Service Level Agreement

VERSION 3.0, CURRENT AS OF 29 November 2023

RIB 4.0

RIB Software GmbH

Epplestraße 225, Haus 2,
70567 Stuttgart,
Germany

Contents

1. Introduction

1.1. Overview

1.1.1. This Service Level Agreement (hereinafter “Hosting SLA”, or “SLA”) defines the levels of support & maintenance services that RIB agrees to provide in connection with the Application and its hosting on the Cloud Platform to any Customer purchasing from RIB or any of its Affiliates a subscription to the cloud-based software solution (hereinafter “Application”, as defined in Clause 2.3).

1.1.2. In the event of a conflict between the provisions of this SLA and the provisions of the RIB General Terms & Conditions and/or service level agreements for the Hosting Services referred to or otherwise incorporated in the RIB General Terms & Conditions, the provisions of this SLA shall prevail.

1.2. Scope

1.2.1. What support & maintenance services are included?

Subject to due payment by the Customer of the amounts invoiced for the support and maintenance of Application in accordance with the Quote and / or Licence Agreement, RIB or RIB Service Partner shall provide the Customer with the following services for the Application and the cloud computing services used by RIB to host the Application in the Cloud Platform:

a) Second, Third and Fourth level support of the Application, either via RIB or an RIB Service Partner;

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

c) Monitoring and maintenance of the cloud computing services used by RIB to host the Application on the Cloud Platform; and

d) Access to the Commercially Released Version of the Application (if any) that is released by RIB during the relevant Support & Maintenance Term and made generally available in the given country to all other Customers which are entitled to receive same support and maintenance services for the Application.

RIB will provide support and maintenance services only for the Application modules as specified in the Quote and subscribed to by Customer as part of the Application under the applicable Agreement.

1.2.2. What support & maintenance services are excluded?

The following are excluded from RIB’s support and maintenance services of the Application and Cloud Platform:

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

b) Where the Application is altered or modified unless the modification is made by RIB or RIB Service Partner or Affiliates. Modification means any custom configuration and additional interfaces, or integrations done by the Customer or any other 3rd party not authorised by RIB to make such modifications.

c) Where defects occur in the Application due to modification made by the Customer as defined in Clause 1.2.2 b) above, abuse, or improper use by the Customer. Abuse or improper use means a use of the Application that is not complying with the Documentation.

d) Any version of the Application for which support, and maintenance services is no longer provided by RIB in accordance with Section 6.8.3 of this SLA.

e) Training, customization, integration, and any issues arising from non-standard usage of the Application where non-standard usage shall be any usage not compliant with the applicable Documentation.

f) Any on-site support related to this SLA by RIB or RIB Service Partner.

g) Assistance in developing user-specific customizations or configurations of the Application.

h) All Customer Systems, other than the Application.

i) Assistance with installation or configuration of hardware, including computers, hard drives, networks, or printers.

j) Assistance with non-RIB products, services, or technologies, including implementation, administration or use of third-party enabling technologies such as databases, computer networks or communications systems.

k) Other professional services such as, but not limited to,

I. on-site support, training, Customer's own 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 under a separate professional services agreement agreed to between Customer and RIB or RIB Service Partner.

II. any specific support services such as commonly called "priority support" or "custom support plan" which may be separately purchased from RIB or RIB Service Partner as add-on services under a separate professional services agreement agreed to between Customer and RIB or RIB Service Partner.

1.3. Versioning

RIB reserves the right to update this SLA to reflect evolutions in RIB standard practices and new updates of this SLA will be shared with the Customer as soon as they are

released.

1.4. Customer Care Centres

RIB and RIB Service Partner delivers support & maintenance services to Customers through their Regional and Global Customer Care Centres.

The technical support resources and the contact details of our Customer Care Centres will be provided during implementation of the Application.

The Customer Care Centre will manage all customers' requests for technical support received directly through those channels (e.g. RIB Service Portal, RIB Service Partner service portals, Email and Phone where applicable) as agreed upon between RIB, RIB Service Partner and the Customer.

1.5. Support Contacts

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

In the case of this SLA as defined in Section 6.1, First Level support is provided by the Customers key users and Second Level support will be provided by the In-Region Customer Care Centre, additional Third Level support will be provided by the Global Customer Care Centre during standard business hours of the Global Customer Care Centre, which may fall outside the standard business hours of the In-region Customer Care Centre, and Fourth Level support will be provided by RIB product management and development during of standard business hours of RIB product management and development, which may fall outside the standard business hours In-region Customer Care Centre.

The standard business hours of the Customer Care Centres are aligned to standard working hours of their respective country which are usually from 08:00 - 17:00 in such country's business days. Local country public/bank holidays are applicable and shall not be considered as business days.

Where applicable to a Customer, Incidents shall be submitted via the RIB Service Portal that can be contacted as detailed in Section 6.2 below.

2. Definitions

Where a term in this SLA is capitalised but not otherwise defined, such term adopts the meaning given to it in RIB General Terms and Conditions.

2.1. "**Agreement**": means the licence agreement and/or General Terms & Conditions entered into by the Customer and RIB upon the Customer's acceptance of the Quote to which this SLA is appended or in connection with which it has been provided to Customer.

2.2. “**Affiliates**”: means as to RIB or Customer, any other entity that directly or indirectly controls, is under common control with, or is controlled by, such party; as used in this definition, “control” and its derivatives mean possession, directly or indirectly, of (i) the majority of the shares or of the share capital of an entity, or (ii) power to direct the management or policies and who are authorised to make modification to the source code Application.

2.3. "**Application**”: means the software application, also known as iTWO 4.0, MTWO and RIB 4.0, developed by RIB, to be 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 the like, and any and all revisions, modifications, and updates thereof delivered or made available to the Customer by RIB or through an RIB Service Partner pursuant to the Agreement.

2.4. “**Application Fee**”: means the monthly or annual fees as specified in the Quote for the Application modules and subscribed to by Customer as part of the Application under the applicable Agreement.

2.5. “**Availability**”: (also referred to as “being “Available”) means that both the Cloud Platform and the Application are accessible. Excused Outages shall not be taken into account for measuring Availability.

2.6. “**Cloud Platform**”: means the Microsoft Azure cloud computing service (often referred to as Azure) operated by Microsoft for application management via Microsoft-managed data centres on which RIB is hosting the Application.

2.7. "**Cloud Platform Azure Consumption Fee**”: means the total monthly usage charged by Microsoft Azure to RIB calculated for the actual Azure consumption by Application on the Cloud Platform plus a handling fee. Azure consumption is the usage of products and/or services sourced through Microsoft Azure.

2.8. “**Commercially Released Version**”: means any Major Release, Minor Release, or updates to a Major or Minor Release that may be released from time to time by RIB. (a) Major Releases may include architectural and structural changes, modifications or enhancements to the Application as designated by a change in the number to the left of the first decimal in the version number. For example, V6.0 is the next Major Release after V5.0. (b) Minor Releases may include code updates and changes to features of the Application, as are normally identified by the number immediately following the first decimal point. For example, V6.1 is a Minor Release after V6.0. (c) updates to Major or Minor Releases which includes code corrections, patches and updates of the Application as designated by the addition of an Alpha character following the numerical number. For example, V6.0 update A is an update of V6.0. means the most recent version of the Application released and deployed by RIB from time to time.

2.9. “**Customer**”: means the legal person receiving the support & maintenance services described in this SLA for the Application and its hosting on the Cloud Platform as subscribed by said legal person from RIB, any of its Affiliates or authorized Service Partners.

2.10. "**Customer Care Centre**": means either the RIB or RIB Service Partner In-Region Customer Care Centre located in the Customer's country or the closest country to the Customer's where RIB or RIB Service Partner has an office with Application support capabilities or the Global Customer Care Centre with the overall responsibility for Application and Cloud Platform support.

2.11. "**Customer Contact(s)**": qualified named person(s) within Customer's organization acting as authorized user of the Application.

2.12. "**Customer Systems**": Customer's own computer networks or infrastructures such as 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.

2.13. "**Cyber Threat**": any circumstance or event with the potential to adversely impact, compromise, damage, or disrupt the Application, Cloud Platform, RIB Systems, Customer Systems or that may result in any unauthorized access, acquisition, loss, misuse, destruction, disclosure, and/or modification of Customer Systems, including any data, including through malware, hacking, or similar attacks.

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

2.15. "**Documentation**": means the online documentation and any other materials describing the functions of the Application and, as applicable, the procedures or instructions relating to its use, in either case in the formats and versions determined by RIB for release.

2.16. "**Downtime**": means the total number of minutes during a calendar month that the Application is not accessible or otherwise not available to the Customer when such inaccessibility or unavailability is solely caused by a Defect in the Application, the inaccessibility or unavailability of the Cloud Platform or other factors within RIB's reasonable control. Downtime does not include Emergency Downtime, Scheduled Downtime and General Unavailability.

2.17. "**Emergency Downtime**": means those times when RIB or Microsoft Azure becomes aware of a vulnerability of the Cloud Platform or its hosting infrastructure that RIB or Microsoft Azure deems to require prompt remediation and, as a result, the Application and Cloud Platform is temporarily made unavailable for remediation of such vulnerability.

2.18. "**Excused Outage**": means Unavailability (i) during Emergency Downtime, Scheduled Downtime and/or General Unavailability (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 gaining access to the Application due to any such negligent act or omission or willful misconduct, (iii) arising from the

Customer's instruction or direction to RIB that RIB cease making the Application Available to Customer, or (iv) during a Force Majeure Event.

2.19. "**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.

2.20. "**Functional Specifications**": has the meaning set forth in RIB General Terms & Conditions.

2.21. "**General Terms & Conditions**": means the agreement entered into by and between RIB, and the Customer which can be found on https://www.mtwocloud.com/legal-terms-all-versions.

2.22. "**General Unavailability**": means network outages, infrastructure outages, unavailability caused by a third party (not under RIB's control) or Customer's hardware or software or unavailability caused by acts or omissions of Customer or its employees, subcontractors, or agents, such as Unavailability resulting from the failure or lack of availability of third-party cloud services upon which the Cloud Platform depends.

2.23. "**Hosting Fee**": means the fee that RIB or RIB Service Partner will charge to the Customer for access to the Cloud Platform. This fee includes Cloud Platform Azure Consumption Fee plus any markup and services fees RIB may include for the support and maintenance of the of the cloud computing services used by RIB to host the Application on the Cloud Platform.

2.24. "**Incident**": means each individual Defect of the Application reported to RIB's Customer Care Centre by a Customer Contact or any individual cause of unavailability or inaccessibility of the Cloud Platform.

2.25. **"Non-Production Environment**": means any environment confirmed by the Customer to RIB as being a, trial, pre-production or test environment in which the Customer wishes to use the Application as hosted on the Cloud Platform for amongst others testing, evaluation, and other non-use purposes.

2.26. "**Production Environment**": means the environment confirmed by the Customer to RIB as being the environment in which the Customer wishes to use the Application as hosted on the Cloud Platform for the purpose of its ordinary course of business. Non-Production Environments are excluded from Production Environment.

2.27. "**Quote**": means the agreement that includes the commercial terms and conditions regarding to the licence fee, subscription fee, implementation fee and other applicable fees for accessing the Application, and to be provided by RIB or RIB Service Partner.

2.28. "**RIB**": means the RIB entity as defined in the General Terms and Conditions that delivers the Support & Maintenance services described in this SLA either directly or

through its local Affiliates to which the In-Region or Global Customer Care Centres are reporting.

2.29. "**RIB Service Partner**": has the meaning set forth in RIB General Terms & Conditions.

2.30. "**Scheduled Downtime**": means the period of time when the Application is unavailable because of scheduled deployment of the Application or the Scheduled Maintenance of the Cloud Platform or the cloud infrastructure within which the Cloud Platform is hosted.

2.31. "**Scheduled Maintenance**": means the maintenance performed by RIB in accordance with Section 6.4.2 below.

2.32. "**Service Portal**": means a web-based systems to be used by the Customer for Incidents submission and by RIB or RIB Service Partners for responses to the Customer. Access to a Service Portal and URL, where agreed, will be provided when the Customer is onboarded by Customer Care Centre.

2.33. "**SLA Uptime Commitment**": has the meaning set forth in Section 4.5.1 below.

2.34. "**Subscription Period**": means the period of time as defined in the Quote or Agreement for which Customer has subscribed to the Application.

2.35. "**Unavailability**": (also referred to as "being "Unavailable") means that either the Cloud Platform or the Application, or both, is/are not Available.

2.36. "**Unexcused Outage**": means Unavailability outside of periods of Excused Outages.

2.37. "**Uptime**": means the total number of minutes during a calendar month in which the Cloud Platform and the Application is Available. In order to determine if RIB meets the SLA Uptime Commitment for a calendar month, the Uptime percentage will be calculated as stated in Section 4.5.4 below.

3. Key Requirements

The successful deployment and implementation of the Application is based on the following key requirements:

3.1. This SLA applies to the sole extent that the Application is hosted on the Cloud Platform, which is specifically configured by RIB.

3.2. Successful deployment of the Application requires that an appropriate Internet connection is available at the Customer from each user(s)' groups (regardless of geographic distribution).

3.3. For key Customer locations, Microsoft Azure has dedicated access options that can be provided by RIB at an additional cost.

3.4. It is the Customer's responsibility to ensure that appropriate connectivity is available for the Application to provide the functionalities defined in the Documentation or, as applicable, in the Functional Specifications.

3.5. The Customer must have a valid test system for the testing of new versions and incident resolutions based on the Customers data.

4. Hosting Support & Maintenance Service

4.1. Incident Priority Definitions

To enable RIB to provide support and maintenance services of 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 Service Portal.

RIB or RIB Service Partner will prioritize the reported Incidents according to the severity levels criteria described below. Each Incident submitted by the Customer to the relevant Customer Care Centre will be subject to the average response time applicable to the severity level assigned by RIB or RIB Service Partner as per the severity levels defined below:

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

  Critical production issue affecting all Customer Users, including Cloud Platform unavailability and data integrity issues with no workaround available and the operation is business-critical for the Customer.

  Priority 1 – Critical Severity incidents are only supported when occurring in Production Environments.

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

  Major functionality is impacted, or performance is significantly degraded. Issue is persistent and affects many users and/or major functionality which significantly impacts the Customer's business. No reasonable workaround is available.

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

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

- **Priority 4 – Low Severity (P4)**

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

4.2. Response and Resolution Times

4.2.1. The table below indicates the targeted response times associated with Production Environments. RIB or RIB Service Partner will apply best effort to respond as per the table below for Non-Production Environments. For this SLA, Production Environments will in all Incidents receive priority over Non-Production Environments.

Severity Level	Targeted Response Time
Priority 1 – Critical Severity (P1)	2 hours
Priority 2 – Major Severity (P2)	4 hours

Priority 3 – Minor Severity (P3)	8 hours
Priority 4 – Low Severity (P4)	24 hours

4.2.2. Response time will be calculated from the time the Incident is submitted via the Service Portal until the Customer receives the first response from RIB which may be automated.

4.2.3. RIB or RIB Service Partner will apply best efforts to provide a temporary resolution aimed to restore Availability of the cloud computing services used by RIB to host the Application in the Cloud Platform as soon as possible.

4.2.4. Permanent resolution times, if required, will depend on the complexity of the Incident and will be determined on a case-by-case basis. RIB may choose not to provide a permanent resolution in cases where the temporary resolution is deemed sufficient.

4.2.5. 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 or RIB Service Partner should follow to reproduce the Incident in a timeously manor. Additional information including access to the Customer's environment may be requested where necessary. Any delays in providing the information or granting access may affect RIB's or RIB Service Partner's ability to resolve the Incident.

4.3. Support Availability Times

4.3.1. The Response times indicated above are applicable during the working hours as stated below for the Global Customer Care Centre. The In-Region Customer Care Centre working hours are provided in section 1.5 above.

Severity Level	Service Hours – Incident Resolution
Priority 1 - Critical Severity (P1)	Monday to Friday between UTC + 7 to UTC - 2 (Service Hours maybe affected by Public Holidays in different regions)
Priority 2 - Major Severity (P2)	Monday to Friday between UTC +7 to UTC -2 (Service Hours maybe affected by Public Holidays in different regions)
Priority 3 - Minor Severity (P3)	
Priority 4 - Low Severity (P4)	

4.4. Change Requests

4.4.1. Changes to the configuration of the cloud computing services used by RIB to host the Application in the Cloud Platform can be requested through a Change Request. RIB or RIB Service Partner will schedule Change Requests upon

consultation with the Customer. Change Requests are billed on a time-and-materials basis at prevailing rates to be provided by RIB or RIB Service Partner. RIB or RIB Service Partner do not have an obligation to agree to execute a Change Request if this is deemed by RIB or RIB Service Partner to have any adverse effect. Should RIB or RIB Service Partner decline to execute a Change Request, an explanation will be promptly provided to the Customer. Some 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 will apply for urgent changes.

4.5. Availability Targets

4.5.1. During the term of the Agreement, Uptime for Production Environments will be 99% (the "SLA Uptime Commitment") and is based on Single Zone redundancy within Azure.

4.5.2. The SLA Uptime Commitment does not include: (a) Unavailability due to Emergency Downtime, Scheduled Downtime and General Unavailability; (b) instances where RIB has taken the Application offline due to 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 and not managed or controlled by RIB.

4.5.3. RIB is not responsible for breaches of this SLA arising due to the failures, acts or omissions of Microsoft Azure and any third-party service providers not under control of RIB in connection with the cloud infrastructure hosting the Cloud Platform.

4.5.4. Calculation of the Uptime in percentage

The "Availability" percentage (hereinafter referred to as "A") measures the Uptime percentage and is calculated based on the "Maximum Monthly Availability" (MMA) and "Downtime" (DT) measured in the same month at the end of the month as specified in the formula below measured in minutes:

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

Availability is calculated for Production Environments only. No Availability commitments apply to Non-Production Environments.

The MMA period is equal to the total number of hours per month.

Downtime that is the result of Scheduled Maintenance or Emergency Downtime or General Unavailability is not included in the MMA calculation. A joint decision by RIB and the Customer to perform changes to the Cloud Platform configuration

in accordance with Section 4.4.1 may cause the Cloud Platform to become Unavailable during the implementation of the change, such Unavailability will not be taken into account for the calculation of the Downtime.

5. Application Support & Maintenance Services

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 Service Portal.

RIB or RIB Service Partner will prioritize the reported Incidents according to the Severity Level criteria described below. Each Incident submitted by the Customer to the relevant Customer Care Centre will be subject to the average response time applicable to the severity level assigned by RIB or RIB Service Partner as per the severity levels defined below.

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

  The Application is inoperable and the Customer's use of the Application is not possible. Core functionalities of the Application do not perform correctly and could cause the user to make an incorrect decision or act based on erroneous or incomplete information or instruction provided by the Application. No workaround is possible.

  Priority 1 – Critical Severity incidents are only supported when occurring in Production environments.

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

  Defects in the Application that have a consequence in terms of productivity or operation in use of the Application, but they do not lead to provide erroneous or incomplete information or instruction to the user. Customer's use of the Application is continuing; however, there is a serious impact on the Customer's productivity.

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

  Minor Defects in the Application which cause Customer's activity to suffer a minor loss of operational functionality. Customer's use of the Application is continuing with minor impact on the Customer's productivity.

- **Priority 4 – Low Severity (P4)**

  Minor Defects in the Application which do not interfere with the regular use of the Application without impact or minimal impact on the operation of the Application. Customer's use of the Application is continuing.

5.2. Response and Resolution Times

5.2.1. The table below indicates the targeted response times associated with Production environment. RIB or RIB Service Provider will apply best effort to respond as per the table below for Non-Production Environment. For this SLA, Production Environments will in all Incidents receive priority by RIB over Non-

Production Environments.

Severity Level	Response Time
Priority 1 - Critical Severity (P1)	2 hours
Priority 2 - Major Severity (P2)	4 hours
Priority 3 - Minor Severity (P3)	24 hours
Priority 4 - Low Severity (P4)	48 hours

5.2.2. Response time will be calculated from the time the Incident is submitted via the Service Portal until the Customer receives the first response from RIB which maybe an automated.

5.2.3. RIB or RIB Service Provider will apply best effort to provide a temporary resolution aimed to get the customer working as soon as possible.

5.2.4. Permanent resolution times, if required, will depend on the nature and complexity of the Incident and will be determined on a case-by-case basis. RIB may choose not to provide a permanent resolution in cases where the temporary resolution is deemed sufficient.

5.2.5. 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 timeously manor. 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.

5.3. Support Availability Times

5.3.1. The Response and Resolution Time indicated above are applicable during the working hours as state below for the Global Customer Care Centre. The In-Region Customer Care Centre working hours as provide in section 1.5 above.

Severity Level	Service Hours – Incident Resolution
Priority 1 - Critical Severity (P1)	Monday to Friday between UTC – 2 to UTC +7 (Service Hours maybe affected by Public Holidays in different regions)
Priority 2 - Major Severity (P2)	Monday to Friday between UTC – 2 to UTC +7
Priority 3 - Minor Severity (P3)	

Priority 4 - Low Severity (P4)	(Service Hours maybe affected by Public Holidays in different regions)

5.4. Change Requests

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

5.4.2. Changes Request can be submitted via the Service Portal and are viewed as not urgent. RIB will analyse received Change Request for possible inclusion within a future version, however RIB will be under no obligation to do so.

5.4.3. RIB will apply best effort to provide feedback on all Change Request received.

6. General Support and Maintenance Terms

6.1. Levels of Support

6.1.1. **"Customer Key User Support" (also known as Level 1 support):** basic help desk resolution and service desk delivery. Level 1 is provided by the Key User within the Customer's organisation and provides support for basic issues such as solving usage problems and fulfilling service desk requests that need IT involvement. If no solution is available, Level 1 support will escalate the Incident to Level 2 support.

A maximum of 5 authorised Key Users will be allowed to escalate incidents to level 2 or 3 where applicable or as otherwise agreed between the Customer and RIB or RIB Service Provider.

The Key Users will be trained by RIB during the implementation phase to function as Level 1 support to internal users.

6.1.2. **"In Region Support" (also known as Level 2 support**): Single Point of contact, incident management and further processing of Incidents to identify, evaluate, specify and resolve the Incident. Level 2 is provided by the RIB or RIB Service Partner In-Region Customer Care Centre. Where available support may be provided within the local languages of the Customer. Level 2 support provides support for general issues and fulfilling service desk requests. If no solution is available, Level 2 support will escalate the Incident to Level 3 support.

6.1.3. **"Advanced Support" (also known as Level 3 support):** in-depth technical support on both functional and non-functional Incidents including product configuration and is provided by the Global Customer Centre. In regions where Level 2 Support is unavailable or outside the standard business hours of Level 2 support, Level 1 support will be able to escalate Incidents directly to Level 3 support which will be provided in English only. Level 3 support provides solutions for Incidents that cannot be handled by Level 1 or Level 2 and will attempt to replicate Incidents and define root causes. If no solution is available, Level 3 support will escalate the Incident to Level 4.

6.1.4. **"Expert Support" (also known as Level 4 support):** expert product and service

support and is provide by RIB Product Management and Development for the Application and Microsoft for the Cloud Platform. Level 4 has access to the highest technical resources available for problem resolution or new feature creation. Level 4 can attempt to replicate Incidents and define root causes, using product designs, code or specifications.

6.2. Submitting Incidents

6.2.1. Based on the severity of the Incident, the Customer Care Centre prioritises Customer's support needs and assure proper escalation from Level 2 support to Level 4 support when necessary.

This process is tracked through the Incidents created in the Service Portal to follow-up on resolution, actions and provide answers to Customers and keep records of interactions with Customers and technical investigation. Customer Care Centres will endeavour to answer and if possible, solve Customers' requests at Level 2 support. When the Incident requires more complex support, the Customer Care Centres can escalate to Level 3 support and then, as necessary, to Level 4 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 Company & Project Header.

c) Application Version.

d) Environment (Production, UAT or Testing).

e) For Performance issues - Normal time for transaction vs New time for transaction.

f) All support is provided remotely and the Customer should 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 effect 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 the Incidents is available 24 hours per day, 7 days per week and 365 days per year

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 requiring Customer to upgrade the Application to a later 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 ask, in the course of attempting to resolve the Incident, that Customer to remove any unsupported plug-ins or modules. If the Incident disappears upon removal of an unsupported plug-in or module, then RIB or RIB Service Partner will consider the Incident to be resolved.

6.3.3. For Incidents out of scope of Support and Maintenance Services, RIB or RIB Service Partner may close the Incident by identifying the Incident as outside the scope of the Support and Maintenance Services or arising from a version, platform, or usage case which is excluded from this SLA.

6.3.4. 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 5 working days has elapsed.

6.4. Maintenance

6.4.1. RIB will maintain the Application and the cloud computing services used by RIB to host the Application on the Cloud Platform in accordance with the following: (a) The provisions, instructions, guarantee conditions, manuals, and maintenance schedules of RIB and the applicable vendors including but not limited to, the relevant RIB development teams; (b) Instructions from vendors related to security notifications; (c) RIB policies regarding availability, security, integrity, protection of personal information, and confidentiality of data in general.

6.4.2. Scheduled Maintenance

RIB performs maintenance activities within the Maintenance Window described in the section below. Maintenance performed by Microsoft on the Azure platform is excluded from the provisions in this SLA, and Microsoft is exclusively responsible for any maintenance activities on the Azure platform.

RIB will perform Scheduled Maintenance activities in order to safeguard the integrity, availability and consistency of the Application. RIB shall make its best efforts to perform the scheduled maintenance during the Maintenance Window. Scheduled maintenance includes, but is not limited to, security updates and patches as provided by Microsoft which are automatically applied on a monthly basis.

RIB will notify the Customer 24 hours in advance of any Scheduled Maintenance

where downtime is expected. Where no downtime is expected RIB will continue without notification.

Maintenance Window with allowed downtime (Production Systems)
Weekdays, 18:00 to 07:00 and Weekends (24hr) from Saturday 00:00 until Monday 00:00 based on the Data Centre where the Application is hosted.

6.4.3. Emergency/Unplanned Maintenance

RIB may be required to perform Emergency Maintenance activities in order to recover or safeguard the integrity availability and consistency of the Application in the future. RIB makes every reasonable attempt to notify the Customer prior to the commencement of the maintenance. In the event that notification is not possible prior to the commencement of the maintenance activities, notification will be provided as soon as possible after the completion of the maintenance activities.

6.5. Data Protection

6.5.1. Daily Backup

RIB is responsible for daily backups and retention of this data as per the table below. Data within the Cloud Platform is retained for a limited amount of time.

Protection SQL Database	Protection Fileshare	Virtual Machine
Minimum 14 days (every 15 minutes a restore point)	Minimum 30 days (every 24 hours a restore point)	Minimum 30 days (every 24 hours a restore point)

6.5.2. Data Restore

Upon Customer's request, Data can be restored from backups. The Customer can request the recovery of data for a specific date as defined in the Daily Backup section above. The restore time may vary depending on the size of the backup. Recovery can be performed for a complete Application or on a file-by-file basis. Recovery times are excluded from the Availability times defined in this SLA.

6.5.3. Recovery point objectives

In case a system or service is unavailable and needs to be restored or recovered, the maximum RPO (recovery point objective) is the maximum amount of time between the most recent copy of the data and the time at which the Incident occurs.

Maximum RPO
24 Hours

6.6. Availability and Disaster Recover

6.6.1. RIB can offer different architectures and solutions in order to give protection for various disaster scenarios. This SLA offers by default the following protection level and availability guarantee:

Protection Level	Availability
Protection for hardware failures within an Azure Data Centre	99.00%

6.6.2. Protection for unavailability of a complete Azure Data Centre within an Azure region or the unavailability of a complete Azure region either due to an incident or unplanned maintenance, are excluded from this SLA.

6.6.3. Next to the architecture, the operational tasks that need to be executed and the priority given determine how long it will take to recover the full service. This is measured in the Recovery Time objective (RTO): how long does it take to recover the service from the moment the service became unavailable in case of a disaster as described in the Protection levels.

Recovery Time Objective (RTO)
Best Effort

6.6.4. For disasters outside of the architecture per the chosen Protection Level, the RTO is based on best effort by default.

6.7. Monitoring

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

6.7.1. Health Monitoring

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.

6.7.2. Availability Monitoring

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

6.8. Release Management

6.8.1. In order to ensure that the individual services are always compatible with each other and deliver the intended function, release management includes the actual Application in combination with all components and services of the Cloud Platform used by RIB to host the Application. RIB is responsible for release management and carries out releases accordingly.

6.8.2. The Application release cycles are as specified by the RIB. When RIB declares features or versions unsupported then RIB will no longer offer the service per this SLA. A specific Out-of-Support SLA may be offered in specific circumstances and different fees will apply.

6.8.3. For any Commercially Released Version, RIB supports the current last three Minor Releases of the Application (a release family) e.g. V6.1 is the current Minor Release, V6.0 and V5.2 are the previous Minor Releases. Any updates for permanent Incident resolution will always be released as part of (i) the next Minor Release of the supported Release versions or (ii) update of a current Minor Release version. Customer may choose to upgrade the Application within the release family; however, if a Customer's Application falls behind and is on an unsupported release family, RIB is entitled to implement an upgrade of the Application to the most current release family to ensure Customer's access to the latest features as well as the latest security, performance, and availability benefits.

6.8.4. Details of which version are currently supported and when support will be stopped for previous version are published under announcements in the Documentation published with each new Commercially Released Version and could be accessed from the documentation menu in the application.

6.8.5. A specific Out-of-Support SLA may be offered in specific circumstances and different fees will apply.

6.9. Escalation

6.9.1. The escalation path will be communicated by your local RIB or RIB Service Provide Customer Success Manager. The Customer Success Manager can also be contacted when support is needed within the escalation process.

6.9.2. The parties can appoint an Escalation Manager respectively who will be responsible for communication during the escalation process. The Escalation Managers will temporarily own the Incident and have the mandate to deploy adequate resources to resolve the Incident as swiftly as possible. De-escalation is completed when parties reach mutual agreement that the Incident has been resolved, and the parties move to close the Incident.

6.10. Security & Vulnerability Management

6.10.1. Compliance/Security

RIB uses policies and procedures to prevent unauthorized physical and logical access to the cloud computing services used by RIB to host the Application on the Cloud Platform in order to protect Customer data in accordance with current cybersecurity standards, regulations, and guidelines as prescribed by the RIB Information Security Policy and the RIB Cybersecurity Policy for Products and Systems.

RIB is committed to:

a) Having a management control framework to give assurance on the availability,

information security and continuity commitments as set out in this SLA.

b) InTWO, a 100% subsidiary of RIB, is responsible for the management and operation of the cloud computing services used by RIB to host the Application on the Cloud Platform.

- InTWO is a member of several Microsoft programs, enrolled in the Global Expert Management Service Provider program, holds various Microsoft Gold & Silver cloud certificates and is a member of the Azure Elite Group.
- InTWO conducts an annual security audit for SOC I Type 2 by an accredited external party, this validates the design of the control framework as well as its existence and operational effectiveness.
- The following certificate are provided by Microsoft Azure with respect to its standard cloud infrastructure on which RIB host the Application: ISO/IEC 27001:2013, ISO/IEC 27017 and 27018 and German Federal Cyber Security Authority – Basic IT Protection in place .
- A detailed list of all Microsoft certifications can be found at the following Microsoft websites as may be evolved by Microsoft at its discretion overtime: Microsoft Trust Centre (https://servicetrust.microsoft.com) or Microsoft Compliance Offerings (https://docs.microsoft.com/en-gb/compliance/regulatory/offering-home?view=o365-worldwide)

6.10.2. 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 fix a vulnerability, with clear ownership and reporting of actions and progress until the action plan is realized in accordance with a vulnerability level and no longer than:

Vulnerability Definition		Resolution	VSS Score
Rating	Description		
Severe	Any vulnerabilities with a major impact that require only remote access to exploit.	A hot fix will be provided where feasible and provided in next release or service pack which may be extended to the last two releases.	VSS between 75 and 100% severity level 4
High	Any vulnerabilities with a major impact that require local network access to exploit.	A fix will be provided in the release or service pack where feasible.	VSS between 50 and 74% severity level 3
Medium	Any vulnerability with a minor impact or that requires local-server access to exploit.	Best effort will be made to provide a fix within the next release.	VSS between 25 and 49% severity level 2
Low	Vulnerability that are withdrawn or for information only or that have no impact.	No action required	VSS between 0 and 24% severity level 1

A vulnerability is defined as “non-critical” if it has a severity level “1 -LOW”. or “2 -MEDIUM”.A vulnerability is defined as “critical” if it has a severity level “3 -HIGH” or“4 –SEVERE”.

A temporary mitigation solution, such as a hotfix or reconfiguration, shall be implemented for level 4 – SEVERE vulnerabilities, where feasible, to reduce risk until a proper fix is defined and implemented.

- Impact is assessed on a number of factors including CVSS score, data/business criticality, perimeter, involved actors, number of affected users/assets, and disclosure/discovery in the public domain.
- Major Impact has a VSS score of above 50%.
- Minor Impact has a VSS score of between 0 and 49%.

6.11. Disclaimers

RIB shall not bear any obligation to provide support and/or maintenance for Defects that cannot be reproduced, nor for Incidents caused by:

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 or linkages or technical interfaces of the Application with third party systems or software;

c) changes to Customer's internal security policies;

d) changes to browser, operating system or Customer Systems by 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, such as 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 or other instructions to use provided to Customer by RIB or otherwise 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) Customer's non-compliance with one or more of its obligations defined in this SLA or with any operation or maintenance instructions provided by RIB in relation to the Application, such as but not limited the continued use of the Application in its prior version after its Commercially Released Version is made available to Customer by RIB;

i) actions, omissions (such as but not limited to Customer's failure to provide information) or erroneous instructions delivered by Customer to RIB;

j) errors due to 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; or

m) Force Majeure and any other situations that cannot be attributed to RIB.

n) DDoS (Distributed Denial of Service) that makes and online service, network resources or host machine unavailable to it 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 caused 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 of the Customers applications with the Application.

RIB cannot warrant that the Application will be free of vulnerabilities or 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 Section 6.10, RIB shall not bear any obligation to provide support and/or maintenance for Incidents nor any liability resulting from limitations or delays in the Application, which are due to telecommunication networks, the internet or Cyber Threats.

6.12. Termination

Unavailability shall not constitute a breach by RIB to its obligations under the Agreement with the Customer and shall therefore not trigger the Customer's right to terminate the Agreement for breach unless **Unavailability exceeds the following values:**

a) Unavailability is experienced during a cumulated period of non-consecutive **six months in a 12-month period**

b) **Unavailability is experienced** for **four consecutive months**

c) **Unavailability reaches** at least **96.5%** of the time other than periods of Excused Outages (3 consecutive months)

d) **Unavailability reaches at least 90%** of the time, other than periods of Excused Outages (2 consecutive months).