-of-support (EOS) deadlines for Releases of Axway Products affecting the Axway Managed Cloud, in a reasonable time after such dates are announced.
- For Customer’s who do not have Managed Services, Axway is not responsible (a) to conduct regression test following the maintenance or Upgrades (b) to guarantee the regression of Customer configuration or development.

**3.3. Backup and restore.** Axway and its hosting partner will perform all backup and restore actions for the Axway Managed Cloud. A backup plan will be developed during the initial setup of the Axway Managed Cloud. Axway Managed Cloud includes the following backup and restore features:

- Production and Non-Production Environments will be backed up daily.
- Daily backups of Production and Non-Production Environments will be maintained for seven (7) days.
- Weekly backups of Production and Non-Production Environments will be maintained for five (5) weeks.
- Monthly backups of Production Environments will be maintained for three (3) months.
- Restore Action is an Axway decision based on the instability or unavailability of the Product. Customer can request but cannot perform roll-back.

**3.4. Change Management.** Axway will perform a formal Change control procedure to Customer systems in Axway’s Managed Cloud. Goal of Change management is to process changes in the most efficient manner while minimizing business impact, costs, and risks. A change can be either a Standard Change or Emergency Change. Any Change will be monitored by a Change Manager and will have the approval of the Change Advisory Board. Change Management procedure consists of four phases: 1) Creation, 2) Approval, 3) Implementation, 4) Post-Implementation Review.

**3.5. Incident Management.** Incident is any event which is not part of standard operation of a service, and which causes, or may cause, an interruption to, or a reduction in, the quality of that service. Axway will perform Incident Management for quick restoration of Services as defined in the Customer contract.

**3.6. Application Runtime Data Retention and User Data Archiving.** Application runtime data is retained for specific durations depending on the applicable Products selected for Axway Managed Cloud. Options may be available for purchase to: (a) extend the default application runtime data retention period, and (b) provide User Data





Archiving. After any data retention or User Data Archiving period has expired the applicable data will be destroyed automatically.

- 3.7. Capacity Management.** Axway will track capacity across all Environments utilizing standard managed tools.
  - 3.7.1. General.** Increases to capacity will be made to Production Environments and be applied accordingly to Disaster Recovery and Pre-Production Environments.
  - 3.7.2. Storage.** If necessary Axway will increase storage capacity to meet the storage capacity requirements of Excess Use up to a maximum of 16 terabytes.
  - 3.7.3. Upsizing/Downsizing.**
    - 3.7.3.1.** Specific upsizing/downsizing phases may be agreed to by the parties in the applicable Subscription Order Form.
    - 3.7.3.2.** Upsizing/downsizing activities may require maintenance and downtime. Customer will be notified prior to any upsizing/downsizing activity resulting in a change to an applicable Axway usage tier. Any maintenance or downtime will be scheduled at a mutually agreeable time.
    - 3.7.3.3.** Upsizing requires an increase to the Subscription Fee (including fees for Managed Services if purchased) for the increased capacity but does not require additional fees to perform the upsizing.
    - 3.7.3.4.** Downsizing during the current Subscription Term requires a one-time fee and can only be performed and become effective when retained runtime data has been reduced to the corresponding smaller sizing (and related load). Runtime data will be purged from the Production Environment based on the contracted runtime data retention duration. Any upsizing or downsizing requests will be carried out at additional cost via a BSR Service Request.
  - 3.7.4. Availability Management.** Axway manages the Platform Availability in Axway Managed Cloud as described in this section.
    - 3.7.4.1. High Availability (HA), Failover, Recovery.** High Availability level is provided in accordance with the applicable SLA level purchased pursuant to the Subscription Order Form. For SLA Levels Platinum and Gold, the Axway Managed Cloud is distributed across at least two (2) HSP Availability Zones within the same HSP Region. Failover, recovery of services, and recovery of processing will happen automatically, this includes where one (1) whole HSP Availability Zone becomes unavailable.
    - 3.7.4.2. Outage within Primary HSP Region; Optional Separate HSP Region.** In the unlikely event of an outage of the Defined HSP Region, the recovery of Customer's Axway Managed Cloud will be performed, on a best effort basis, as soon as the required HSP services are available. As an available option of the Axway Managed Cloud, Customer may purchase 'DR Environment in Separate HSP Region', in which case Axway will provide a separate Disaster Recovery Environment in another HSP Region other than the Defined HSP Region to recover the Axway Managed Cloud and data processing independently of HSP restoring their services in the Defined HSP Region. This service is intended to be used only in the case of a major Disaster, where all utilized HSP Availability Zones in the primary HSP region are unavailable, and only if the Production Environment is unavailable and not recoverable within the disaster recovery objectives. If the 'DR Environment in Separate HSP Region' option is purchased, Customer and Axway will mutually agree on a disaster recovery plan. Such disaster recovery plan will be tested up to once per year at times mutually agreed by the parties, and additional tests may be available subject to additional fees.
- 3.7.5. Security Management**



- 3.7.5.1. Security Practices.** Axway maintains a strong security posture through administrative, technical, and physical measures, including providing security and vulnerability management at the Infrastructure and Product access level and monitoring of potential security issues, designed to protect the Axway Managed Cloud and Customer’s personal and confidential information from accidental loss and from unauthorized access, disclosure, use, alteration, and destruction. Axway’s security policies and procedures are further described in the Axway Corporate Security Statement, which may be provided upon request.
- 3.7.5.2. Audits and Certifications.** Axway’s IT security and processes are audited by independent third parties performing industry standard audits such as SSAE18, SOC2 and ISO 27001. Those audits encompass the overall Axway Managed Cloud as well as an examination of controls and evidence for customer Environments. Axway, holds the following certifications, which may be requested from Axway. Additional certifications are held by the HSP, information on the certifications held by the applicable HSP can be provided upon request. Axway’s current certifications and compliance certificates are available at: <https://www.axway.com/en/legal/contract-documents/slas-and-support>.
- 3.7.5.3. Security Evaluation.** Axway regularly evaluates applicable vendors and partners to ensure that they maintain the quality and certifications required to mitigate potential risks related to the security of the Axway Managed Cloud and its Environments.
- 3.7.5.4. Vulnerability Management.** As part of its Security Services (standard, advanced or premium) Axway performs regular vulnerability scanning of Environments. Vulnerabilities are treated as support requests and addressed according to SLA and priority in line with potential impact and urgency of the vulnerability (refer to 5.2 Classification of Support Requests). Vulnerabilities are addressed as per the following priorities:

<b>Category</b>	<b>CVSS v3 Base score</b>	<b>Priority of support request</b>
<b>Low</b>	0,0 - 3,9	<i>as required</i>
<b>Medium</b>	4,0 - 6,9	<i>as required</i>
<b>High</b>	7,0 – 8.9	<i>Priority 1</i>
<b>Critical</b>	9.0 -10	<i>Priority 1</i>

**3.7.5.5. Use of Unsecured Product Feature.** Axway will not provision an Environment that has not passed a security test and evaluation confirming that the Environment matches Axway’s security standards. The security test and evaluation ensures that the hardening guidelines have been applied and that the Environment is up to date with all security patches at the time of the test. However, for upward compatibility reasons, the Products provisioned in the Environment may be configured to support unsecured or deprecated network protocol (HTTP, FTP, SSLv1, v2, v3, TLS 1.1...), unsecured or deprecated cyphers, or operated in an unsecured manner (too short password length, anonymous login...). If, in Axway’s reasonable opinion, a change request on a standard provisioned configuration might significantly decrease the security level of the Environment and expose it to external attacks, approval from Customer’s senior security manager is required before being processed. Axway



reserves the right to reject change requests that would, in Axway's reasonable opinion, present a significant risk of attack or breach of the Environment.

### 3.8. Certificates of Service

- 3.8.1. **Default Certificate of Service.** As part of the Axway Managed Cloud subscription Axway will by default provide self-signed certificates of service.
- 3.8.2. **SSL Certificates.** If an SSL certificate from a certificate authority ("CA") is requested by Customer in writing, Axway shall, subject to an additional fee, provide one or more SSL certificates for the exclusive use of the Axway Managed Cloud.
- 3.8.3. **Renewal of Certificates.** Unless Customer provides ninety (90) days advanced written notice of its intent not to renew, certificates will be automatically renewed by Axway for each period of validity until the end of the applicable Axway Managed Cloud subscription.
- 3.8.4. **Customer Certificates.** If available, Customer can provide its own certificates, subject to an additional fee for the deployment of the Customer certificate. Customer is responsible (a) to inform Axway about the expiration of the Customer certificates and (b) to provide at least fifteen (30) days before the expiration date the new certificates.

## 4. ADDITIONAL SERVICES: BUSINESS SERVICE REQUESTS AND PROFESSIONAL SERVICES

### 4.1. Business Service Requests.

- 4.1.1. Customer may make Business Service Requests by purchasing a block of BSR Service Hours or Service Unit Points.
- 4.1.2. Upon receipt of a Business Service Request from Customer, Axway will coordinate with Customer for an agreed schedule for performance of the Business Service Requests. If multiple Business Service Requests are made by Customer at the same time, Axway will coordinate a delivery schedule with Customer based on priority of the BSRs.
- 4.1.3. BSR Services will generally be performed by Axway Monday through Friday from 8 a.m. to 5 p.m. at the physical location of the Axway entity for which Customer has contracted with, excluding bank holidays ("BSR Operation Hours").
- 4.1.4. Each BSR Service performed by Axway will be deducted from Customer's purchased Business Service Hours or Service Unit Points in accordance with the applicable number of BSR Service Hours or Service Unit Points assigned for the applicable BSR Service in the Service Catalog. Requests by Customers to perform BSR Services outside of BSR Operation Hours or by a certain date/time may be subject to increased hour or service business point usage.

- 4.2. **Professional Services.** For implementation, configuration, installation or larger or more complex services not available as a Business Service Request in the Service Catalog, Axway will perform such Professional Services pursuant to a mutually executed SOW.



**5. Service Level Agreements (SLA)**

**Platform Availability:**

Feature	SILVER	GOLD	PLATINUM
Platform Availability (1)(2)(4)	99.5%	99.9%	99.99%

**Ticket Service SLA (Incident support)**

Feature	SILVER		GOLD		PLATINUM	
Method to report tickets	Phone / Web / Email Priority 1 tickets must be reported by phone					
Support Availability	24 / 7					
Business Hours/day <sup>(3)</sup>	07h00 to 17h00 Monday to Friday		07h00 to 17h00 Monday to Friday		07h00 to 17h00 Monday to Friday	
Ticket Service SLA <sup>(2)(5)</sup>	MTTRespond	MTTRestore	MTTRespond	MTTRestore	MTTRespond	MTTRestore
Priority 1 – Critical	1 hour	1 business day	30 minutes	6 hours	15 minutes	4 hours
Priority 2 – Urgent	4 hours	2 business day	30 minutes	10 hours	15 minutes	8 hours
Priority 3 – Important	1 business day	6 business days	1 business day	3 business days	1 business day	2 business days
Priority 4 – Minor/Info	2 business days	10 business days	1 business day	6 business days	1 business day	5 business days

**With Addition of Optional Disaster Recovery (DR):**

DR in a separate HSP Region (when purchased) <sup>(4)</sup>			
RTO (Recovery Objective)	Time	24 hours	8 hours
RPO (Recovery Objective)	Point	12 hours	4 hours
			2 hours

(1) Platform Availability is applicable to Production Environments only.

(2) The SLAs are measured and calculated per calendar month. SLAs do not include the SLA Exclusions set forth below.

(3) Business hours/day are based on MST (US) or CET/CEST (EMEA) depending on the Axway entity for which Customer has contracted with. Customers in certain regions of the world have bank holidays. The Business hours/day time zone will be defined in the Subscription Order Form.

(4) DR in a separate HSP Region is available as optional paid service.

(5) Ticket Service SLAs are applicable for all four layers of the Axway Managed Cloud Stack and all Environments, however tickets for Non-Production Environments may only be classified as Priority 3 or Priority 4.



**5.1. SLA Levels and Summary.** Axway Managed Cloud has three available SLA Levels (Platinum, Gold, Silver) for the Axway Managed Cloud. However, SLA Level Silver and SLA Level Platinum are only available for certain Axway Managed Cloud offerings. The SLAs for each SLA Level are summarized in the table above. Axway will use commercially reasonable efforts to achieve the following service levels per SLA Level:

**5.2. Classifications of Support Requests.** Customer must submit to Axway a customer classification of any error in the Axway Managed Cloud by submitting the “Impact Classification” and “Urgency Classification” in accordance with the respective tables for each below. Once received, Axway, in its sole, reasonable discretion will classify the “Priority” of the error in accordance with the Priority table below:

**5.2.1. Impact Classification.** “Impact Classification” is determined by Axway based on the applicable categories specified below:

Impact classification	
<b>1 – critical</b>	<b>Faults that seriously impair or halt performance in Production Environment.</b> <ul style="list-style-type: none"> <li>System, server, or critical application down, AND</li> <li>The problem cannot be solved by a restart or a bypass or a workaround.</li> </ul>
<b>2 – high</b>	<b>Serious fault that affects productivity or development in Production Environment.</b> <ul style="list-style-type: none"> <li>Issue where Production is proceeding, but in a significantly impaired fashion.</li> <li>The Production Environment is running, but with repeated interruptions.</li> </ul>
<b>3 – medium</b>	<b>Moderate impact on production or non-production</b> Production Environment: <ul style="list-style-type: none"> <li>The Production Environment is running, but with limitations.</li> <li>A function in the Production Environment is failing, but there is a bypass available.</li> </ul> Non-Production Environment: <ul style="list-style-type: none"> <li>A function in the development system is failing, but there is a bypass available.</li> <li>Development project can proceed, but in a significantly impaired fashion.</li> <li>A workaround has been found but it is not acceptable.</li> </ul>
<b>4 – low</b>	<b>Minor faults which do not affect the use of the system or no impact</b>

**5.2.2. Urgency Classification.** “Urgency Classification” is determined by Axway based on the applicable categories specified below:

Urgency Classification	
<b>1 – high</b>	The restoration / resolution is immediately necessary to prevent severe business impact.
<b>2 – medium</b>	The resolution is needed as soon as possible because of potentially damaging service impact.
<b>3 – low</b>	The resolution will solve irritating problems or repair missing functionality but can be scheduled.



**5.2.3. Priority.** “Priority” is determined based on the applicable “Impact Classification” and “Urgency Classification” in accordance with the table below:

Priority based on Urgency Classification → And Impact Classification ↓	1 – High	2 – Medium	3 – Low
1 – Critical	Priority 1	Priority 2	Priority 3
2 – High	Priority 2	Priority 2	Priority 3
3 – Medium	Priority 3	Priority 3	Priority 4
4 – Low	Priority 3	Priority 4	Priority 4

**5.3. Service Quality Key Performance Indicators.** The tables below summarize the methodology for calculation of the service quality Key performance indicators (“KPIs”) as well as the frequencies of these indicators used by Axway for SLAs.

**5.3.1. Service Quality KPI Categories.** The KPIs are split into three categories (others may be available for an additional fee if the following do not meet Customer’s needs):

- “Key Incident Indicator”: indicator that evaluates the level of services provided in relation to incidents occurring on the Axway Managed Cloud
- “Key Service Indicator”: indicator that measures the performance of the Axway Managed Cloud
- “Key Informative and Performance Indicator”: other indicators that are used as complementary information to Key Incident Indicator and Key Service Indicator

**5.3.2. KPIs**

**5.3.2.1. MTTRespond**

Service Quality KPI Category	Key Incident Indicator
Data Required	<ul style="list-style-type: none"> <li>• Date and time of registration in the event management tool as “OPENED” status.</li> <li>• Date and time the status changes from “OPENED” to another status</li> </ul>
Data Source	Axway ITSM ticketing tools
Data Recording Methodology	Automatic
Measurement Period	Every calendar month
Key Definitions	<p>“Response Time” is the amount of time between automatic detection or reporting of the ticket and the time when the incident is no longer in “OPEN” status.</p> <p>“MTTRespond Target” is the maximum average mean Response Time per Priority to meet applicable SLA Level.</p> <p>“Average Response Time” is the sum of Response Time for all tickets associated to this priority divided by the number of tickets (as measured for tickets assigned the same priority and the same Measurement Period).</p>

Calculation	MTTRespond is measured by dividing the Average Response Time for a specific priority by the MTTRespond Target for the same priority during the Measurement Period.
SLA Achievement	The resulting percentage indicates whether Axway has fulfilled the MTTRespond SLA, as follows: A value equal to or below 100% indicates the MTTRespond SLA has been met.  A value over 100% indicates the MTTRespond SLA has not been met

### 5.3.2.2. MTTRestore

Service Quality KPI Category	
Service Quality KPI Category	Key Incident Indicator
Data Required	<ul style="list-style-type: none"> <li>• Date and time of registration in the event management tool as status OPENED.</li> <li>• Date and time of registration of change to status "AWAITING CUSTOMER FEEDBACK"</li> <li>• Date and time of registration changing status from "AWAITING CUSTOMER FEEDBACK" to another status.</li> <li>• Date and time of last "RESOLVED" status</li> </ul>
Data Source	Axway ITSM ticketing tools
Data Recording Methodology	Automatic
Measurement Period	Every calendar month
Key Definitions	<p>"Restore Service Time" is the amount of time between ticket creation and ticket resolution, less the time the ticket is in status "Awaiting Customer Feedback."</p> <p>"MTTRestore Target" is the maximum average mean Response Time per Priority to meet the applicable SLA Level.</p> <p>"Average Restore Time" is the sum of Response Time for all tickets associated to this priority divided by the number of tickets (assigned to the same priority and the same Measurement Period).</p>
Calculation	MTTRestore is measured by dividing the Average Restore Service Time for a specific priority by the MTTRestore Target for the same priority level during the Measurement Period.
SLA Achievement	The resulting percentage indicates whether Axway has achieved the MTTRestore SLA, as follows:  A value equal to or below 100% indicates the MTTRestore SLA has been met.  A value over 100% indicates the MTTRestore SLA has not been met

### 5.3.2.3. Platform Availability

Service Quality KPI Category	Key Service Indicator
Data Required	<ul style="list-style-type: none"> <li>• Date and time of registration in the event management tool as status OPENED.</li> <li>• Date and time of registration of change to status "AWAITING CUSTOMER FEEDBACK"</li> <li>• Date and time of registration changing status from "AWAITING CUSTOMER FEEDBACK" to another status.</li> <li>• Date and time of last "RESOLVED" status</li> </ul>
Data Source	Axway ITSM ticketing tools
Data Recording Methodology	Automatic
Measurement Period	Every calendar month
Key Definitions	<p>"Availability Duration" means the total duration that the Production Environment is not experiencing a Priority 1 classified outage of the Platform during the Measurement Period</p> <p>"Duration Period" means the total duration of the measurement period less scheduled maintenance time, as measured in minutes</p> <p>The durations of overlapping incident periods are not accumulated and are counted as a single duration.</p>
Calculation	Platform Availability means the Availability Duration divided by the Duration Period
SLA Achievement	<p>The resulting Platform Availability percentage indicates whether Axway has achieved the Platform Availability SLA, as follows:</p> <p>A percentage value equal to or over the applicable Platform Availability percentage for the SLA Level purchased indicates the Platform Availability SLA has been met.</p> <p>A percentage value less than the applicable Platform Availability percentage for the SLA Level purchased indicates the SLA has not been met.</p>

### 5.3.2.4. RTO – Recovery Time Objective (This only applies if DR has been purchased)

Service Quality KPI Category	Key Service Indicator
Data Required	<ul style="list-style-type: none"> <li>• Date and time of declaration of Disaster ("OPEN" status)</li> <li>• Date and time of registration of Axway Customer Information Request ("AWAITING CUSTOMER FEEDBACK"</li> </ul>



	<ul style="list-style-type: none"> <li>• Date and time of registration of the change of status "AWAITING CUSTOMER FEEDBACK" to another status following the provision of information by the customer.</li> <li>• Date and time of transition to "RESOLVED" status</li> </ul>
Data Source	Axway ITSM ticketing tools
Data Recording Methodology	Manual ticket entry recording of Disaster
Measurement Period	Only measured in Disaster Duration Period
Key Definitions	<p>"Disaster" means the complete unavailability of the Platform in Production and the datacenter is not available.</p> <p>"Disaster Duration Period" means the total time for which a Disaster is ongoing, as calculated by the time of resolution of the Disaster (by indicated by change to "Resolved" status) minus the time of creation of the Disaster ticket (as indicated by creation of "OPEN" ticket)</p>
Calculation	<p>RTO is equivalent to the Disaster Duration Period</p> <p>RTO means date of resolution of disaster incident minus date of creation of disaster incident</p>
SLA Achievement	<p>An RTO equal to or below the applicable RTO for the SLA Level purchased indicates the SLA has been met.</p> <p>An RTO greater than the applicable RTO for the SLA level indicates the SLA has not be met.</p>

**5.3.2.5. RPO – Recovery Point Objective** (Applies only if Customer is entitled to a Disaster Recovery Environment)

Service Quality KPI Category	
Service Quality KPI Category	Key Service Indicator
Data Required	<ul style="list-style-type: none"> <li>• Date and time of the creation of Disaster incident via status Opened.</li> <li>• Date and time of the last backup snapshot available before the Disaster</li> </ul>
Data Source	Axway ITSM ticketing tools
Data Recording Methodology	<p>Manual ticket entry recording of Disaster.</p> <p>Time stamp of last backup snapshot from Axway Managed Cloud</p>
Measurement Period	Only occurs at beginning of Disaster Duration Period
Key Definitions	<p>"Disaster" means the complete unavailability of the Platform in Production and the datacenter is not available.</p> <p>"Disaster Duration Period" means the total time for which a Disaster is ongoing, as calculated by the time of resolution of the Disaster (by marking as "Resolved") minus the time of creation of the Disaster ticket (as indicated by creation of "OPEN" ticket)</p>

	“Time Since Last Backup” means the total time difference between the time of creation of the Disaster ticket (as indicated by creation of “Open” ticket) and the time of the last time stamp of the backup of the system.
Calculation	RPO is equivalent to the Time Since Last Backup
SLA Achievement	An RPO equal to or below the applicable RPO for the SLA Level purchased indicates the SLA has been met.  An RPO greater than the applicable RPO for the SLA level indicates the SLA has not be met.

**5.4. SLA Exclusions.** Axway’s failure to meet any SLA will be excused (and not included in any SLA calculation) to the extent the failure is due to or arises from:

- Acts of God, exchange controls, export/import controls or other government restrictions, wars, hostilities, blockades, pandemic, civil disturbances, revolutions, strikes, terrorist attacks, lockouts, or any other cause beyond the reasonable control of a party (“Force Majeure”)
- The acts or omissions of the Customer or its agents, including, but not limited to:
  - Improper use of the Axway Managed Cloud by Customer or its partners
  - Usage in excess of the peak processing load per hour
  - Failure to provide reasonably necessary information for Axway to address incident.
  - Failure to perform tests reasonably requested by Axway.
  - Failure to perform functional validation before deployment to Production.
  - Failure to provide Axway access to Environment.
  - Incomplete or improper test cases defined by Customer and executed in Non-Production Environments
  - Modifications made to the Axway Managed Cloud by Customer (or a third party acting on behalf of Customer)
- Suspension or termination of the Axway Managed Cloud subscription.
- Axway Managed Cloud not functioning due to unavailability of Customer or Customer’s partner services, i.e.:
  - Lookup to Customer database or API or similar unavailable
  - Data transmission to Customer or Customer’s partner destination service or system unavailable.
- Use of a Solution Layer configuration prior to Solution Layer configuration being fully validated in Production Environment by Axway
- Blocking issues, system throttling, or other negative impacts caused by components or configurations developed, modified, or deployed by the Customer.
- Delays and other problems inherent to the operation of the Internet and electronic communications

**5.5. Errors Caused by Customer or Customer’s Partners.** If an incident or error in the Axway Managed Cloud arises from improper use by the Customer or Customer’s end users (or a third party working on behalf thereof), for example, network problems on the Customer’s side, configuration changes performed by the Customer, or poor data quality in Customer’s files, then, following Customer’s request, Axway will perform the work necessary to restore the Axway Managed Cloud subject to additional Professional Services fees.

**5.6. Service Credits**

**5.6.1. Applicable KPIs.** Notwithstanding anything to the contrary, Service Credits are provided for the following KPIs (as specified above): (a) Platform Availability (only for the Production Environment) and (b) MTTRestore Service (only for Priority 1 and Priority 2 tickets (collectively, “Service Credit KPIs”). For purposes of determining Service Credits, each Service Credit KPI is measured monthly. Service Credits only apply to Production Environments.

**5.6.2. Service Credit Calculation.** Customer’s Service Credits are determined by calculating the total number of monthly Service Credit Penalty Points for the applicable KPIs and assigning the applicable Service Credit Percentage as follows:

**5.6.2.1. Determination of Penalty Points.**

KPI	Service Credit Penalty Points
KPI1: Platform Availability	1 point for each 0.2% below 99.99% (PLATINUM) 1 point for each 0.2% below 99.9% (GOLD) 1 point for each 0.2% below 99.5% (SILVER)
KPI2: MTTRestore	2 points if MTTRestore is greater than 100% 4 points if MTTRestore is greater than 150% 6 points if MTTRestore is greater than 200%

**5.6.2.2. Service Credit Percentage.** The applicable Service Credit Percentage, as set forth below only relates to Subscription Fee for the month measured.

Number of Service Credit Penalty Points	Service Credit Percentage
0	0%
1-2	2%
3-4	4%
5-6	6%
7-10	8%
Over 10	10%

**5.6.3. Service Credit Limitations and Restrictions**

**5.6.3.1.** Notwithstanding anything to the contrary, Customer is only eligible for Service Credits if:

- \*Customer opens a support ticket within twenty-four (24) hours of an event affecting the Service Credit KPI
- \*\*Customer requests a Service Credit be applied in writing.

\* Axway will notify Customer via email of all Service Credit KPI impacting events.

\*\*Axway will investigate and validate the request and respond to Customer’s request within ten (10) business days. In the event Axway has a valid justification to oppose the request for Service Credit, Axway shall respond and communicate such justification, with related evidence, to the Customer within ten (10) business days from the request date.



- 5.6.3.2. Notwithstanding anything to the contrary, Customer's Service Credits shall be capped at a total of five percent (5%) of the Subscription Fees over the prior four (4) quarters of the Subscription Term.
- 5.6.3.3. Service Credits may only be applied to future invoices of Customer's Subscription Fees for the Axway Managed Cloud for which the Service Credits originated, Axway will not issue refunds.
- 5.6.3.4. Service Credits may not be applied to any other account.
- 5.6.3.5. Service Credits are Customer's only remedy for interruptions of use to the Axway Managed Cloud, Axway is not responsible for any direct or indirect damages caused by service interruptions.

## 6. AXWAY MANAGED CLOUD SUPPORT ORGANIZATION DETAILS.

- 6.1. **Support Organization.** Axway Managed Cloud offers a 24x7 global organization utilizing IT Service Management (ITSM) best practices, with support centers around the world and local support representatives in different regions offering phone, email, and web support.
  - 6.1.1. Axway Managed Cloud Support: Support for the Axway Managed Cloud focuses on problem management versus simple incident management. Problem management seeks to identify and solve the root cause of the problem to resolve not only the current incident but prevent future similar incidents. Problem management determines the necessary corrective action such as the application of a patch, service pack, etc. The problem is closed when the recommended corrective action has been completed.
  - 6.1.2. Support "Level 0". Support calls are initially routed to Axway's global support center, where the call is prioritized and routed to "Level 1". Phone numbers for the helpdesk can be found at: <https://support.axway.com/en/auth/contacts> . Customers may also submit incident and request tickets via e-mail or the Axway web portal.
  - 6.1.3. Support "Level 1". Level 1 is responsible for ongoing monitoring of all Production Environments and proactively addressing all alerts and incoming support tickets. For routine responses, Level 1 addresses and resolves the ticket. If the ticket requires greater involvement Level 1 will identify the appropriate Level 2 team and hand-off the ticket.
  - 6.1.4. Support "Level 2". If the incident cannot be resolved by Level 1, Level 2 identifies the source of the error and implements the necessary actions to correct in accordance with the SLA Level purchased. Level 2 will engage or escalate to Level 3 when additional expertise is necessary.
  - 6.1.5. Support "Level 3": If an incident cannot be resolved by Level 2, it is escalated to Level 3 where the ticket is addressed by solution expert teams within Axway. Level 3 includes experts in administration, tuning, design, architecture, and hosting of the solution. Level 3 is responsible for coordinating with third party HSP providers on behalf of Customer. In all cases, Support will provide regular and timely updates to the Customer.

## 7. CUSTOMER SUCCESS ORGANIZATION

- 7.1. **Customer Success Manager.** Axway Managed Cloud customers may be assigned an Axway Customer Success Manager ("CSM") who will be responsible for managing the overall Customer relationship, including acting as the primary point of contact for Customer. The CSM will strategize with Customer to successfully achieve their desired business outcomes by: (a) overseeing and ensuring the applicable Axway resources carry out smooth provisioning and onboarding; (b) monitoring SLAs and providing the appropriate standard and detail reports for trend analysis and forecasting; and (c) scheduling recurring business reviews and ad hoc meetings to track progress and KPIs found in the mutually agreed success plan.



## **EXHIBIT A**

### **DEFINITIONS**

**As used in this Axway Managed Cloud Description, the following terms shall have the following meanings:**

1. **"Business Service Request"** or **"BSR"** means a request by Customer for Axway to perform BSR Services for Customer's Axway Managed Cloud.
2. **"BSR Services"** means standard service items for the Axway Managed Cloud as set forth solely in the applicable Axway Service Catalog.
3. **"BSR Service Hours"** means the applicable number of hours assigned to certain BSR Services, as set forth in the applicable Axway Service Catalog.
4. **"Customer"** means the entity for which Axway has agreed to provide Axway Managed Cloud pursuant to a Subscription Order Form between the parties.
5. **"Change"** means the addition, modification or removal of anything that could have an effect on Subscription Services. The scope should include all Subscription Services, configuration items, processes, documentation, etc.
6. **"Change Advisory Board (CAB)"** means a group of people who advises the Change manager in the assessment, prioritization, and scheduling of Changes. This board is made up of representatives from all areas within the Axway Managed Cloud Service.
7. **"Customer Network Connectivity Type"** means the type of connection between the Customer's Axway Managed Cloud and customer's backend data center, as specified in the Subscription Order Form.
8. **"Disaster"** means the complete unavailability of the Platform in Production and the datacenter is not available.
9. **"Disaster Recovery Environment"** means an inactive Environment which is used for Production in the event of a Disaster when the Production Environment fails.
10. **"Emergency Change"** means a Change that is introduced as soon as possible in order to reduce or avoid adverse impact on the business. Risk and impact analysis are mandatory. It is directly linked to an existing Incident (or problem).
11. **"Environment"** means the combination of one or more systems and software that is directly connected with each other to form and provide a specific service in the Axway Managed Cloud.
12. **"Excess Use"** means use in excess of the applicable Usage Metrics.
13. **"High Availability"** or **"HA"** means the characteristic of a system which aims to ensure an agreed level of operational performance, usually uptime, for a higher-than-normal period.
14. **"Hosting Services Partner"** or **"HSP"** means the third-party partner utilized by Axway as a provider of hosting services for the Axway Managed Cloud, as set forth in the applicable Subscription Order Form.
15. **"Incident"** means any event which is not part of standard operation of a service, and which causes, or may cause, an interruption to, or a reduction in, the quality of that service.
16. **"Infrastructure"** means the HSP virtual cloud Environment and all resources thereto, including operating system, databases, storage, network, network services (like DNS, NTP), load balancing, firewalls, access controls and connections to the Internet and the Customer network like VPN or MPLS (where applicable).
17. **"Instance"** means software running in one (1) computer system as a single occurrence in RAM (Random Access Memory).
18. **"Managed Services"** means the value-added services provided by Axway for the Run Activities of the Axway Managed Cloud.
19. **"Non-Production Environment"** means an Environment used for processing data for other purposes than Production processing, for example, development, test, UAT, QA, and integration testing.
20. **"Patches"** shall have the meaning as set forth in Axway's "Product Life Cycle Policy".
21. **"Platform"** means collectively the Hosting Layer and Application Layer of the Axway Managed Cloud.
22. **"Platform Availability"** means the Platform is available for use by Customer.
23. **"Pre-Production Environment"** means a specific Non-Production Environment with sizing and architecture equivalent to the Production Environment on a single availability zone. Pre-Production Environments are typically used for Production equivalent simulation and testing, esp. for performance and load testing.
24. **"Production"** means use to perform and support the actual business processes of the Customer.



25. **"Production Environment"** means an Environment used to perform Production processing. Production Environments are typically connected to Production Instances of other software and/or external business partners, for business data exchange.
26. **"Products"** means the underlying software products to which Axway permits access to in the Axway Managed Cloud, as specified in the Subscription Order Form.
27. **"Professional Services"** means installation, implementation, configuration, consulting or other services or training delivered by Axway to Customer pursuant to a mutually executed statement of work.
28. **"Regular Maintenance Window"** means a regularly scheduled maintenance period of at least four (4) hours per month agreed upon by Axway and Customer prior to Production go live.
29. **"Run Activities"** refers to the runtime operational activities for the Axway Managed Cloud, including but not limited to monitoring, operations, incident management and notification.
30. **"Service Catalog"** means the Axway standard service catalog (by applicable Product) setting forth certain standard Business Service Requests for the Axway Managed Cloud and the applicable BSR hours or Service Unit Points associated with performing such service.
31. **"Service Credits"** means the eligible credit that is available to Customer for Axway missing an applicable KPI.
32. **"Service Packs"** shall have the meaning as set forth in Axway's "Product Life Cycle Policy".
33. **"Service Unit Points"** means the applicable point value assigned to certain BSR Services, as set forth in the applicable Axway Service Catalog.
34. **"SLAs"** means the specific service level agreements provided for the Axway Managed Cloud.
35. **"SLA Level"** means the applicable service level agreement levels for Axway Managed Cloud (Platinum, Gold, or Silver), as set forth in the applicable Subscription Order Form.
36. **"Standard Change"** means a pre-approved Change that is low risk, relatively common and follows a written/shared/known procedure (or work instruction).
37. **"Subscription Fees"** means the subscription fees for Customer's Axway Managed Cloud subscription, as set forth in the Subscription Order Form, Subscription Fees include Subscription Services fees but specifically exclude Professional Services fees.
38. **"Subscription Order Form"** means Axway's standard subscription order form (or other similar document duly executed by the Parties) which specifies Customer's Axway Managed Cloud subscription and the fees therefor.
39. **"Subscription Services"** means collectively, in context of the Axway Managed Cloud description, the subscription to Axway Managed Cloud and Managed Services.
40. **"Subscription Term"** means the period identified in the applicable Subscription Order Form during which Axway is required to provide Customer with the purchased Subscription Services.
41. **"Snapshot"** means incremental backups, where only the blocks on the device that have changed after the previous snapshot will be saved.
42. **"Upgrades"** shall have the meaning as set forth in Axway's "Product Life Cycle Policy".
43. **"Usage Metrics"** means the quantitative limitations and units of measure, along with any other grants of or restrictions on use, applicable to the Customer's Subscription Services, as set forth in the applicable Subscription Order Form.
44. **"Versions"** shall have the meaning as set forth in Axway's "Product Life Cycle Policy".



## EXHIBIT B

### AXWAY AND CUSTOMER RESPONSIBILITIES

The below tables are provided to summarize Axway and Customer's respective responsibilities for both Run Activities and BSR Services. The parties' respective responsibilities are indicated according to the following legend:

Axway = responsibility is with Axway
Customer = responsibility is with Customer
Axway/Customer = responsibility is shared between Axway and Customer

#### Setup and Access Control

	Private SaaS	Managed Services
Setup of connectivity between Infrastructure and Customer network (e.g. VPN)	Axway/Customer	Axway/Customer
HSP Infrastructure and HSP console access	Axway	Axway
Direct access to systems (OS shell), file systems, database (SQL) of HSP resources	Axway	Axway
Administration user interface access	Axway	Axway
*Configuration user interface access	Axway/Customer	Axway
*Monitoring user interface access	Axway/Customer	Axway/Customer

\*Upon prior approval from Axway, Axway will permit Customer to access user interfaces for configuration and monitoring of the Axway Managed Cloud.

#### Run Activities

	Private SaaS	Managed Services
<b>Hosting Layer</b>		
Infrastructure provisioning	Axway	Axway
Infrastructure operations	Axway	Axway
Infrastructure monitoring and incident resolution	Axway	Axway
Infrastructure support	Axway	Axway
Data backup (snapshots) and restore	Axway	Axway
Infrastructure failover and DR management (as per SLA level and subscribed DR options)	Axway	Axway
Infrastructure maintenance, including OS and other security patching (monthly and on-demand)	Axway	Axway
Infrastructure capacity management	Axway	Axway
<b>Application Layer</b>		
Product deployment	Axway	Axway
Product configuration	Axway	Axway
Product operations (e.g. start/stop)	Axway	Axway
Product monitoring and incident resolution	Axway	Axway



	Private SaaS	Managed Services
Product support	Axway	Axway
Product failover and DR management	Axway	Axway
Product Patches and Service Packs	Axway	Axway
*Product Upgrades (installation and validation on Application Layer) *Customer specific customizations may require a separate statement of work. Customer must validate the flows after the upgrade is complete	Axway/Customer	Axway/Customer
<b>Data and Solution Layers</b>		
24/7 monitoring and alerting of data flow processing	Customer	Axway
Data flow processing incident management  (Includes incident analysis, re-process or re-send of failed messages due to Infrastructure or connection issues (e.g., failed to send because of temporary unavailability of receiver, and other resolutions))	Customer	Axway
Analyze and resolve inquiries from Customer solution administrators	Customer	Axway
Direct interaction with external third-party partners of the Customer	Customer	Customer
Apply configuration changes and deploy configuration artifacts (if applicable)	Customer	Axway (performed as BSR Services in accordance with Service Catalog)
Deploy configuration artifacts directly into file system of Axway Managed Cloud Environment (Only applicable if deployment action is within supported boundaries of Product)	Axway	Axway
Enable/disable configuration items	Customer	Axway
Reporting and gathering statistics	Axway/Customer	Axway
Customer testing support	Customer	Axway





**BSR Services (as listed solely in applicable Axway Service Catalog):** When purchasing BSRs, the following responsibilities shall apply in order for Axway to perform the BSRs.

	Private SaaS	Managed Services
<b>Description</b>		
Direct contact with external partners of Customer (e.g., for Partner onboarding for B2Bi)	Customer	Customer
Provide functional specifications for data flows	Customer	Customer
Development of data flows and required artifacts	Customer	Axway
Configuration of data flows within user interfaces	Customer	Axway
Unit testing of data flows and all configuration objects	Customer	Axway
Versioning of all configuration objects	Customer	Axway
Creating detailed description for deployment of configuration objects	Customer	Axway
Validation of deployment description and related configuration objects	Customer	Axway
Deployment of configuration objects – within user interfaces provided by product	Customer	Axway