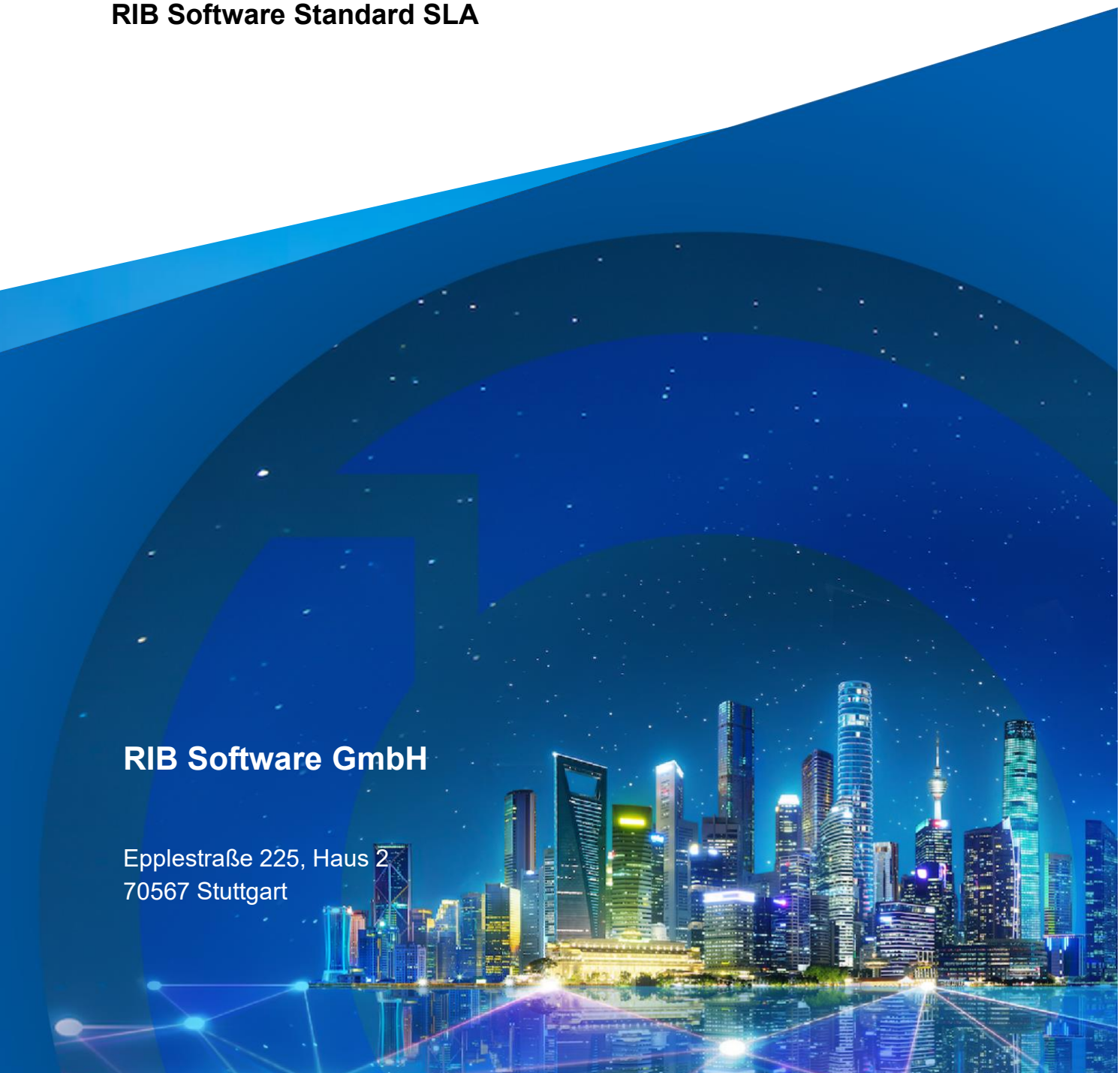
Service Level Agreement

RIB Software Standard SLA



RIB Software GmbH

Epplestraße 225, Haus 2
70567 Stuttgart

Copyright © 2025 by RIB Software GmbH

This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise.

© RIB Software GmbH. All Rights Reserved

Contents

Service Level Agreement 0

1. Definitions 3
2. Introduction 7
   - 2.1. Interpretation 7
   - 2.2. Scope 7
   - 2.3. Versioning 9
   - 2.4. Customer Support Centres 9
   - 2.5. Support Contacts 9
3. Key Requirements 10
4. Hosting Support & Maintenance Service 11
   - 4.1. Incident Priority Definitions 11
   - 4.2. Response Times 11
   - 4.3. Service Hours 12
   - 4.4. Change Requests 12
   - 4.5. Availability Targets 13
   - 4.6. Maintenance 14
   - 4.7. Data Protection 14
   - 4.8. Availability and Disaster Recovery 15
   - 4.9. Monitoring 16
   - 4.10. Security & Vulnerability Management 16
5. Application Support & Maintenance Services 18
   - 5.1. Incident Priority Definitions 18
   - 5.2. Incident Priority Validation 19
   - 5.3. Response Time 19
   - 5.4. Service Hours 20
   - 5.5. Suggestion Requests 20
6. General Support and Maintenance Terms 21
   - 6.1. Levels of Support 21
   - 6.2. Submitting Incidents 21
   - 6.3. Resolution or Closure of Incidents 22
   - 6.4. Release Management 23
   - 6.5. Escalation 23
   - 6.6. Disclaimers 24

1. Definitions

Any term used in this Service Level Agreement (hereinafter “SLA”) that is capitalised and not otherwise defined herein shall have the meaning ascribed to it in the RIB General Terms and Conditions.

1.1. "**Application**” means the software application developed by RIB and provided to the Customer by RIB or through a RIB Service Partner, together with any associated database structures and queries, user interfaces, system interfaces, tools, and similar components, and any and all revisions, modifications, and updates thereof delivered or made available to the Customer by RIB or through a RIB Service Partner pursuant to the Agreement.

1.2. “**Availability**” means the total number of minutes during a calendar month in which both the Cloud Platform and the Application are accessible to the Customer in the context of RIB Hosted or RIB SaaS deployment models. This definition does not apply to Self-Hosted environments. Excused Outages are excluded from the calculation of Availability. For the purpose of determining whether RIB meets its Availability Target for a given month, the percentage shall be calculated as described in Clause 4.5.4 of this SLA.

1.3. “**Cloud Platform**” means the cloud computing infrastructure used by RIB for hosting the Application in the context of RIB Hosted or RIB SaaS deployment models, as defined in the applicable Product Annexure. This typically includes third-party Cloud Platform Provider operated via provider-managed data centres. This definition shall not apply to Self-Hosted environments.

1.4. "**Cloud Platform Consumption Fee**” means the total monthly usage charges incurred by RIB for the Application’s operation on the Cloud Platform under the RIB Hosted deployment model only, as further specified in the applicable Product Annexure. Such charges include the usage of products and/or services sourced through the Cloud Platform Provider, plus any applicable handling fees. This fee does not apply to RIB SaaS or Self-Hosted deployments.

1.5. **“Cloud Platform Provider”** means a third-party service provider that supplies the underlying cloud infrastructure on which the Application is hosted and operated. This includes, but is not limited to, providers offering computing, storage, networking, and other related platform services necessary for the operation of the Application (e.g., Microsoft Azure). The Cloud Platform Provider shall be responsible for maintaining the availability, performance, and security of its infrastructure, while RIB shall remain responsible for the deployment, configuration, management, and support of the Application and Services running on such infrastructure in accordance with this Agreement.

1.6. “**Commercially Released Version**” means the most recent version of the Application that has been formally released and made available by RIB for general commercial use under RIB Hosted and Self-Hosted deployment models. This includes any of the following, as defined by RIB’s versioning conventions:

(a) Major Releases: Releases that may include architectural or structural changes, new features, or significant enhancements to the Application, typically designated by a change in the leading version number (e.g., V25.0 following V24.3).

(b) Minor Releases: Releases that introduce feature updates, improvements, or non-breaking changes, typically indicated by the first decimal point (e.g., V24.3.1 following V24.3).

(c) Updates: Patches, bug fixes, or incremental improvements to an existing Major or Minor Release, typically designated by additional characters (e.g., V24.3.1.A or similar).

This definition shall not apply to RIB SaaS deployments, where new functionality, fixes, and improvements may be deployed continuously or through managed release cycles as determined by RIB. Details regarding RIB SaaS products shall be outlined in the applicable Product Annexure.

1.7. "**Customer Support Centre**" means either: (I) the RIB or RIB Service Partner In-Region Customer Support Centre located in the Customer's country or the closest country to the Customer's where RIB or RIB Service Partner maintains an office with Application support capabilities; or (ii) the Global Customer Support Centre, which bears overall responsibility for supporting the Application and Cloud Platform.

1.8. "**Customer Contact(s)**" means the qualified named individuals(s) within the Customer's organisation who acts as authorised user(s) of the Application.

1.9. "**Customer Systems**" means the Customer's own computer networks or infrastructures (including but not limited to those using operating technology ("OT") or internet of things technology ("IoT"), platforms, information technology systems, tangible or virtual machines, software, application programs and data, whether or not related to its Production Environment, on which Customer runs the Application or which Customer uses, monitors, controls or helps to secure the Application.

1.10. "**Cyber Threat**" means any circumstance or event that has the potential to adversely impact, compromise, damage, or disrupt the Application, Cloud Platform (where applicable under RIB Hosted or RIB SaaS), RIB Systems, or Customer Systems; or that may result in unauthorized access, acquisition, loss, misuse, destruction, disclosure, and/or modification of data. This includes, but is not limited to, threats arising from malware, ransomware, hacking, denial-of-service attacks, or similar malicious activities, regardless of hosting model.

1.11. "**Defect**" any error, bug or failure of the Application, when operated in accordance with the Documentation, to provide the functionalities specified in the Documentation or to perform in full conformity with the applicable Functional Specifications.

1.12. "**Documentation**" means the online documentation and any other materials that describe the functions of the Application and, where applicable, the procedures or instructions relating to its use. In each case, such documentation and materials shall be in the formats and versions as exclusively determined by RIB for release.

1.13. "**Downtime**" means the total number of minutes in any calendar month during which the Application is inaccessible or otherwise unavailable to the Customer under the RIB Hosted or RIB SaaS deployment models, provided that such inaccessibility or unavailability is solely caused by: (i) a Defect in the Application; (ii) unavailability of the Cloud Platform; or (iii) other factors within RIB's reasonable control. This definition shall not apply to Self-Hosted environments. Downtime specifically excludes periods classified as Emergency Downtime, Scheduled Downtime, or General Unavailability.

1.14. "**Emergency Downtime**" means those times when RIB or Cloud Platform Provider becomes aware of a vulnerability of the Cloud Platform or its hosting infrastructure that RIB or Cloud Platform Provider deems to require prompt remediation and, as a result, the Application and Cloud Platform is temporarily made unavailable for remediation of such vulnerability. Emergency Downtime shall apply solely to RIB Hosted and RIB SaaS environments.

1.15. "**Excused Outage**" means unavailability: (i) occurring during Emergency Downtime, Scheduled Downtime and/or General Unavailability; or (ii) caused by or resulting from negligent acts or omissions or willful misconduct, of the Customer, its Affiliates, their respective employees, contractors, or agents, or any other party that gains access to the Application due to any such negligent act or omission or willful misconduct; or (iii) arising from the Customer's instruction or direction to RIB that RIB cease making the Application available to the Customer; or (d) occurring during a Force Majeure Event. This definition shall apply solely to RIB Hosted and RIB SaaS deployments.

1.16. "**Force Majeure**" means any event reasonably beyond the direct control of RIB and not due to RIB's own fault or negligence or that of its contractors or representatives or other persons acting on its behalf, and which could not have been prevented through commercially reasonable measures, including but not limited to Acts of God, acts of terrorists or criminals, acts of domestic or foreign governments, change in any law or regulation, fires, floods, explosions, epidemics, disruptions in communications, power, or other utilities, strikes or other labour problems, riots, or unavailability of supplies.

1.17. "**Functional Specifications**" means the descriptions of features and functions of the Application as expressly set forth in the online documentation.

1.18. "**General Unavailability**" means any period during which the Application is inaccessible due to network outages, infrastructure outages, unavailability caused by a third party not under RIB's control, or issues related to the Customer's own hardware or software. This includes unavailability resulting from acts or omissions of the Customer, its employees, subcontractors, or agents, as well as failures or lack of availability of third-party cloud services upon which the Cloud Platform depends. This definition shall apply solely to RIB Hosted and RIB SaaS deployment models.

1.19. "**Incident**" means each individual Defect in the Application reported to RIB's Customer Support Centre by a Customer Contact, or any individual cause of unavailability or inaccessibility of the Cloud Platform under RIB Hosted or RIB SaaS deployment models. For Self-Hosted environments, an Incident refers shall refer solely to Application-related Defects reported to RIB.

1.20. **"Key Users"** means selected individuals or representatives of the Customer who are entitled to report Incidents and service requests to RIB or RIB Service Partner.

1.21. **"Non-Production Environment**" means any environment that is designated by the Customer and has been confirmed to RIB as a trial, pre-production, staging, or test environment in which the Customer intends to use the Application for purposes such as testing, evaluation, training, or development. Where applicable, this includes environments hosted on the Cloud Platform under RIB Hosted or RIB SaaS models.

1.22. **"Product Annexure"** means the annexure attached to this SLA, which specifies the product-specific terms and conditions, support details, hosting models (e.g., RIB Hosted, RIB SaaS, or Self-Hosted), service levels, exclusions, and other relevant provisions applicable to the particular Application. **Each Product Annexure shall form an integral part of this SLA and takes precedence over the general clauses of this SLA to the extent that it contains more specific terms than such general clauses.**

1.23. "**Production Environment**" means the environment that is designated by the Customer and has been confirmed to RIB as the environment in which the Customer uses the Application in the ordinary course of its business. For RIB Hosted and RIB SaaS models, the Production Environment refers specifically to the environment the Customer uses the Application in, to perform their ordinary course of business, which is hosted on the Cloud Platform. For Self-Hosted deployments, it refers specifically to the Customer's own production environment. Non-Production Environments are expressly excluded from the definition of Production Environment.

1.24. **"RIB Hosted"** means a deployment model where the Application is hosted and operated by RIB on a managed Cloud Platform that is provisioned and controlled by RIB. RIB shall be responsible for managing the hosting infrastructure, platform maintenance, and associated cloud consumption. The Customer accesses the Application remotely and does not have direct control over the hosting infrastructure.

1.25. **"RIB SaaS"** means a software-as-a-service (SaaS) deployment model where the Application is delivered by RIB as a fully managed and continuously updated cloud-based service. RIB shall be responsible for all aspects of Application hosting, deployment, maintenance, updates, and infrastructure. The Customer shall consume the Application solely as a service, with no access to or control over the underlying platform or deployment configuration.

1.26. "**RIB Service Partner**" means any reseller authorized by RIB that provides services to the Customer under a separate agreement to be entered into between the Customer and the RIB Service Partner.

1.27. **"Self-Hosted"** means a deployment model where the Customer installs, hosts, and operates the Application on its own infrastructure or infrastructure that is procured and managed independently of RIB. The Customer shall be solely responsible for all infrastructure, security, hosting, and maintenance activities, whereas RIB shall provide support for the Application itself as specified in this SLA.

1.28. "**Scheduled Downtime**" means the period of time during which the Application is intentionally made unavailable due to scheduled deployments, updates, or maintenance activities performed by RIB or its cloud service provider. This includes maintenance of the Application, the Cloud Platform, or the underlying cloud infrastructure. Scheduled Downtime shall apply solely to RIB Hosted and RIB SaaS deployment models and shall not apply to Self-Hosted environments, where the Customer shall be responsible for scheduling its own maintenance.

1.29. "**Scheduled Maintenance**" means the maintenance performed by RIB in accordance with Clause 4.6.2 of this SLA.

1.30. "**RIB Support Portal**" means the web-based platform designated by RIB for use by the Customer to submit Incidents and service requests, and by RIB or its authorized Service Partners to manage and respond to such requests. The RIB Support Portal is accessible at: https://support.rib-software.com

1.31. "**Unavailability**" means that either the Cloud Platform or the Application, or both, are not Available under the RIB Hosted or RIB SaaS deployment models. This definition shall not apply to Self-Hosted environments.

2. Introduction

2.1. Interpretation

2.1.1. This SLA defines the levels of support and maintenance services that RIB agrees to provide in connection with the Application and its respective hosting model (e.g., RIB Hosted, RIB SaaS, or Self-Hosted) to any Customer that purchases a license or subscription to the software solution from RIB or any of its Affiliates.

2.1.2. This SLA contains general clauses applicable to all RIB products and hosting models. Specific terms, inclusions, and exclusions applicable to each product and hosting model shall be detailed in the annexures attached hereto.

2.2. Scope

2.2.1. What support & maintenance services are included?
Subject to timely payment by the Customer of the amounts invoiced for support and maintenance in accordance with the Order Form and/or RIB General Terms and Conditions, RIB or a RIB Service Partner shall provide the Customer with the following services for the Application and, where applicable, the associated hosting infrastructure:

For RIB Hosted and RIB SaaS customers:

a) First, Second, and Third Level support of the Application to the Customer's Key Users, either via RIB or a RIB Service Partner;

b) Second and Third Level support of the cloud computing services used by RIB to host the Application, either via RIB or a RIB Service Partner;

c) Monitoring and maintenance of the cloud infrastructure used by RIB to host the Application; and

d) Access to Commercially Released Versions of the Application (if any) that are made generally available in the Customer's region to other customers entitled to such updates under their support and maintenance agreements.

For Self-Hosted customers:

a) First, Second, and Third Level support of the Application to the Customer's Key Users, either via RIB or a RIB Service Partner;

b) Access to Commercially Released Versions of the Application (if any), made available under the Customer's support and maintenance entitlement.

RIB will provide support and maintenance services only for the Application modules specified in the Order Form and subscribed to by the Customer under the applicable Agreement. Any additional modules subscribed to in the future shall be covered under this SLA, subject to payment of associated fees.

2.2.2. What support & maintenance services are excluded?

The following shall be excluded from RIB's support and maintenance services **under this SLA, irrespective of the hosting model**:

a) Where the Application is used on or in conjunction with hardware or software other than as specified in the applicable Documentation.

b) Where alterations or modifications to the Application, except where such modifications are made by RIB or RIB Service Partner or Affiliates. For the purposes of this clause, "modification" includes any custom configuration and additional interfaces, or integrations implemented by the Customer or any other third party not authorised by RIB to perform such modifications.

c) Where defects occur in the Application due to modifications made by the Customer as defined in Clause 1.10 above, abuse, or improper use by the Customer. For the purposes of this clause, "abuse" or "improper use" means any use of the Application that is not in compliance with the Documentation.

d) Any version of the Application for which support and maintenance services are no longer provided by RIB in accordance with Clause 6.4.3 of this SLA.

e) Training, customisation, integration, and any issues arising from non-standard usage of the Application; for the purpose of this clause "non-standard" usage means any usage not compliant with the applicable Documentation.

f) Any on-site support provided by RIB or RIB Service Partner in connection with this SLA.

g) Assistance in developing user-specific customisations or configurations of the Application, where applicable.

h) All Customer Systems, other than the Application.

i) Assistance with installation or configuration of hardware, including but not limited to computers, hard drives, networks, or printers.

j) Assistance with non-RIB products, services, or technologies, including but not limited to implementation, administration or use of third-party enabling technologies such as databases, computer networks or communications systems that do not form part of the Application.

k) Other professional services including but not limited to:

(i). on-site support, training, the Customer's provision of support to any third-parties, implementation, or any other consulting services which may be separately purchased from RIB or RIB Service Partner as add-on services pursuant to a separate professional services agreement entered into between Customer and RIB or RIB Service Partner.

(ii). any specific support services (e.g., those commonly referred to as "priority support" or "custom support plan") that may be separately purchased from RIB or RIB Service Partner as add-on services pursuant to a separate professional services agreement entered into between Customer and RIB or RIB Service Partner.

2.3. Versioning

RIB reserves the right to update this SLA to reflect evolutions in RIB standard practices. Any updated version of this SLA shall be shared with the Customer upon its release.

2.4. Customer Support Centres

RIB and RIB Service Partner provide support and maintenance services to Customers through their respective Regional and Global Customer Support Centres.

The technical support resources and contact details of such Customer Support Centres shall be provided during the implementation of the Application.

All requests for technical support submitted directly by the Customer through RIB's prescribed channels (e.g. RIB Support Portal, RIB Service Partner service portals, Email and Phone where applicable) shall be managed by the Customer Support Centre, in accordance with the terms agreed upon between RIB (or RIB Service Partner) and the Customer.

2.5. Support Contacts

Support and maintenance services shall be provided through the In-region Customer Support Centres and/or the Global Customer Support Centre. The In-region Customer Support Centre may be located in the Customer's country or the closest country to the Customer where RIB or RIB Service Partner maintains a Customer Support Centre.

In respect of this SLA as defined in Clause 6.1:

- Level Zero support shall be provided by the Customers Key Users;
- First Level support shall be provided by the In-Region or Global Customer Support Centre, depending on the availability of support resources for the relevant region;
- Additional Second Level support shall be provided by the Global Customer Support Centre during its standard business hours, which may, if applicable, fall outside the standard business hours of the In-region Customer Support Centre; and
- Third Level support shall be provided by RIB Managed Services (where applicable) and/or RIB product management and development during their standard business hours, which may fall outside the standard business hours In-region Customer Support Centre.

The standard business hours of the Customer Support Centres are aligned with the standard working hours of their respective countries, which are typically from 08:00 - 17:00 on such countries' business days. Public holidays and bank holidays in the local country shall apply and shall not be deemed business days. Refer to the specific product annexure for service hours.

For Customers to whom this applies, Incidents shall be submitted via the RIB Support Portal, the contact methods of which are set out in Clause 6.2.3.

3. Key Requirements

The successful deployment and operation of the Application shall be subject to the following key requirements. Such requirement may vary depending on the selected hosting model (RIB Hosted, RIB SaaS, or Self-Hosted) and the specific product and are further detailed in the applicable Product Annexure.

3.1. This SLA shall apply solely where the Application is provided under one of the defined hosting models in this SLA, as follows:

- For RIB Hosted and RIB SaaS models: the Application is hosted on a Cloud Platform that is configured and managed by RIB.
- For Self-Hosted model: the Application is deployed and managed on infrastructure controlled by the Customer.

3.2. Where applicable, the successful use of the Application shall require that an appropriate and reliable Internet connection is available at the Customer's locations for all intended users, irrespective of geographic distribution. This requirement shall not apply to products or deployments that operate offline or within isolated networks, as specified in the relevant Product Annexure.

3.3. The Customer shall be responsible for ensuring that the necessary infrastructure (including network and hardware) is in place to support the Application's functionality as defined in the Documentation or, where applicable, the Functional Specifications

which includes ensuring connectivity where required.

3.4. The Customer must maintain a valid test or staging environment (where applicable as detailed in the product annexure) based on its own data, for the purpose of testing new versions and verifying incident resolutions.

4. Hosting Support & Maintenance Service

This section shall apply solely to Customers subscribed to RIB Hosted or RIB SaaS deployment models. It shall not apply to Self-Hosted deployments, where infrastructure is fully managed by the Customer.

4.1. Incident Priority Definitions

To enable RIB to provide support and maintenance services for the cloud computing services used by RIB to host the Application in the Cloud Platform, the Customer shall report these Incidents to RIB or RIB Service Partner via the RIB Support Portal.

RIB or RIB Service Partner will prioritize the reported Incidents according to the severity levels criteria set forth below. Each Incident submitted by the Customer to the relevant Customer Support Centre shall be subject to the average response time applicable to the severity level assigned by RIB or RIB Service Partner pursuant to the severity levels defined below:

- **Priority 1 – Critical Severity (P1)**

  A critical production issue that affects all Customer Users, including unavailability of Cloud Platform and data integrity issues, where:(i) no workaround is available; and (ii) the affected operation is business-critical to the Customer.

  Priority 1 – Critical Severity incidents shall be solely supported when occurring in Production Environments.

- **Priority 2 – Major Severity (P2)**

  An issue where: (i) major functionality is impacted or performance is significantly degraded;(ii) the issue is persistent and affects a substantial number of users and/or major functionality; (iii) such impact significantly impairs the Customer's business; and (iv) no reasonable workaround is available.

- **Priority 3 – Moderate Severity (P3)**

  A system performance issue or bug affecting some but not all users with minimal impact on the Customer's business. Short-term workaround is available, but not scalable.

- **Priority 4 – Minor Severity (P4)**

  A request on a routine technical issue or an error that affects a small number of users. Appropriate workaround available and no impact to the Customer's business.

4.2. Response Times

4.2.1. The targeted response times for Incidents reported in Production Environments are specified in the applicable Product-Specific Annexure to this SLA.

4.2.2. RIB or RIB Service Partner will apply best effort to respond to Incidents in Non-Production Environments. For the purpose of this SLA, support for Production Environments shall always take priority over support for Non-Production Environments.

4.2.3. Response time shall be calculated from the time an Incident is submitted via the RIB Support Portal until the Customer receives the first response from a RIB Customer Support consultant. The Customer will also receive an automated confirmation acknowledging successful submission of the ticket.

4.2.4. RIB or RIB Service Partner shall apply best efforts to provide a temporary resolution aimed to restoring the Availability of the cloud computing services used by RIB to host the Application on the Cloud Platform as soon as reasonably possible.

4.2.5. Where permanent resolution is required, the time frame for such resolution shall depend on the complexity of the Incident and shall be determined on a case-by-case basis. RIB may elect not to provide a permanent resolution in cases where the temporary resolution is deemed sufficient.

4.2.6. The time frames for temporary and permanent Resolution shall depend on the Customer providing as much information regarding the Incident as possible, including but not limited to detailed steps that RIB or RIB Service Partner should follow to reproduce the Incident in a timely manner. Additional information (including access to the Customer's environment) may be requested where necessary. Any delays in providing the information or granting such access may affect RIB's or RIB Service Partner's ability to resolve the Incident.

4.3. Service Hours

4.3.1. The Response Times referenced in this section shall apply during the standard working hours of the Customer Support Centre. Where applicable, the working hours of the In-Region Customer Support Centre are set forth in Clause 2.5 of this SLA.

4.3.2. Product-specific service hours for Incident resolution are defined in the relevant Product-Specific Annexure to this SLA.

4.4. Change Requests

4.4.1. Where applicable, changes to the configuration of the cloud computing services used by RIB to host the Application on the Cloud Platform can be requested via a Change Request. RIB or RIB Service Partner will schedule such Change Requests upon consultation with the Customer. Change Requests shall be billed on a time-and-materials basis at prevailing rates to be provided by RIB or RIB Service Partner. RIB or RIB Service Partner shall

not be obligated to agree to execute a Change Request RIB or RIB Service Partner deems that the request would have any adverse effect. If RIB or RIB Service Partner declines to execute a Change Request, it shall promptly provide the Customer with an explanation. Certain changes may require prompt execution upon the Customer's request. The timing of the execution of urgent changes is determined in consultation with RIB and/or RIB Service Partner. Additional fees shall apply to such urgent changes.

4.5. Availability Targets

4.5.1. During the term of the Agreement, the Availability Target for Production Environments shall be defined in the applicable Product-Specific Annexure to this SLA. Availability calculations are based on the hosting model and infrastructure redundancy, including single zone redundancy within the Cloud Platform for RIB Hosted deployments.

4.5.2. The SLA Availability Target shall not include: (a) Unavailability arising from Excused Outage (e.g., Emergency Downtime, Scheduled Downtime or General Unavailability); (b) instances where RIB has taken the Application offline to protect the security interests of its business or its customers; and (c) the availability or non-availability and/or uptime or downtime of any third-party device, software, infrastructure or system provisioned by the Customer that is not managed or controlled by RIB.

4.5.3. RIB shall not be liable for breaches of this SLA arising from failures, acts or omissions of any third-party Cloud Platform Provider not under control of RIB, in connection with the cloud infrastructure hosting the Cloud Platform.

4.5.4. Calculation of the Availability in percentage

4.5.5. The "Availability" percentage (hereinafter referred to as "A") is calculated based on the "Maximum Monthly Availability" (MMA) and "Downtime" (DT) for the same month, with such measurements (in minutes) determined at the end of the month in accordance with the following formula :

$$A = \frac{MMA - DT}{MMA} * 100\%$$

Availability shall be calculated solely for Production Environments. Availability Target shall not apply to Non-Production Environments.

The MMA period is equal to the total number of minutes in the calendar month.

Downtime resulting from Excused Outage, such as Scheduled Maintenance, Emergency Downtime or General Unavailability shall not be included in the MMA calculation. If RIB and the Customer jointly decide to implement changes to the Cloud Platform configuration in accordance with Clause 4.4.1 and such implementation causes the Cloud Platform to become Unavailable, such Unavailability shall not be taken into account for the calculation of the Downtime.

4.6. Maintenance

4.6.1. RIB will maintain the Application and the cloud computing services used to host the Application on the Cloud Platform in accordance with:

(a) the provisions, instructions, guarantee conditions, manuals, and maintenance schedules of RIB and applicable vendors (including the relevant RIB development teams);

(b) instructions from vendors related to security notifications; and

(c) RIB's policies on availability, security, integrity, personal data protection, and general data confidentiality.

4.6.2. Scheduled Maintenance

RIB shall perform scheduled maintenance activities to safeguard the integrity, availability, and consistency of the Application. These activities may include updates, patches, or other preventative or corrective actions.

The Maintenance Window applicable to each product shall be defined in the relevant Product-Specific Annexure to this SLA.

Maintenance performed by the Cloud Platform Provider shall be excluded from this SLA; the Cloud Platform Provider shall remain solely responsible for such activities.

RIB will provide at least 48 hours' prior notice of any Scheduled Maintenance that is expected to cause downtime. Where no downtime is anticipated, maintenance may proceed without prior notification.

4.6.3. Emergency/Unplanned Maintenance

RIB may be required to perform Emergency Maintenance activities to recover or safeguard the integrity, availability and consistency of the Application. RIB shall make every reasonable effort to notify the Customer prior to the commencement of such maintenance. If prior notification is not possible, notification will be provided as soon as reasonably possible after the completion of the maintenance activities.

4.7. Data Protection

4.7.1. Daily Backup

RIB shall be responsible for performing daily backups and retaining data within the Cloud Platform for a limited period, in accordance with the Product-Specific Annexure applicable to the Customer's product. The backup frequency, retention periods, and scope (e.g. SQL Databases, Fileshares, Virtual Machines, etc.) shall be defined per product and hosting model. Backup responsibilities shall apply solely to RIB Hosted and RIB SaaS deployments. For Self-Hosted environments, the Customer shall be solely responsible for backup and recovery procedures.

4.7.2. Data Restore

Upon the Customer's request, data may be restored from backups. The Customer may request recovery of data for a specific date within the retention period defined in Clause 4.7.1 and detailed within the product annexure. Restore times may vary depending on the volume of data. For the purpose of this section, recovery times are excluded from the Availability calculations under this SLA.

4.7.3. Recovery Point Objectives

In the event that a system or service becomes unavailable and requires restoration, the Recovery Point Objective (RPO) shall mean the maximum acceptable period of data loss, measured from the time of the most recent backup to the time the Incident occurs.

The applicable RPO for each product and hosting model shall be as defined in the corresponding Product-Specific Annexure.

RPO commitments shall apply solely to RIB Hosted and RIB SaaS environments. For Self-Hosted environments, the Customer shall be responsible for defining and managing its own backup frequency and data protection strategy.

4.8. Availability and Disaster Recovery

RIB offers different architectural options and configurations to provide resilience and protection against various disaster scenarios. The default disaster recovery architecture and associated availability guarantees for each product shall be defined in the applicable Product-Specific Annexure.

Protection levels may include, but are not limited to, mitigation of hardware failures within a single Cloud Platform data centre, zone redundancy, or geographic failover, depending on the selected deployment and service level.

These provisions shall apply solely to RIB Hosted and RIB SaaS environments. For Self-Hosted environments, the Customer shall be responsible for implementing and maintaining its own disaster recovery strategies to ensure protection.

4.8.1. The protection for unavailability of the entire Cloud Platform Provider data centre within an region, or the unavailability of an entire region (whether due to an incident or unplanned maintenance), are excluded from this SLA.

4.8.2. In addition to the underlying architecture, the time required to restore full service availability following a disaster shall depend on the operational recovery tasks, incident severity, and priority assigned to the affected environment.

The Recovery Time Objective (RTO) shall mean the maximum targeted duration between the onset of a service disruption and the complete restoration of service.

Unless otherwise specified in the applicable Product-Specific Annexure, the RTO is provided on a best-effort basis for standard RIB Hosted deployments. Enhanced RTOs may be available through custom disaster recovery solutions or

premium service tiers.

4.8.3. For disasters beyond the scope of the architecture corresponding to the chosen protection level, the RTO shall be based on best effort by default.

4.9. Monitoring

RIB shall pro-actively monitor the cloud computing services used by RIB to host the Application on the Cloud Platform:

Health Monitoring

4.9.1. The purpose of health monitoring is to generate a snapshot of the current health of the system to verify that all components of the system are functioning as expected.

Availability Monitoring

4.9.2. The purpose of availability monitoring is to track the availability of the system and its components or to generate statistics about the Availability of the application provided.

4.10. Security & Vulnerability Management

4.10.1. Compliance/Security

RIB uses defined policies and procedures to prevent unauthorized physical and logical access to the cloud computing services used to host the Application on the Cloud Platform, in line with current cybersecurity standards, regulations, and internal RIB security policies.

RIB is committed to:

a) Implementing a management control framework that supports the availability, information security, and continuity objectives as set forth in this SLA;

b) Hosting the Application on Microsoft Azure or similar infrastructure that has various certifications, including ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, and German BSI IT-Grundschutz (Basic IT Protection);

c) Providing transparency regarding Azure compliance certifications via:

- Microsoft Trust Center - https://servicetrust.microsoft.com/
- Microsoft Compliance Offerings - https://docs.microsoft.com/en-gb/compliance/regulatory/offering-home?view=o365-worldwide

4.10.2. Vulnerability Management

Vulnerability Management in RIB (including the Application) follows specific rules defined in the RIB Vulnerability Management Policy as it pertains to vulnerability discovery, triage, remediation, tracking, and closure.

Code and infrastructure vulnerability search and discovery capabilities shall be achieved proactively by RIB through multiple ways, such as automated vulnerability scanning, penetration testing, or through engagement with external sources.

Vulnerability severity attribution takes into account a vulnerability severity in accordance with the Common Vulnerability Scoring System (CVSS) v3.0 or higher, as well as a RIB context score which accounts for Data/Business criticality, perimeter, involved actors, or number of users/assets affected, resulting in a RIB Vulnerability Severity Score (VSS).

Vulnerability remediation consists of an action plan to address the vulnerability, with clear ownership, and reporting of actions and progress until the action plan is implemented in accordance with a vulnerability level and shall not exceed the following timeframes:

Vulnerability Definition		Resolution	VSS Score
Rating	Description		
Severe	Major vulnerabilities exploitable remotely.	Hotfix where feasible; otherwise, resolved in next release or service pack, may cover last 2 releases.	75–100% (Severity Level 4)
High	Major vulnerabilities require local network access.	Fix included in next feasible release or service pack.	50–74% (Severity Level 3)
Medium	Minor impact or requires local server access.	Best effort to resolve in the next release.	25–49% (Severity Level 2)
Low	Informational or withdrawn vulnerabilities with no impact.	No action required	0–24% (Severity Level 1)

- A vulnerability shall be deemed “critical" if it has a severity level of 3 (High) or 4 (Severe), and "non-critical" if it falls under 1 (Low) or 2 (Medium).
- For Level 4 – Severe vulnerabilities, temporary mitigation measures (e.g., hotfix or reconfiguration) will be applied, where feasible, until a permanent resolution is implemented.

- Impact assessments shall take into account in CVSS score, data/business criticality, exposure perimeter, number of affected users/assets, and public disclosure.

5. Application Support & Maintenance Services

This section shall apply to all Customers, regardless of their hosting model. For Self-Hosted deployments, the services defined in this section shall be limited solely to Application-level support only. RIB shall not provide infrastructure, platform, or network-level support for Self-Hosted environments. Additional details and exclusions are set forth in Clause 5 of this SLA and the Product Annexure.

5.1. Incident Priority Definitions

To enable RIB to provide Application support and maintenance services for the Application, the Customer shall report these Incidents to RIB or RIB Service Partner via the RIB Support Portal.

RIB or RIB Service Partner will prioritize the reported Incidents according to the severity level criteria. Each Incident submitted by the Customer to the relevant Customer Support Centre shall be subject to the average response time applicable to the severity level assigned by RIB or RIB Service Partner in accordance with the severity levels defined below.

- **Priority 1 – Critical Severity (P1)**

  The Application is inoperable, and the Customer is unable to use the Application. Core functionalities of the Application fail to perform correctly and could cause the user to make an incorrect decision or take action based on erroneous or incomplete information or instruction provided by the Application. No workaround is available and affects critical users or a large number of users (e.g., key customers).

  - Critical system failure with no viable workaround, and/or;
  - Loss of essential functionality or data, and/or;
  - Security vulnerabilities with high potential for exploitation, and/or;
  - Performance to the point where the majority of the Application is unusable.

  Priority 1 – Critical Severity incidents shall be supported solely when they occur in Production Environments and within functionality in use by the Customer.

  For Self-Hosted environments, incidents must be confirmed as Application-related and shall not be caused by Customer-managed infrastructure.

- **Priority 2 – Major Severity (P2)**

  Defects in the Application that impact productivity or operations in use of the Application, but do not result in the provision of erroneous or incomplete information or instruction to the user. The Customer's use of the Application may continue; however, there is a serious impact on the Customer's productivity and affects a substantial number of users.

  - Major functionality degradation or performance issues, and/or.

- Important features or services fail to function as expected, and/or.
- Security vulnerabilities with a moderate potential for exploitation.

- **Priority 3 – Moderate Severity (P3)**

  Moderate Defects in the Application which cause the Customer's activity to suffer a minor loss of operational functionality. The Customer's use of the Application may continue with minor impact on the Customer's productivity.

  - Non-critical features are not working correctly, and/or
  - Minor performance degradation or intermittent issues.
  - A known workaround is available.

- **Priority 4 – Minor Severity (P4)**

  Minor Defects in the Application which do not interfere with the regular use of the Application, with no impact or minimal impact on the operation of the Application. The Customer's use of the Application may continue.

  - Cosmetic issues or minor UI glitches, and/or
  - Non-essential features fail to function as expected, and/or
  - Requests for documentation clarifications or general inquiries, and/or
  - Issue involves non-core functionality.

5.2. Incident Priority Validation

RIB shall reserve the right to validate and adjust the severity level assigned by the Customer in accordance with the priority set forth in this SLA.

- RIB will map the reported Incident against its internal incident classification guidelines.
- For confirmed Priority 1 Incidents, RIB's Incident Response Plan will be triggered immediately.
- If the priority is adjusted, RIB will notify the Customer and proceed under the updated severity level.

5.3. Response Time

5.3.1. Targeted response times for Application-related Incidents in Production Environments are defined in the applicable Product-Specific Annexure to this SLA.

RIB or the designated RIB Service Partner shall apply best effort to respond to Incidents occurring in Non-Production Environments, but such environments shall not be covered by guaranteed response commitments.

For all reported Incidents, response and resolution efforts for Production Environments shall take priority over those for Non-Production Environments.

5.3.2. Response time shall be calculated from the moment an Incident is submitted via the RIB Support Portal until the Customer receives the first response from a RIB Customer Support consultant. Upon submission, the Customer shall also receive an automated confirmation acknowledging successful receipt of the ticket.

5.3.3. RIB or RIB Service Provider shall apply best effort to provide a temporary resolution aimed at enabling the Customer to resume operations as soon as reasonably possible.

5.3.4. If permanent resolution is required, the time for such resolution shall depend on the nature and complexity of the Incident and shall be determined on a case-by-case basis. RIB may elect not to provide a permanent resolution in cases where the temporary resolution is deemed sufficient.

5.3.5. Temporary and permanent resolution times are depended on the Customer providing as much information regarding the incident as possible, including but not limited to detailed steps that RIB should follow to reproduce the Incident in a timely manner. Additional information (including access to the Customers environment and data) may be requested where necessary. Any delays in providing the information or granting access may affect RIB's ability to resolve the Incident.

5.4. Service Hours

The applicable service hours for Incident response and resolution are defined in the relevant Product-Specific Annexure to this SLA.

Standard service coverage shall be provided by the Global Customer Support Centre, with regional variations as defined in Clause 2.5 for In-Region Customer Support Centres.

Service hours may be affected by public holidays in different regions. Customers should refer to their respective annexure to confirm product-specific and regional service hours.

5.5. Suggestion Requests

5.5.1. Suggestion Requests are software enhancements and/or additions to the current functionality of the Application that a Customer may request from time to time.

5.5.2. Suggestion Requests may be submitted via the RIB Support Portal and shall be deemed non-urgent. RIB will analyse each received Suggestion Request for possible inclusion within a future version; however RIB shall be under no obligation to do so.

5.5.3. RIB will apply best effort to provide feedback on all Suggestion Requests received.

6. General Support and Maintenance Terms

6.1. Levels of Support

6.1.1. “Customer Key User Support” (also known as Level 0 support): basic help desk resolution and service desk delivery. Level 0 is provided by the Key User within the Customer’s organisation and shall include support for basic issues, such as solving usage problems and fulfilling service desk requests that need IT involvement. If no solution is available, Level 0 support shall escalate the Incident to Level 1 support.

6.1.2. The Key Users will be trained by RIB during the implementation phase to function as Level 0 support to internal users.

6.1.3. “In Region Support” (also known as Level 1 support): A single point of contact, incident management and further processing of Incidents to identify, evaluate, specify and resolve the Incident. Level 1 support shall be provided by the RIB or RIB Service Partner In-Region Customer Support Centre. Where available, support may be provided within the local languages of the Customer. Level 1 support shall include support for general issues and fulfilling service desk requests. If no solution is available, Level 1 support shall escalate the Incident to Level 2 support.

6.1.4. “Advanced Support” (also known as Level 2 support): In-depth technical support for both functional and non-functional Incidents, including product configuration, provided by the Global Customer Centre. In regions where Level 1 Support is unavailable or outside the standard business hours of Level 1 support, Level 1 support shall be able to escalate Incidents directly to Level 2 support which may be provided in English only. Level 2 support provides solutions for Incidents that cannot be handled by Level 0 or Level 1, and shall attempt to replicate Incidents and identify root causes. If no solution is available, Level 2 support shall escalate the Incident to Level 3 support.

6.1.5. “Expert Support” (also known as Level 3 support): expert product and service support provided by RIB Managed Services, Product Management and Development for the Application, and by Microsoft for the Cloud Platform. Level 3 support shall have access to the highest technical resources available for problem resolution or new feature creation. Level 3 support can attempt to replicate Incidents and identify root causes, using product designs, code or specifications.

6.2. Submitting Incidents

6.2.1. Based on the severity of the Incident, the Customer Support Centre prioritises the Customer’s support needs and ensure proper escalation from Level 1 support to Level 3 support when necessary.

This process shall be tracked through the Incidents created in the RIB Support Portal to follow-up on resolution, actions and provide responses to

the Customers and keep records of interactions with the Customers and technical investigation. Customer Support Centres shall endeavour to respond to and, where possible, resolve the Customers' requests at Level 1 support. When the Incident requires more complex support, the Customer Support Centres may escalate to Level 2 support and then, as necessary, to Level 3 support.

The following information should always be included when Customer submits incidents:

a) Detailed information on the Incident must be provided. Screenshots or Recordings are preferred.

b) Instructions on how to reproduce the Incident including details of relevant data being used (e.g. Company & Project Header).

c) Application Version.

d) Environment (Production, UAT or Testing).

e) For Performance issues – the normal time for transaction vs the new time for transaction.

f) All support is provided remotely and the Customer shall provide access to RIB or RIB Service Partner to Customer's Application to assist in understanding and solving the Incident.

g) The Customer must timeously respond to questions and requests for additional information as these response times may affect the delivery time of the temporary or permanent resolution.

6.2.2. There is no limit to the number of Incidents a customer may create during any calendar month.

6.2.3. Access to the RIB Service Portal for recording Incidents is available 24 hours a day, 7 days a week and 365 days a year. Service Portal could be access via this URL: https://www.rib-software.com/en/support

6.3. Resolution or Closure of Incidents

RIB or RIB Service Provider shall use its best effort to resolve the submitted Incidents where technically possible as quickly as feasible.

Incidents shall be resolved or closed in the following manner:

6.3.1. For solvable Incidents, and depending on its nature, the resolution may take the form of an explanation, a recommendation, usage instructions, workaround instructions, or a requirement for the Customer to upgrade or roll back the Application to a later or earlier Commercially Released Version.

6.3.2. In the event that custom or unsupported plug-ins or modules are used, RIB or RIB Service Partner may, in the course of attempting to resolve the Incident, request that Customer to remove any unsupported plug-ins or

modules. If the Incident disappears upon removal of an unsupported plug-in or module, RIB or RIB Service Partner shall consider the Incident resolved.

6.3.3. For Incidents falling outside the scope of support and maintenance services, RIB or RIB Service Partner may close the Incident by identifying that it is outside such scope, or that it arises from a version, platform, or usage case that is excluded from this SLA.

6.3.4. For dropped Incidents, RIB or RIB Service Partner may close the Incident if the Customer Contact has not responded to at least two (2) attempts made by RIB or RIB Service Partner to collect additional information required to solve the Incident, or if a period of more than five(5) working days has elapsed since such attempts.

6.4. Release Management

6.4.1. In order to ensure that individual services remain compatible with each other and deliver the intended function, release management shall include the actual Application itself, in combination with all components and services of the Cloud Platform used by RIB to host the Application where applicable. RIB shall be responsible for release management and shall carry out releases accordingly.

6.4.2. The Application's release cycles are as specified by RIB. If RIB declares features or versions as unsupported, RIB shall no longer provide the services pursuant to this SLA. A specific Out-of-Support SLA may be offered in specific circumstances with different fees applicable.

6.4.3. For any Commercially Released Version, the supported version shall be defined in the specific Product Annexure for the relevant Application.

6.4.4. Details of currently supported versions and the end-of-support dates for preceding versions shall be published in announcements within the Documentation accompanying each new Commercially Released Version, and shall be accessible via the documentation menu in the Application.

6.4.5. The SLA and all provisions contained herein do not apply to services, Applications and/or versions declared "end-of-life" by RIB.

6.5. Escalation

6.5.1. The escalation path shall be communicated by local RIB or RIB Service Provider's customer success manager. The customer success manager may also be contacted when support is needed during the escalation process.

6.5.2. Each party may appoint an escalation manager, respectively, who shall be responsible for communication during the escalation process. The escalation managers shall temporarily take the ownership of the Incident and shall have the authority to deploy adequate resources to resolve the Incident as swiftly as possible. De-escalation shall be completed when the parties reach a

mutual agreement that the Incident has been resolved, and the parties move to close the Incident.

6.6. Disclaimers

RIB shall not be obligated to provide support and/or maintenance for Defects that cannot be reproduced, nor for Incidents caused by any of the following:

a) Any third-party items, including any third-party commercial software, firmware, hardware or any information or memory data contained in or stored on third party products or services;

b) Integrations, linkages, or technical interfaces of the Application with third-party systems or software;

c) Changes to the Customer's internal security policies;

d) Changes to browser, operating system or Customer Systems made by the Customer or third-party providers not under RIB’s control;

e) Any unauthorized use or any misuse of the Application and/or the Cloud Platform by the Customer or any person under its control, including but not limited to inappropriate use of the access rights (e.g., credentials) provided by RIB and/or operating errors in the use of the Application or the Cloud Platform;

f) Use of the Application and/or the Cloud Platform not in accordance with the Documentation, other instructions provided to the Customer by RIB, or other terms agreed between RIB and Customer under the Agreement;

g) Use of the Application and/or the Cloud Platform in violation of the RIB General Terms and Conditions;

h) The Customer's non-compliance with one or more of its obligations under this SLA, or with any operation or maintenance instructions provided by RIB in relation to the Application (including but not limited to the continued use of the Application in its prior version after a Commercially Released Version has been made available to the Customer by RIB);

i) Actions, omissions (including but not limited to the Customer’s failure to provide information), or erroneous instructions delivered by the Customer to RIB;

j) Errors arising from systems, networks, connections, infrastructure, equipment, software or hardware of Customer, its affiliates or its/their respective contractors or service providers;

k) Use of the Application and/or the Cloud Platform in conjunction with any unsupported platform, software, equipment, hardware or devices;

l) Any modification or alteration to the Application and/or the Cloud Platform made by Customer or any other person not under RIB’s control;

m) Force Majeure or any other situations that cannot be attributed to RIB;

n) Distributed Denial of Service (DDoS) that render online service, network resources or host machine unavailable to its users on the Internet;

o) Damage caused by zero-day exploits (e.g., viruses, Trojans, malware, etc.) that could not be detected by virus scanners considered up-to-date at the time of the attack;

p) Downtime occurring after the implementation of a new Commercially Released Version where such downtime is caused by a customer-initiated change request or customer-developed customisation to the Application;

q) Incompatibility between the Customer's applications with the Application.

RIB does not warrant that the Application will be free of vulnerabilities, Cyber Threats or protected against all viruses or other contamination factors that may threaten the security or integrity of the Application or Customer Systems. Without prejudice to Clause 4.10, RIB shall not be obligated to provide support and/or maintenance for Incidents, nor shall it bear any liability for limitations or delays in the Application caused by telecommunication networks, the internet or Cyber Threats.