Raiffeisen Bank Kosovo J.S.C. Procurement Terms and Conditions

Version 2.0 | Date: 2026-08-01

Executive Summary

Raiffeisen Bank Kosovo J.S.C. requires Suppliers to operate with high standards of compliance, security, data protection, and ethical conduct. These T&Cs set mandatory baselines in the areas of purchase control, delivery and acceptance, pricing and payment, warranties, IP ownership, information security, data protection, business continuity, regulatory audit access, and termination and exit. Annexes provide templates—SOW, POE, subcontractor approval—and checklists covering security and ESG obligations. The document is structured to align with Kosovo law and Raiffeisen Bank Kosovo J.S.C.'s regulatory environment.

Table of Contents (update in Word)

- 1. Definitions and Interpretation
- 2. Purchase Orders and Contract Formation
- 3. Scope of Work and Changes
- 4. Delivery, Acceptance, and Rejection
- 5. Pricing, Taxes, and Invoicing
- 6. Payment Terms and Set-Off
- 7. Proof of Execution (POE)
- 8. Personnel, Subcontracting, and Vetting
- 9. Compliance, Ethics, and Anti-Corruption
- 10. Information Security and Data Protection
- 11. Business Continuity and Disaster Recovery
- 12. Intellectual Property Rights and Licensing
- 13. Warranties and Remedies
- 14. Liability, Indemnity, and Insurance
- 15. Confidentiality and Records
- 16. Audit Rights and Regulatory Access
- 17. Term, Termination, and Exit
- 18. Governing Law and Dispute Resolution
- 19. General Provisions
- Annexes: A–F

1. Definitions and Interpretation

Definitions and Interpretation. The capitalized terms used in these T&Cs have the meanings set out below or in the relevant SOW or PO. Headings are for convenience only and do not affect interpretation. The singular includes the plural and vice versa. References to a law include that law as amended, consolidated, or re-enacted from time to time. In the event of a conflict, the following order of precedence applies: (1) a duly executed master agreement; (2) a SOW; (3) these T&Cs; and (4) a PO, unless the PO expressly states otherwise.

- "Affiliate" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Affiliate encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- "Agreement" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Agreement encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- "Applicable Law" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Applicable Law encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- "Background IP" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Background IP encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- "Business Day" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Business Day encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- "Change Order" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Change Order encompass equivalent concepts used in related Raiffeisen Bank

Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.

- "Confidential Information" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Confidential Information encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- "Controller" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Controller encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- "Data Breach" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Data Breach encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- "Data Protection Laws" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Data Protection Laws encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- "Deliverables" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Deliverables encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- "Dispute" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Dispute encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- "Fees" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires,

references to Fees encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.

- "Foreground IP" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Foreground IP encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- "Good Industry Practice" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Good Industry Practice encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- "Incident" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Incident encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- "Intellectual Property Rights" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Intellectual Property Rights encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- "Invoice" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Invoice encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- "Personal Data" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Personal Data encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- "PO (Purchase Order)" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for

financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to PO (Purchase Order) encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.

- "POE (Proof of Execution)" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to POE (Proof of Execution) encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- "Processing" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Processing encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- "Processor" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Processor encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- "Regulator" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Regulator encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- "Sanctions" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Sanctions encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- "Security Controls" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Security Controls encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.

- “Services” means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Services encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- “SLA (Service Level Agreement)” means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to SLA (Service Level Agreement) encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- “SOW (Statement of Work)” means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to SOW (Statement of Work) encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- “Subcontractor” means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Subcontractor encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- “Term” means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Term encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- “Termination” means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Termination encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- “Third-Party Software” means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Third-Party Software encompass equivalent concepts used in related

Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.

- "Transition Assistance" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Transition Assistance encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- "VAT" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to VAT encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- "Warranty" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Warranty encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.
- "Work Product" means the concept customarily understood by that term within commercial contracts, as applied to these T&Cs, and includes the nuances necessary for financial services outsourcing, data protection, and security. Unless the context otherwise requires, references to Work Product encompass equivalent concepts used in related Raiffeisen Bank Kosovo J.S.C. policies, standards, and local law, and do not limit broader obligations expressly stated elsewhere.

2. Purchase Orders and Contract Formation

No work shall commence until an approved Purchase Order (PO) is issued by Raiffeisen Bank Kosovo J.S.C.. Each PO constitutes an offer to purchase and is accepted by the Supplier upon the earlier of (a) written acceptance or (b) commencement of performance. Any terms in Supplier quotations or order acknowledgements that are inconsistent with these T&Cs are expressly rejected and shall be of no effect.

The PO must accurately reference the scope, deliverables, service locations, delivery dates, agreed pricing, currency, and applicable taxes. Raiffeisen Bank Kosovo J.S.C. is under no obligation to pay for goods or services delivered without a valid PO or that deviate from the PO or SOW without prior written approval.

3. Scope of Work and Changes

The Supplier shall deliver the goods and/or perform the services described in the applicable SOW or PO, including all deliverables, milestones, and acceptance criteria. Changes to the scope must be agreed through a written change order that specifies impacts on cost, time, and quality. The Supplier shall not unreasonably withhold or delay agreement to a change requested by Raiffeisen Bank Kosovo J.S.C..

If a change results from Supplier's failure to meet agreed requirements, the Supplier shall implement the change at no additional cost to Raiffeisen Bank Kosovo J.S.C.. Raiffeisen Bank Kosovo J.S.C. may request de-scoping, substitution of equivalent items, or rescheduling in line with business needs, provided that any resulting price adjustments are fair and reflect avoided costs.

4. Delivery, Acceptance, and Rejection

Delivery shall occur in accordance with the agreed Incoterms (if applicable) and dates. Time is of the essence. The Supplier must notify Raiffeisen Bank Kosovo J.S.C. immediately of any actual or anticipated delay and propose a mitigation plan at no cost to Raiffeisen Bank Kosovo J.S.C.. Risk of loss transfers upon formal written acceptance by Raiffeisen Bank Kosovo J.S.C., unless otherwise set out in a master agreement.

Raiffeisen Bank Kosovo J.S.C. will conduct acceptance testing or inspection within a reasonable period after delivery. If goods or services fail to conform to the specifications, Raiffeisen Bank Kosovo J.S.C. may reject them and require prompt repair, replacement, or reperformance at the Supplier's cost, or obtain a refund. Acceptance shall not waive latent defects, fraud, or misrepresentation.

5. Pricing, Taxes, and Invoicing

All prices are firm, fixed, and inclusive of all costs, charges, and expenses necessary to perform the contract unless expressly stated otherwise. The Supplier shall issue accurate invoices referencing the PO number, line items, quantities, unit prices, tax breakdowns, service periods, and the applicable Proof of Execution (POE) documentation.

Invoices that are incomplete, inaccurate, duplicative, or unsupported by POE may be returned or rejected. Raiffeisen Bank Kosovo J.S.C. may withhold contested amounts pending resolution, without prejudice to its rights and remedies. The Supplier warrants that prices are no less favorable than those offered to similarly situated customers for comparable scope, quantity, and terms.

6. Payment Terms and Set-Off

Unless otherwise agreed in writing, payment terms are Net 30 days from receipt of a valid, undisputed invoice and required POE. Raiffeisen Bank Kosovo J.S.C. may set-off any amounts

due from the Supplier against amounts payable to the Supplier. Early payment shall not constitute acceptance of non-conforming goods or services.

If Raiffeisen Bank Kosovo J.S.C. is required by law to withhold any taxes from payments, it will do so and provide reasonable evidence of such withholding. The parties shall cooperate on obtaining applicable tax exemptions or reduced withholding rates where available under law or treaty.

7. Proof of Execution (POE)

As a condition precedent to payment, the Supplier shall provide POE appropriate to the engagement, such as delivery receipts, service completion certificates, timesheets, acceptance reports, or other auditable evidence. POE must clearly tie to the PO and demonstrate performance in accordance with scope and quality requirements.

Raiffeisen Bank Kosovo J.S.C. may request supplemental documentation, including logs, test results, and sign-offs, to validate performance. Failure to provide POE in a timely manner may result in delayed or withheld payment without liability to Raiffeisen Bank Kosovo J.S.C..

8. Personnel, Subcontracting, and Vetting

The Supplier remains fully responsible for the performance of all personnel, including subcontractors. Subcontracting of any material portion requires Raiffeisen Bank Kosovo J.S.C.'s prior written consent. The Supplier shall ensure that subcontractors are bound by obligations no less protective than these T&Cs and shall remain liable for their acts and omissions.

Where services are performed on Raiffeisen Bank Kosovo J.S.C. premises or systems, Supplier personnel must complete onboarding, comply with site rules, pass background checks permitted by law, and complete mandatory training. Raiffeisen Bank Kosovo J.S.C. may request removal and replacement of any personnel for reasonable cause.

9. Compliance, Ethics, and Anti-Corruption

The Supplier shall comply with all applicable laws and Raiffeisen Bank Kosovo J.S.C. policies communicated to the Supplier, including anti-bribery and corruption, anti-money laundering, sanctions, competition law, export controls, and human rights. The Supplier shall not offer, give, request, or accept any bribe, kickback, or improper advantage, including facilitation payments.

Gifts and hospitality must be modest, infrequent, and lawful. The Supplier shall maintain accurate books and records that fairly reflect transactions and shall promptly report suspected violations to Raiffeisen Bank Kosovo J.S.C.. Raiffeisen Bank Kosovo J.S.C. may immediately terminate for material compliance breaches.

10. Information Security and Data Protection

If the Supplier processes personal data on behalf of Raiffeisen Bank Kosovo J.S.C., the parties shall execute a data processing agreement consistent with the GDPR and applicable local laws. The Supplier shall implement technical and organizational measures aligned to recognized frameworks (e.g., ISO/IEC 27001) to protect Confidential Information and systems against unauthorized access, loss, or alteration.

Security incidents affecting Raiffeisen Bank Kosovo J.S.C. data or services must be reported to Raiffeisen Bank Kosovo J.S.C. without undue delay and within legally required timelines, accompanied by facts, impact assessment, containment measures, and remediation plans. The Supplier shall support audits, penetration tests (as applicable), and corrective actions.

11. Business Continuity and Disaster Recovery

The Supplier shall maintain and test business continuity and disaster recovery (BC/DR) plans proportionate to the criticality of the services. Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) shall meet or exceed the values specified in the SOW. Raiffeisen Bank Kosovo J.S.C. may review test summaries and request corrective measures where gaps are identified.

In the event of a disruption, the Supplier shall prioritize restoration of Raiffeisen Bank Kosovo J.S.C. services, communicate status at agreed intervals, and provide root-cause analyses. Costs arising from failure to maintain adequate BC/DR capabilities shall be borne by the Supplier.

12. Intellectual Property Rights and Licensing

Each party retains ownership of its Background IP. Unless otherwise stated, Raiffeisen Bank Kosovo J.S.C. owns all Foreground IP created specifically for Raiffeisen Bank Kosovo J.S.C. under the engagement upon creation. The Supplier hereby assigns, and shall procure assignment by its personnel and subcontractors of, all right, title, and interest in such Foreground IP to Raiffeisen Bank Kosovo J.S.C., and shall execute documents necessary to perfect ownership.

For Supplier materials embedded in deliverables, the Supplier grants Raiffeisen Bank Kosovo J.S.C. a perpetual, worldwide, transferable, sublicensable, royalty-free license to use, reproduce, adapt, and distribute such materials as necessary for Raiffeisen Bank Kosovo J.S.C.'s internal business purposes. Open-source components shall be disclosed in a bill of materials and used in compliance with applicable licenses.

13. Warranties and Remedies

The Supplier warrants that goods are new and free from defects in design, material, and workmanship, and that services will be performed in a professional and workmanlike manner by appropriately skilled personnel, in accordance with industry standards. Deliverables shall conform to specifications and documentation.

In case of breach of warranty, the Supplier shall promptly repair, replace, or reperform at its cost. If the Supplier fails to cure within a reasonable time, Raiffeisen Bank Kosovo J.S.C. may obtain substitute performance and recover the associated costs, or receive an appropriate price reduction or refund, without prejudice to other remedies.

14. Liability, Indemnity, and Insurance

The Supplier shall indemnify, defend, and hold harmless Raiffeisen Bank Kosovo J.S.C., its affiliates, and their respective directors, officers, and employees from and against claims, losses, liabilities, damages, costs, and expenses (including reasonable legal fees) arising out of (a) third-party claims alleging IP infringement; (b) personal injury or property damage caused by Supplier; (c) breach of law or these T&Cs; or (d) data protection or confidentiality breaches attributable to Supplier.

Except for liability that cannot be limited under applicable law, the parties' aggregate liability under these T&Cs shall be subject to a reasonable cap stated in the SOW or PO (e.g., 100% of fees paid or payable in the 12 months preceding the event). The Supplier shall maintain insurance coverage (e.g., commercial general liability, professional indemnity, cyber) with reputable insurers and provide certificates upon request.

15. Confidentiality and Records

'Confidential Information' means non-public information disclosed by a party that is identified as confidential or that should reasonably be understood as confidential, including business plans, financial data, customer information, source code, and security documentation. The receiving party shall protect Confidential Information using at least the same degree of care as it uses to protect its own information of similar importance, but in no event less than a reasonable standard of care.

Confidentiality obligations do not apply to information that is or becomes public through no fault of the receiving party, is independently developed, or is rightfully obtained from a third party without obligation of confidentiality. Obligations survive termination for at least five (5) years, or longer for trade secrets and personal data as required by law.

16. Audit Rights and Regulatory Access

Raiffeisen Bank Kosovo J.S.C. may audit the Supplier's compliance with these T&Cs, including review of security controls, POE, invoices, and delivery records, upon reasonable notice. The Supplier shall cooperate fully and address findings within agreed timelines. Where services constitute outsourcing under applicable banking regulations, the Supplier shall facilitate access by Raiffeisen Bank Kosovo J.S.C.'s regulators and auditors to relevant information, subject to reasonable confidentiality and security controls.

The Supplier shall maintain complete and accurate records for at least seven (7) years from the later of performance or termination, or longer if required by law or regulator guidance.

17. Term, Termination, and Exit

Raiffeisen Bank Kosovo J.S.C. may terminate for convenience upon written notice, without cause, in which case Raiffeisen Bank Kosovo J.S.C. shall pay for conforming goods and services delivered up to the effective date and reasonable, properly documented demobilization costs. Either party may terminate for cause if the other commits a material breach and fails to cure within thirty (30) days after notice, or immediately in case of insolvency events.

Upon termination or expiry, the Supplier shall provide orderly transition assistance for up to ninety (90) days (or as agreed) to mitigate business disruption, including knowledge transfer, handover of assets, and data return or deletion certificates.

18. Governing Law and Dispute Resolution

These T&Cs and any disputes arising out of or in connection with them are governed by the laws of Kosovo, without regard to conflict-of-law rules. The parties shall seek to resolve disputes amicably through good-faith negotiations and, if necessary, mediation.

If unresolved, disputes shall be finally settled by aRaiffeisen Bank Kosovo J.S.C.tration under the Vienna Rules before a panel of one or three aRaiffeisen Bank Kosovo J.S.C.trators seated in Vienna, Kosovo. The language of the proceedings shall be English or German, as elected by Raiffeisen Bank Kosovo J.S.C..

19. General Provisions

Notices shall be in writing and delivered by reputable courier, registered mail, or email to the addresses specified in the SOW or PO. Assignment requires the other party's prior written consent, except that Raiffeisen Bank Kosovo J.S.C. may assign to an affiliate. No waiver is effective unless in writing. If any provision is held invalid, the remainder remains in effect. The parties may execute counterparts, including via electronic signature.

These T&Cs, together with the SOW and PO, constitute the entire agreement with respect to the subject matter and supersede prior understandings. Amendments must be in writing and signed by authorized representatives. Provisions that by their nature should survive termination shall so survive.

Annex A: Information Security Requirements

The Supplier shall implement and maintain a comprehensive information security program aligned with ISO/IEC 27001 or an equivalent framework, proportionate to the risk and criticality

of the services. The following control domains describe minimum expectations and reporting obligations.

Access Control

- The Supplier shall establish documented policies and procedures for access control, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for access control must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that access control applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where access control relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of access control assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Identity and Authentication

- The Supplier shall establish documented policies and procedures for identity and authentication, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for identity and authentication must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that identity and authentication applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where identity and authentication relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of identity and authentication assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Privileged Access Management

- The Supplier shall establish documented policies and procedures for privileged access management, review them at least annually, and ensure they are approved by accountable leadership.

- Controls for privileged access management must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that privileged access management applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where privileged access management relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of privileged access management assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Network Security

- The Supplier shall establish documented policies and procedures for network security, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for network security must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that network security applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where network security relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of network security assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Endpoint Protection

- The Supplier shall establish documented policies and procedures for endpoint protection, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for endpoint protection must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that endpoint protection applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where endpoint protection relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.

- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of endpoint protection assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Vulnerability Management

- The Supplier shall establish documented policies and procedures for vulnerability management, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for vulnerability management must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that vulnerability management applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where vulnerability management relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of vulnerability management assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Patch Management

- The Supplier shall establish documented policies and procedures for patch management, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for patch management must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that patch management applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where patch management relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of patch management assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Malware Defense

- The Supplier shall establish documented policies and procedures for malware defense, review them at least annually, and ensure they are approved by accountable leadership.

- Controls for malware defense must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that malware defense applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where malware defense relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of malware defense assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Email Security

- The Supplier shall establish documented policies and procedures for email security, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for email security must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that email security applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where email security relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of email security assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Data Loss Prevention

- The Supplier shall establish documented policies and procedures for data loss prevention, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for data loss prevention must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that data loss prevention applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where data loss prevention relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.

- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of data loss prevention assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Encryption at Rest

- The Supplier shall establish documented policies and procedures for encryption at rest, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for encryption at rest must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that encryption at rest applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where encryption at rest relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of encryption at rest assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Encryption in Transit

- The Supplier shall establish documented policies and procedures for encryption in transit, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for encryption in transit must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that encryption in transit applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where encryption in transit relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of encryption in transit assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Key Management

- The Supplier shall establish documented policies and procedures for key management, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for key management must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.

- The Supplier shall ensure that key management applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where key management relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of key management assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Logging and Monitoring

- The Supplier shall establish documented policies and procedures for logging and monitoring, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for logging and monitoring must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that logging and monitoring applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where logging and monitoring relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of logging and monitoring assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

SIEM Integration

- The Supplier shall establish documented policies and procedures for siem integration, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for siem integration must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that siem integration applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where siem integration relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of siem integration assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Incident Response

- The Supplier shall establish documented policies and procedures for incident response, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for incident response must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that incident response applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where incident response relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of incident response assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Threat Intelligence

- The Supplier shall establish documented policies and procedures for threat intelligence, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for threat intelligence must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that threat intelligence applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where threat intelligence relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of threat intelligence assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Secure Development Lifecycle

- The Supplier shall establish documented policies and procedures for secure development lifecycle, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for secure development lifecycle must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.

- The Supplier shall ensure that secure development lifecycle applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where secure development lifecycle relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of secure development lifecycle assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Change Management

- The Supplier shall establish documented policies and procedures for change management, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for change management must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that change management applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where change management relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of change management assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Configuration Management

- The Supplier shall establish documented policies and procedures for configuration management, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for configuration management must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that configuration management applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where configuration management relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.

- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of configuration management assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Backup and Recovery

- The Supplier shall establish documented policies and procedures for backup and recovery, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for backup and recovery must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that backup and recovery applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where backup and recovery relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of backup and recovery assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Resilience and High Availability

- The Supplier shall establish documented policies and procedures for resilience and high availability, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for resilience and high availability must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that resilience and high availability applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where resilience and high availability relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of resilience and high availability assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Third-Party Risk Management

- The Supplier shall establish documented policies and procedures for third-party risk management, review them at least annually, and ensure they are approved by accountable leadership.

- Controls for third-party risk management must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that third-party risk management applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where third-party risk management relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of third-party risk management assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Physical Security

- The Supplier shall establish documented policies and procedures for physical security, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for physical security must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that physical security applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where physical security relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of physical security assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Cloud Security Posture

- The Supplier shall establish documented policies and procedures for cloud security posture, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for cloud security posture must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that cloud security posture applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where cloud security posture relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.

- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of cloud security posture assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Container Security

- The Supplier shall establish documented policies and procedures for container security, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for container security must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that container security applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where container security relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of container security assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

API Security

- The Supplier shall establish documented policies and procedures for api security, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for api security must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that api security applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where api security relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of api security assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Segregation of Duties

- The Supplier shall establish documented policies and procedures for segregation of duties, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for segregation of duties must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.

- The Supplier shall ensure that segregation of duties applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where segregation of duties relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of segregation of duties assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

User Awareness Training

- The Supplier shall establish documented policies and procedures for user awareness training, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for user awareness training must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that user awareness training applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where user awareness training relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of user awareness training assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Penetration Testing

- The Supplier shall establish documented policies and procedures for penetration testing, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for penetration testing must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that penetration testing applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where penetration testing relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.

- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of penetration testing assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Red Team Exercises

- The Supplier shall establish documented policies and procedures for red team exercises, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for red team exercises must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that red team exercises applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where red team exercises relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of red team exercises assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Zero Trust Architecture

- The Supplier shall establish documented policies and procedures for zero trust architecture, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for zero trust architecture must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that zero trust architecture applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where zero trust architecture relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of zero trust architecture assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Micro-Segmentation

- The Supplier shall establish documented policies and procedures for micro-segmentation, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for micro-segmentation must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.

- The Supplier shall ensure that micro-segmentation applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where micro-segmentation relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of micro-segmentation assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Certificate Management

- The Supplier shall establish documented policies and procedures for certificate management, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for certificate management must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that certificate management applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where certificate management relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of certificate management assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Secrets Management

- The Supplier shall establish documented policies and procedures for secrets management, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for secrets management must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that secrets management applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where secrets management relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.

- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of secrets management assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Remote Access Security

- The Supplier shall establish documented policies and procedures for remote access security, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for remote access security must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that remote access security applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where remote access security relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of remote access security assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Mobile Device Management

- The Supplier shall establish documented policies and procedures for mobile device management, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for mobile device management must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that mobile device management applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where mobile device management relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of mobile device management assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Bring Your Own Device (BYOD)

- The Supplier shall establish documented policies and procedures for bring your own device (byod), review them at least annually, and ensure they are approved by accountable leadership.

- Controls for bring your own device (byod) must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that bring your own device (byod) applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where bring your own device (byod) relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of bring your own device (byod) assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Data Classification

- The Supplier shall establish documented policies and procedures for data classification, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for data classification must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that data classification applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where data classification relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of data classification assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Retention and Disposal

- The Supplier shall establish documented policies and procedures for retention and disposal, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for retention and disposal must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that retention and disposal applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where retention and disposal relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.

- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of retention and disposal assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Monitoring of Critical Services

- The Supplier shall establish documented policies and procedures for monitoring of critical services, review them at least annually, and ensure they are approved by accountable leadership.
- Controls for monitoring of critical services must be risk-based, measured via KPIs and KRIs, and supported by evidence suitable for Raiffeisen Bank Kosovo J.S.C. audits, including logs, reports, and configuration baselines.
- The Supplier shall ensure that monitoring of critical services applies consistently across production, test, development, and disaster-recovery environments, with segregation preventing unauthorized propagation of risk.
- Where monitoring of critical services relies on third-party services, the Supplier shall assess and monitor those dependencies, implement compensating controls, and maintain exit strategies to mitigate concentration risk.
- The Supplier shall provide Raiffeisen Bank Kosovo J.S.C., upon request, with summaries of monitoring of critical services assessments, remediation plans, and target dates, and shall promptly address high or critical findings.

Annex B: Responsible Sourcing, ESG, and DNSH

The Supplier acknowledges Raiffeisen Bank Kosovo J.S.C.'s commitment to responsible sourcing and to the Do No Significant Harm (DNSH) principle under EU sustainability frameworks. The Supplier shall operate in accordance with internationally recognized standards and provide transparent reporting to evidence progress.

- Greenhouse Gas Emissions: The Supplier shall set measurable objectives, maintain action plans, and share annual progress reports upon request. Where feasible, the Supplier shall prioritize low-impact materials, renewable energy, and circular practices, and shall remedy adverse impacts discovered through audits, assessments, or stakeholder feedback.
- Energy Efficiency: The Supplier shall set measurable objectives, maintain action plans, and share annual progress reports upon request. Where feasible, the Supplier shall prioritize low-impact materials, renewable energy, and circular practices, and shall remedy adverse impacts discovered through audits, assessments, or stakeholder feedback.
- Water Stewardship: The Supplier shall set measurable objectives, maintain action plans, and share annual progress reports upon request. Where feasible, the Supplier shall prioritize low-impact materials, renewable energy, and circular practices, and shall remedy adverse impacts discovered through audits, assessments, or stakeholder feedback.
- Waste Reduction: The Supplier shall set measurable objectives, maintain action plans, and share annual progress reports upon request. Where feasible, the Supplier shall prioritize

low-impact materials, renewable energy, and circular practices, and shall remedy adverse impacts discovered through audits, assessments, or stakeholder feedback.

- Circular Economy: The Supplier shall set measurable objectives, maintain action plans, and share annual progress reports upon request. Where feasible, the Supplier shall prioritize low-impact materials, renewable energy, and circular practices, and shall remedy adverse impacts discovered through audits, assessments, or stakeholder feedback.
- Sustainable Packaging: The Supplier shall set measurable objectives, maintain action plans, and share annual progress reports upon request. Where feasible, the Supplier shall prioritize low-impact materials, renewable energy, and circular practices, and shall remedy adverse impacts discovered through audits, assessments, or stakeholder feedback.
- Biodiversity Protection: The Supplier shall set measurable objectives, maintain action plans, and share annual progress reports upon request. Where feasible, the Supplier shall prioritize low-impact materials, renewable energy, and circular practices, and shall remedy adverse impacts discovered through audits, assessments, or stakeholder feedback.
- Do No Significant Harm (DNSH): The Supplier shall set measurable objectives, maintain action plans, and share annual progress reports upon request. Where feasible, the Supplier shall prioritize low-impact materials, renewable energy, and circular practices, and shall remedy adverse impacts discovered through audits, assessments, or stakeholder feedback.
- Human Rights and Labor Standards: The Supplier shall set measurable objectives, maintain action plans, and share annual progress reports upon request. Where feasible, the Supplier shall prioritize low-impact materials, renewable energy, and circular practices, and shall remedy adverse impacts discovered through audits, assessments, or stakeholder feedback.
- Modern Slavery Prevention: The Supplier shall set measurable objectives, maintain action plans, and share annual progress reports upon request. Where feasible, the Supplier shall prioritize low-impact materials, renewable energy, and circular practices, and shall remedy adverse impacts discovered through audits, assessments, or stakeholder feedback.
- Diversity and Inclusion: The Supplier shall set measurable objectives, maintain action plans, and share annual progress reports upon request. Where feasible, the Supplier shall prioritize low-impact materials, renewable energy, and circular practices, and shall remedy adverse impacts discovered through audits, assessments, or stakeholder feedback.
- Supplier Code of Conduct: The Supplier shall set measurable objectives, maintain action plans, and share annual progress reports upon request. Where feasible, the Supplier shall prioritize low-impact materials, renewable energy, and circular practices, and shall remedy adverse impacts discovered through audits, assessments, or stakeholder feedback.
- Ethical Sourcing of Materials: The Supplier shall set measurable objectives, maintain action plans, and share annual progress reports upon request. Where feasible, the Supplier shall prioritize low-impact materials, renewable energy, and circular practices, and shall remedy adverse impacts discovered through audits, assessments, or stakeholder feedback.
- Conflict Minerals: The Supplier shall set measurable objectives, maintain action plans, and share annual progress reports upon request. Where feasible, the Supplier shall prioritize

low-impact materials, renewable energy, and circular practices, and shall remedy adverse impacts discovered through audits, assessments, or stakeholder feedback.

- Community Engagement: The Supplier shall set measurable objectives, maintain action plans, and share annual progress reports upon request. Where feasible, the Supplier shall prioritize low-impact materials, renewable energy, and circular practices, and shall remedy adverse impacts discovered through audits, assessments, or stakeholder feedback.
- Health and Safety: The Supplier shall set measurable objectives, maintain action plans, and share annual progress reports upon request. Where feasible, the Supplier shall prioritize low-impact materials, renewable energy, and circular practices, and shall remedy adverse impacts discovered through audits, assessments, or stakeholder feedback.
- Fair Wages and Working Hours: The Supplier shall set measurable objectives, maintain action plans, and share annual progress reports upon request. Where feasible, the Supplier shall prioritize low-impact materials, renewable energy, and circular practices, and shall remedy adverse impacts discovered through audits, assessments, or stakeholder feedback.
- Anti-Harassment and Non-Discrimination: The Supplier shall set measurable objectives, maintain action plans, and share annual progress reports upon request. Where feasible, the Supplier shall prioritize low-impact materials, renewable energy, and circular practices, and shall remedy adverse impacts discovered through audits, assessments, or stakeholder feedback.
- Transparency and Reporting: The Supplier shall set measurable objectives, maintain action plans, and share annual progress reports upon request. Where feasible, the Supplier shall prioritize low-impact materials, renewable energy, and circular practices, and shall remedy adverse impacts discovered through audits, assessments, or stakeholder feedback.

Annex C: Data Processing Addendum (Summary)

Roles and Responsibilities: Raiffeisen Bank Kosovo J.S.C. acts as Controller and the Supplier acts as Processor for personal data processed under the services, unless otherwise agreed in writing.

Processing Instructions: Supplier shall process personal data only on documented instructions from Raiffeisen Bank Kosovo J.S.C., including with regard to transfers, sub-processing, and retention periods.

Sub-Processing: Sub-processors require Raiffeisen Bank Kosovo J.S.C.'s prior written authorization; Supplier remains liable for their actions. A current list of sub-processors shall be maintained and notified to Raiffeisen Bank Kosovo J.S.C..

Security Measures: Supplier shall implement appropriate technical and organizational measures considering the state of the art, costs, and risks to rights and freedoms of natural persons.

International Transfers: Transfers outside the EEA shall rely on a valid transfer mechanism under GDPR (e.g., SCCs), with supplementary measures where required by law.

Data Subject Rights: Supplier shall assist Raiffeisen Bank Kosovo J.S.C. in responding to requests and in meeting obligations regarding security, breach notifications, DPIAs, and prior consultations.

Return and Deletion: Upon termination, Supplier shall return personal data to Raiffeisen Bank Kosovo J.S.C. and securely delete copies, subject to legal retention requirements, and provide a deletion certificate.

Annex D: Templates

D1. Statement of Work (SOW) Template

1. 1. Background and Objectives: [Describe business context, drivers, and intended outcomes]
2. 2. Scope and Deliverables: [Enumerate deliverables, artifacts, and exclusions]
3. 3. Milestones and Schedule: [Provide timeline, dependencies, and critical path]
4. 4. Roles and Responsibilities: [RACI table summary]
5. 5. Service Levels and Reporting: [Define SLAs, KPIs, credits]
6. 6. Acceptance Criteria and Testing: [Detail test plans and success criteria]
7. 7. Governance and Meetings: [Cadence, participants, escalation path]
8. 8. Security and Compliance: [Controls, audits, certifications]
9. 9. Data Protection: [Processing summary, retention, transfer, sub-processors]
10. 10. Pricing and Payment: [Commercial model, invoicing]
11. 11. Change Control: [Process and approval matrix]
12. 12. Assumptions and Constraints: [List key assumptions and limits]
13. 13. Risks and Mitigations: [Top risks and mitigations]
14. 14. Exit and Transition: [Handover, knowledge transfer, acceptance of exit]

D2. Proof of Execution (POE) Template

15. 1. PO Reference and Line Items
16. 2. Description of Work Performed and Service Period
17. 3. Evidence of Delivery or Completion (attachments)
18. 4. Acceptance Sign-Off (Raiffeisen Bank Kosovo J.S.C. Representative)
19. 5. Exceptions / Deviations and Resolutions
20. 6. Supplier Representative and Contact Details

D3. Subcontractor Approval Request

21. 1. Subcontractor Legal Name and Registered Address
22. 2. Scope of Work to be Performed
23. 3. Due Diligence Summary (financial, compliance, security)
24. 4. Data Processing Involvement and Locations
25. 5. Contractual Flow-Downs and SLAs
26. 6. Risk Assessment and Mitigation Plan
27. 7. Raiffeisen Bank Kosovo J.S.C. Approval Signatures

Annex E: Financial Services Regulatory Considerations

The Supplier acknowledges that certain arrangements may constitute outsourcing or material outsourcing under applicable EU and Kosovon regulations. The Supplier shall support Raiffeisen Bank Kosovo J.S.C.'s compliance with supervisory expectations, including clear documentation of services, locations, subcontractors, and exit strategies.

The Supplier shall provide access and audit rights to Raiffeisen Bank Kosovo J.S.C., its internal audit, external auditors, and competent authorities, including on-site inspections where lawfully required and feasible, subject to reasonable confidentiality and security measures.

The Supplier shall notify Raiffeisen Bank Kosovo J.S.C. of material changes, incidents, or events that may affect service delivery, resilience, or compliance posture, and shall cooperate in remediation and regulatory notifications as requested by Raiffeisen Bank Kosovo J.S.C..

Annex F: Illustrative Examples and Guidance

Example 1: Non-Conforming Delivery

If software delivered fails user acceptance testing due to unmet functional requirements, Supplier shall remediate defects within the cure period at no cost and resubmit for acceptance. Raiffeisen Bank Kosovo J.S.C. may withhold payment until acceptance and may seek service credits where SLAs are breached.

Example 2: Security Incident Reporting

Upon discovering unauthorized access to a Supplier system that stores Raiffeisen Bank Kosovo J.S.C. data, Supplier must notify Raiffeisen Bank Kosovo J.S.C. without undue delay, share initial facts within 24 hours, and provide rolling updates, containment, and remediation plans, followed by a final root-cause analysis and lessons learned.

Example 3: Subcontractor Onboarding

Before engaging a new sub-processor to provide analytics, Supplier submits a Subcontractor Approval Request with due diligence results, data flow diagrams, and SLAs. Raiffeisen Bank Kosovo J.S.C. reviews, requests additional controls, and provides conditional approval subject to penetration testing results.