The Ultimate Request For Proposal Guide to AML Software

>pingwire_

The Ultimate Request for Proposal Guide to AML Software

This Request for Proposal (RFP) guide has been created to provide a clear and structured way of gathering the information required to purchase the perfect AML software for your company. It is designed for use when engaging with AML software providers, ensuring that you receive consistent, detailed, and comparable responses across all key areas of evaluation.

The framework covers essential topics such as customer onboarding, transaction monitoring, sanctions and PEP screening, case management, reporting, data protection, IT security, and regulatory compliance. By using this guide, you can be confident that every critical dimension is addressed, reducing the risk of gaps in your assessment process.

Using this guide will help you:

Save Time

Avoid the need to design new questionnaires for each provider

Standardize Responses

Make it easier to compare offerings across the market

Ensure Complete Information

Decisions backed by complete, reliable, and audit-ready information

This guide complements your internal procurement and compliance procedures, helping you to move through the evaluation process with greater efficiency and confidence.

Contributers to this Guide

Kimilia Carlsson Edland

Founder at RUBY

With a strong background in finance, compliance, and business development, Kimilia has led organizations through growth and transformation. She combines legal expertise with hands-on experience in scaling companies, bringing a pragmatic perspective to complex challenges.

Peter Lange

Chief Product Officer Pingwire

Peter has extensive experience in compliance and product development. He has served as a legal officer at the SFSA, a senior associate at a law firm specializing in regulatory law, an MLRO, and head of compliance at several financial institutions. With deep knowledge of both anti-money laundering regulations and product development, he ensures that Pingwire's solutions stay relevant and meet the complex demands of both companies and the market.

Gustav Ek

CEO Pingwire

Gustav leads Pingwire, developing advanced AML software that helps companies prevent financial crime. He is committed to pushing the boundaries of AML and fraud prevention by combining data science, software engineering, and regulatory insight, so organizations not only defend against risk but build resilience and trust.

Preparing for an RFP

What to do before sending out your Request for Proposal

To get the most value out of an RFP process, a solid internal groundwork is essential. Like any system procurement or implementation, the success of the project depends on how well the organization defines its needs, aligns stakeholders, and prepares the foundation for evaluation and execution.

Below are the key steps to take before issuing an RFP.

1. Preliminary Analysis and Needs Definition

Before sending out an RFP, your organization should conduct:

Needs Assessment: Identify the actual business, technical, and strategic requirements. What problem are you trying to solve?

Current State Analysis: Review existing systems and workflows. What works well, and what doesn't? Are you open to adjusting processes to fit a new system, or do you need a solution that fits your current setup?

Goal Setting: Define what you want to achieve, both qualitatively and quantitatively. Establish clear success metrics and KPIs.

Gap Analysis: Understand why current tools or processes aren't sufficient. Identify obstacles such as missing system support, limited internal expertise, or process inefficiencies.

2. Internal Alignment and Stakeholder Involvement

RFPs often originate from management initiatives, but success depends on the involvement of the right stakeholders:

- **Business Operations:** Ensure the solution meets operational needs and daily realities, while also incorporating identified components required to fulfill regulatory obligations. The solution should align with both business efficiency and compliance requirements.
- **Technology:** Assess integration, architecture, and security requirements early.
- **Finance and Procurement:** Confirm budget parameters and ensure procurement compliance.
- **End Users:** Engage early to capture expectations and usability insights.

A common pitfall is focusing only on strategic goals while overlooking operational realities leading to solutions that look good on paper but fail in practice.

3. Budget, Market Insight, and Selection Strategy

Budget: Define a realistic and well-anchored budget. Clarity on funding sources and limits reduces the risk of stalled procurement.

Market Research: Talk to peers in similar organizations and learn from their experiences.

Shortlisting: Conduct early market screening, reference checks, or an RFI (Request for Information) to refine your shortlist and improve the quality of your RFP.

RFP Questions

From here on, please find all the questions that are relevant and important to ask to a vendor of AML software in a purchasing process.

1. Background and Vendor Overview

1. Describe your organisation's core capabilities and how they align with AML/CTF use-cases. Include examples of previous AML/CTF implementations with similar clients.
2. Provide evidence of your financial stability, reputation and relevant certifications (e.g., ISO 27001, SOC 2, AML/CTF compliance).
3. List reference clients with sector, project scope and implementation date. Contact details are to be provided upon request.
4. Outline your organisational structure, number of employees and consultants, and any planned expansions.
5. Describe your experience serving financial institutions in Sweden and the broader European market.

2. Functional Capabilities

> *For the purposes of this RFP, 'rules' refer to configurable detection logic used in transaction monitoring (e.g., thresholds, conditions, and scenarios).

Screening and Due Diligence

1. What type of screenings do your system support?
2. Explain how your system performs PEP/RCA/sanctions screening. Describe how different parties involved in a transaction can be screened.
3. How does your system handle fuzzy matching, name variations and spelling errors in both real-time and batch screening?
4. Which external data providers (e.g., Moody's, Dow Jones, Acuris) and official regulatory watchlists (e.g., OFAC, EU, UN, UK HMT) do you support? How are these lists updated and managed?
5. Describe your approach to suppressing false positives and reducing unnecessary alerts.
6. Describe your capability to run batch screenings and simulate new or modified rules on historical data.

Transaction Monitoring

1. Is transaction monitoring performed synchronous or asynchronous?
2. Describe how transaction monitoring is performed in real-time as well as in batch.
3. Describe the flexibility in your rule configuration? Can rules be defined using multiple parameters (e.g., type of transaction, currency, sender/receiver, geography, KYC risk class, etc.). And how can these be simulated before deployment?
4. How does the system prioritise and deduplicate alerts? Can alerts be grouped and closed in bulk?
5. Explain your case-management functionality: how are cases escalated, prioritised and documented, and how are they linked to customer profiles?
6. Provide examples of pre-configured transaction monitoring scenarios (e.g., repeated deposits and withdrawals, deposits from corporate accounts to personal accounts, high-risk country transactions).

Analysing data

1. Describe your data analysis and reporting capabilities. What parameters and metrics can users access and analyse within the system?
2. Describe how audit trails are maintained. Is every action logged immutably, and can logs be exported for regulatory review?
3. Explain whether users can extract data for rule validation, create customised reports, and integrate with external BI tools.

Customer Due Diligence (KYC/EDD)

1. Describe how your system receives and updates KYC data (e.g., name, identification, beneficial ownership) via API or batch.
2. Do you offer adverse media screening, high-risk area classification and integration with government or regulatory databases (e.g., GoAML)?
3. Explain how your system supports the screening of foreign customers and individuals with foreign national identifiers.
4. Describe your enhanced due diligence workflow: how are complex corporate structures handled? Can users upload and analyse supporting documents?
5. How is the initial customer risk score calculated and updated throughout the customer lifecycle? Can different KYC flows be triggered based on customer type or risk profile?

3. Technical and Architectural Requirements

1. Specify your availability targets (e.g., ≥99.9 % uptime) and demonstrate how you achieve this.
2. Provide your Recovery Time Objective (RTO) and Recovery Point Objective (RPO) commitments.
3. Which deployment models do you support (on-premises, cloud, hybrid)?
    - For cloud deployments, describe encryption in transit and at rest.
    - For on-premises deployments, describe storage encryption and key management.
4. How does your system scale to accommodate increasing transaction volumes or additional workloads? Is auto-scaling available?
5. Describe your authentication and access control mechanisms, including support for AD/LDAP, SSO and MFA. Do you offer both role-based (RBAC) and attribute-based (ABAC) access control?
6. Detail your integration capabilities: which API standards do you support, and do you provide SDKs or connectors for common banking platforms and third-party data providers?
7. How do you validate incoming data and protect against data corruption or tampering? Describe your data integrity checks.
8. Do you support localisation, multi-language user interfaces and accessibility standards (e.g., ADA)?
9. Describe how your system facilitates link analysis and relationship graphs between customers, accounts and third parties.

4. Security and Privacy

1. Confirm that all personal and transaction data are stored and processed within the EU/EEA and identify all data centre locations.
2. Describe your encryption practices for data at rest and in transit, including key management and the entities responsible for encryption keys.
3. Provide a copy of your standard Data Processing Agreement (DPA) and explain how you support data subject rights (access, rectification, deletion, portability).
4. How are audit logs implemented? Are they write-once-read-many (WORM) and do they capture rule changes, user actions and case management events?
5. Detail your vulnerability management programme, including frequency of penetration testing, vulnerability scanning and patch management.
6. Explain how API calls are secured (e.g., OAuth 2.0, mutual TLS) and what measures are in place to prevent unauthorized access.
7. Do you offer dedicated environments for clients who require physical or logical separation of their data? If so, how is data segregation achieved in multi-tenant environments?
8. Describe how your employees and partners are granted and audited for access to raw customer data.
9. Explain your backup and redundancy strategies, including retention periods and geographic diversity of backups.
10. Describe your data deletion processes, including on-demand deletion and automatic deletion after account termination or retention periods.
11. Outline your logging policies at both application and infrastructure levels, including log retention periods and how clients can access logs.

5. Artificial Intelligence and Machine Learning

1. Explain the role of machine learning and statistical models in your transaction monitoring. What techniques do you use (rule-based, statistical, ML) and how do you ensure models remain effective?
2. What measures do you take to mitigate bias in training data and ensure fair and transparent model outcomes? Provide key performance metrics such as precision, recall and false-positive rates.
3. Specify which data sources are used for model training (client data, vendor datasets, external sources) and whether they are representative of individual client portfolios.
4. Describe how often models are retrained and validated, and how clients are informed of model updates.
5. Can clients adjust model sensitivity or exclude certain features? How do you provide explanations for ML-generated alerts?
6. Do you log the model version and parameters that generate each alert? How is this information made available to clients?
7. Is a non-production environment available for testing AI/ML rules before they are deployed?

6. Service Levels and Support

1. Provide your service-level targets for availability, API response times and batch processing windows. Include penalties for SLA breaches.
2. Describe your incident-response process as well as SLAs (e.g., initiation times and resolution times for critical and major incidents).
3. Outline your support model: hours of coverage, languages supported, support channels (phone, email, ticket portal) and the availability of dedicated account managers.
4. Describe your onboarding and training process for administrators and investigators. Do you provide ongoing training and refresher sessions?
5. Explain your change-management and update processes, including notification of downtime and client testing opportunities prior to production deployment.
6. Describe your product roadmap and how client feedback is incorporated into future development.
7. Do you provide regulatory updates and advisory services as part of your support offering?

7. Implementation and Professional Services

1. Describe your implementation methodology and provide a typical project plan from requirement gathering to go-live. Include estimated timelines and resource commitments.
2. Distinguish between functionality available out-of-the-box and functionality requiring custom development. Provide an overview of your change-management process and how customisations are maintained.
3. How are historical alerts and transaction data migrated into the new system? Do you assist with data cleansing and mapping?
4. Will you provide a dedicated onboarding team to configure rules and workflows in collaboration with our risk experts?
5. Do you offer a test environment that mirrors production for user acceptance testing and rule tuning?
6. What documentation, training materials and knowledge transfer will be provided during implementation?
7. Explain how you manage integrations with existing systems (e.g., AWS, Snowflake, core banking systems) and the typical time required for such integrations.

8. Pricing and Commercial Terms

1. Describe your pricing model, including base subscription fees, variable fees (e.g., per transaction or per user) and any minimum commitments.
2. How does pricing scale with increased transaction volumes or additional modules? Describe any tiered pricing or volume discounts.
3. List and price optional modules such as adverse media screening, link analysis, enhanced due diligence and integration with regulatory authorities.
4. Provide an estimate for implementation, configuration and consulting services, including typical ranges for small, medium and large clients.
5. Outline the contract term and renewal options. What termination clauses and notice periods are standard?
6. Specify the data vendor costs (e.g., Moody's, Dow Jones) that are not included in your software subscription.
7. Describe your invoicing frequency, payment terms and any applicable taxes or fees.
8. If your solution includes credit-based pricing, describe the credit system and provide pricing per credit.
9. Explain any minimum variable fee commitments and how they relate to actual usage.
10. Provide details of any service credits or refunds offered in the event of SLA breaches.

9. Risk Management and Compliance

1. How does your platform help institutions meet AML, CTF and fraud-prevention regulations (e.g., EU AMLDs, FATF recommendations, national regulations)?
2. Describe your processes for monitoring regulatory changes and updating your platform to meet new requirements. Do you provide regulatory advisories to clients?
3. Provide details of your internal risk assessment framework, including financial, operational and compliance risk assessments. Include how often assessments are performed.
4. Do you work with subcontractors or third-party service providers? If so, describe how you assess and monitor their performance and compliance.
5. How do you continuously monitor the performance and compliance of your service (e.g., KPI tracking, incident reviews, regular audits)?
6. Describe your offboarding process when a client terminates the service: data return or destruction, timeline, and certification of deletion.
7. Do you support regulatory reporting workflows (e.g., STR/SAR submission via goAML) and provide templates for other regulatory reports?
8. How do you ensure independence of compliance functions within your organisation (e.g., separation of product development and compliance teams)?
9. Explain your approach to operational resilience and adherence to the Digital Operational Resilience Act (DORA).

10. Additional Considerations

1. Describe your roadmap for future development and innovation, including features under consideration and expected release timelines.
2. What local languages does your solution support, and can you adapt user interfaces to local regulatory terminology?
3. Explain your collaboration model: communication cadence, project governance, and escalation procedures.
4. Do you offer co-development or custom feature development as part of your engagement?
5. Describe any community or user forums, user groups or client advisory boards available to share best practices.
6. Are there any limitations or exclusions in your solution that potential clients should be aware of?

The Ultimate Request For Proposal Guide to AML Software

Contact us

Pingwire
Brahegatan 10
114 37 Stockholm
Sweden

info@pingwire.io

>pingwire_