

RIB Product Lifecycle Policy

First publication:	November 2025
Current publication:	November 2025
Version:	V1.0
SE Reference Version:	N/A
Document type:	Policy
Scope:	RIB Unify Product

Copyright © 2025 by RIB Software GmbH and it's subsidiaries.

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.

Policy name

RIB Product Lifecyle Policy

Purpose and objectives

This Software Lifecycle Policy establishes RIB's principles and requirements for managing software products and services throughout their complete lifecycle, ensuring regulatory compliance, customer protection, and operational effectiveness.

Audience

All RIB employees and contractors involved in software product development, support, sales, or customer management for RIB Unify.

Confidentiality Status

Public.

Local adaptation authorization

No adaptations allowed

References

RIB Unify Product Lifecycle Standard

Policy Owner

Jakob Pichlmayr, Vice President, Innovation SaaS Product Portfolio

Policy Approver

Rolf Helmes, Global Chief Product Officer

Content

1. INTRODUCTION 4

1.1 SCOPE 4
1.2 EXCLUSIONS 4
1.3 DISCLAIMER 4

2. PRINCIPLES 4

3. LIFECYCLE REQUIREMENTS 5

3.1 PILOT PHASE 5
3.2 GENERAL AVAILABILITY 5
3.3 END-OF- SALES 5
3.6 END-OF-LIFE 5

4. EMERGENCY PROVISIONS 6

5. DECISION-MAKING REQUIREMENTS 6

5.1 ASSESSMENT CRITERIA 6
5.2 GOVERNANCE 6
5.3 EXCEPTION PROCESS 7
5.4 DOCUMENTATION 7

6. COMPLIANCE AND ENFORCEMENT 7

6.1 REGULATORY COMPLIANCE 7
6.2 POLICY ENFORCEMENT 7

7. IMPLEMENTATION 8

7.1 OWNERSHIP 8
7.2 STANDARDS AND PROCEDURES 8
7.3 REVIEW AND UPDATES 8

8. DOCUMENT REVISIONS 8

1. Introduction

This Product Lifecycle Policy establishes RIB's principles and requirements for managing software products and services throughout their complete lifecycle, ensuring regulatory compliance, customer protection, and operational effectiveness.

1.1 Scope

This policy applies to the following RIB software products and services throughout their complete lifecycle, from Pilot phase through to End-of-Life:

1. RIB Unify
2. RIB Unify mobile applications

1.2 Exclusions

This policy does not apply to:

- Internal development or testing versions not released to customers
- Individual feature deprecations within actively supported products

1.3 Disclaimer

- This Policy applies only where the customer holds a valid subscription or maintenance agreement and operates in a supported configuration.
- RIB shall not be liable for damages, costs, or losses arising from use of software versions that have reached End-of-Life, e.g., the software products/versions have been retired or where software development efforts are no longer available.
- RIB reserves the right to modify, update, or discontinue any product or software version at its sole discretion.
- This Policy may be revised by RIB at any time without prior notice.
- This Policy applies exclusively to RIB products. It does not extend to third-party software, integrations, or customer-specific customisations.

2. Principles

Customer Protection

RIB will provide customers with adequate advance notice and support during product lifecycle transitions to minimize business disruption.

Regulatory Compliance

All lifecycle decisions must comply with applicable regulatory frameworks, including the EU Cyber Resilience Act and other relevant legislation.

Transparency

Lifecycle decisions and timelines will be communicated clearly and consistently to affected stakeholders.

Business Flexibility

While maintaining customer commitments, RIB reserves the right to adapt lifecycle timelines based on technical, regulatory, or business circumstances.

3. Lifecycle Requirements

3.1 Pilot Phase

- Limited customer access with clear identification as pre-production
- Basic technical support with best-effort availability
- Regular updates on development progress

Pilot Discontinuation: Products that do not proceed from pilot to General Availability may be discontinued with reasonable notice to pilot participants without following the full End-of-Life process outlined in section 3.4 End-of-Life

3.2 General Availability

- Standard commercial availability
- Full production support as per Service Level Agreement (SLA)
- Regular maintenance updates and security patches
- Compliance with all applicable regulatory requirements

3.3 End-of-Sales

- Recommended Notice Period: End-of-Sales should take immediate effect
- New Customer restrictions: Product no longer available for new customer acquisition
- Existing Customer Continuity: Current customers may continue to renew and expand within stated limitations
- Support Continuation: Full support maintained per existing SLA terms
- Product Updates: Regular maintenance updates and security patches

3.4 End-of-Life

Minimum Notice Period: 6 months advance notice before End-of-Life

During the Notice Period:

- New Customer Restrictions: Product not available for new customer acquisition
- Existing Customer Continuity: Current customers may continue to renew and expand within stated limitations
- Support: At a minimum, support provided for data migration and security updates

- Updates: At a minimum, any updates required to facilitate data migration and security patches

After the Notice Period:

- New Customer Restrictions: Product not available for new customer acquisition
- Existing Customer Restrictions: Product not available for renewal of existing subscriptions
- No Support: No support provided for product
- No Updates: Product environments are decommissioned and cannot be updated

4. Emergency Provisions

RIB reserves the right to accelerate standard timelines in cases of:

- Critical security vulnerabilities that cannot be remediated
- Regulatory or legal requirements mandating immediate action
- Third-party dependency failures beyond RIB's control
- Force majeure events

In such cases, RIB will provide immediate notification and expedited transition assistance.

5. Decision-Making Requirements

5.1 Assessment Criteria

Lifecycle decisions must consider:

- Customer expectations and business impact
- Contractual obligations to customers and partners
- Product nature, intended purpose, and usage patterns
- Technical viability
- Security requirements
- Third-party dependencies, integrations, and their lifecycles
- Regulatory compliance obligations
- Industry benchmarks for products with similar functionality
- Business and competitive factors
- Availability of alternative solutions within our portfolio

5.2 Governance

- Cross-functional review by stakeholders as defined in section 7.1 is required for all lifecycle decisions.
- Executive approval is required for all lifecycle decisions.
- The exception approval process must be followed for any deviation from standard timelines.

5.3 Exception Process

All exceptions to the standard lifecycle process must meet the following requirements.

- Risk Assessment: An analysis of customer, legal, compliance, and business risks must be documented.
- Business Justification: A clear business rationale for not meeting the standard requirements must be documented.
- Mitigation Measures: Actions taken to minimize negative impacts.
- Legal Review: All exceptions must undergo legal review prior to executive review.
- Approval Authority: All exceptions require Executive Management approval.
- Customer Communication: Documented plan for informing affected customers of changes.

5.4 Documentation

- Decision rationale must be documented per regulatory requirements.
- Compliance verification must be included in the product's conformity assessment technical documentation.
- All exceptions must be documented with full rationale and approval records.

6. Compliance and Enforcement

6.1 Regulatory Compliance

- This policy provides an approach for compliance with the requirements of the EU's Cyber Resilience Act Article 13(8) requirements for product lifecycles.
- Security vulnerability assessment and remediation must occur throughout the support lifecycle.
- Technical documentation for the support period must be kept and reviewed at least annually.

6.2 Policy Enforcement

- Product Security will conduct periodic reviews to monitor compliance with this policy.
- Independent verification will be done in accordance with our CRA conformity assessment framework.
- Regular audits of lifecycle processes must be conducted at least annually to validate:
    - Where product transitions have occurred, that they have been in conformance with this policy.
    - That products covered by this policy have reviewed their support periods to ensure they meet the current policy standards and any updated regulatory guidance.
- Exceptions must be tracked as part of the compliance program.
- Compliance reports must be provided to executive management at least annually.

7. Implementation

7.1 Ownership

Process Owner: Product Management team
Compliance Monitoring: Internal Compliance team
Stakeholders: Legal, Customer Care, Customer Success, Development, Quality Engineering, Product Security, Sales, Strategy, Managed Services

7.2 Standards and Procedures

Detailed implementation standards and procedures are documented separately and may be updated to reflect operational requirements and regulatory changes without requiring policy revision.

7.3 Review and Updates

This policy must be reviewed annually and updated as necessary to maintain regulatory compliance and business effectiveness.

8. Document Revisions

Revision	Date	Drafted by	Type of Revision
0.9	November 4, 2025	Gareth Marshall	Final draft
1.0	November 18, 2025	Gareth Marshall	Reviewed
1.0	November 24, 2025	Rolf Helmes	Approved