JSK

CASE STUDY

CASE STUDY

AML OUTSOURCING PROCESS: TRANSACTION MONITORING & KYC

MAINTAINING REGULATORY COMPLIANCE WHILE OUTSOURCING CRITICAL AML FUNCTIONS

Prepared by JSK Overseas Inc.,

Leadership | Confidential | April 2026

TABLE OF CONTENTS

Executive Summary

This case study examines the strategic approach to outsourcing Anti-Money Laundering (AML) operations, specifically transaction monitoring and Know Your Customer (KYC) functions, while maintaining ultimate regulatory compliance responsibility within the financial institution. The study is presented from the perspective of JSK Overseas Inc, a global advisory consultant, and outlines best practices, governance frameworks, and critical implementation considerations for successful AML outsourcing arrangements

Key Learning Points:

- Outsourcing does not transfer regulatory liability, the financial institution remains accountable
- Structured SLAs, KPIs, and oversight mechanisms are essential for effective outsourced AML programs
- BPO providers execute operational tasks; the institution retains governance and strategic authority
- Regular audits, performance monitoring, and continuous oversight ensure program effectiveness and regulatory readiness

1. PROBLEM STATEMENT & BUSINESS CONTEXT

THE CHALLENGE

Financial institutions face mounting pressure to manage AML compliance across an increasingly complex operating environment:

- Regulatory expectations have intensified and regulators now demand proof of program effectiveness, not just documentation
- Transaction volumes continue to grow, straining internal compliance resources
- Building and retaining specialist AML talent is costly and difficult in competitive labor markets
- Technology investments (AI, transaction monitoring systems) require continuous updates and expertise
- Emerging risks (crypto assets, cross-border payments, stablecoins) require specialized knowledge

WHY OUTSOURCING?

Many institutions have turned to Business Process Outsourcing (BPO) providers to manage operational AML activities while retaining strategic oversight. According to PWC research (2023), approximately 61% of financial institutions outsource at least some compliance functions to BPO providers. The market itself is growing at 8.5% CAGR, projected to reach $654.78 billion by 2033.

However, outsourcing introduces governance complexity and regulatory risk. The critical question is: How can an institution outsource operational AML activities while maintaining full regulatory responsibility and compliance accountability?

2. SOLUTION OVERVIEW: THE AML OUTSOURCING FRAMEWORK

CORE PRINCIPLE

Outsourcing divides operational execution from regulatory accountability. The BPO provider executes AML tasks (first line of defense); the financial institution maintains governance, strategic oversight, and ultimate regulatory responsibility (second line of defense).

THE OPERATING MODEL

Function	BPO Provider (Operational)	Institution (Governance)
KYC Execution	Customer verification, document review, PEP screening, risk tier classification	KYC approval, risk assessment sign-off, customer acceptance
Transaction Monitoring	Alert generation, investigation, documentation, escalation preparation	SAR decisions, regulatory filings, policy decisions, MLRO authority
Reporting	Monthly dashboards, quarterly metrics, performance analysis, case documentation	Board reporting, regulatory submissions, annual compliance certificate
Oversight	SLA compliance, audit trail maintenance, quality assurance execution	Regular audits, SLA monitoring, control testing, governance review

3. OUTSOURCEABLE AML ACTIVITIES

KYC (KNOW YOUR CUSTOMER) FUNCTIONS

The following KYC activities can be safely outsourced with proper governance:

- **Customer Identity Verification:** Document validation, biometric checks, ID authentication
- **Beneficial Ownership Checks:** Identifying ultimate beneficial owners, corporate structure mapping
- **PEP Screening:** Sanctions and watchlist screening, periodic refresh
- **Customer Due Diligence (CDD):** Initial and enhanced due diligence reviews
- **KYC Refresh:** Periodic updates to customer information and risk assessments

- **Risk Tier Classification:** Customer risk profiling and categorization
- **Document Review:** Analysis and validation of submitted documentation

TRANSACTION MONITORING FUNCTIONS

Transaction monitoring operations best suited for outsourcing:

- **Real-Time Alert Generation:** Flagging suspicious transactions as they occur
- **Alert Investigation:** Detailed review of alerts to determine legitimacy
- **Case Documentation:** Preparing detailed analysis and case files
- **SAR Preparation:** Documenting findings for regulatory filing
- **False Positive Reduction:** Rule tuning and alert optimization
- **Escalation Management:** Routing high-risk cases to compliance officers

WHAT REMAINS WITH THE INSTITUTION

The following functions must remain under institutional control:

- SAR Decisions and Filing Authority
- Customer Acceptance/Rejection Decisions
- Account Closure and Derisking Decisions
- AML Policy and Procedure Development
- Regulatory Engagement and Reporting
- MLRO Oversight and Final Authority

4. SERVICE LEVEL AGREEMENTS (SLAS) & PERFORMANCE FRAMEWORK

WHAT IS AN SLA?

A Service Level Agreement is a contractual commitment between the financial institution and the BPO provider that specifies performance targets, response times, quality metrics, and remedies for non-compliance. SLAs translate operational requirements into measurable, enforceable commitments.

KYC SLA TARGETS

Activity	Target Timeline	Compliance Target
Initial KYC Completion	3-5 business days	95%+ within SLA
Enhanced Due Diligence	5-10 business days	90%+ within SLA
Beneficial Ownership Verification	5-7 business days	95%+ within SLA
PEP Screening	1-2 business days	99%+ within SLA
Annual KYC Refresh	Within 12 months	100% within SLA

TRANSACTION MONITORING SLA TARGETS

Activity	Target Timeline	Compliance Target
High-Risk Alert Escalation	24 hours	100%
Low-Risk Alert Investigation	2-3 business days	95%+ within SLA
Medium-Risk Alert Investigation	5-7 business days	93%+ within SLA
SAR Filing (from approval)	Within 30 days	100%

QUALITY & COMPLIANCE SLA TARGETS

- Documentation Accuracy: 95%+ compliance on audit review
- False Positive Rate: Target 30-50% (varies by rule and customer base)
- SAR Conversion Rate: Industry average 15-20% (SARs filed ÷ total alerts)
- System Availability: 99.5%+ uptime
- Audit Trail Completeness: 100% documented decisions and actions

5. KEY PERFORMANCE INDICATORS (KPIS)

The financial institution should track KPIs across multiple dimensions to ensure the BPO provider is performing effectively. These KPIs inform monthly management reviews and quarterly compliance committee discussions.

ALERT HANDLING KPIS

- **Alert Volume:** Total alerts generated per month/quarter
- **Alert Backlog:** Pending investigations, aging by cohort (0-5 days, 5-15 days, >15 days)
- **Investigation Turnaround:** Average days from alert generation to closure
- **False Positive Rate:** Percentage of alerts cleared without escalation
- **SAR Conversion Rate:** SARs filed ÷ total alerts investigated

KYC/CDD KPIS

- **KYC Completion Rate:** Percentage of customers with current KYC documentation
- **Volume Processed:** Number of KYC cases completed per month
- **Risk Tier Distribution:** Percentage breakdown across low/medium/high risk

- **EDD Escalation Rate:** Percentage of cases requiring enhanced due diligence
- **Refresh Completion:** Percentage of scheduled KYC refreshes completed within SLA

QUALITY & COMPLIANCE KPIS

- **Documentation Quality Score:** Audit findings on completeness, accuracy, traceability
- **Escalation Accuracy:** Percentage of cases correctly escalated to compliance
- **SLA Compliance:** Percentage of targets met (by function)
- **Control Test Results:** Sampling audit outcomes, error rates, findings

6. GOVERNANCE & OVERSIGHT MODEL

The financial institution must maintain multi-layered oversight to ensure the BPO provider operates effectively within agreed parameters while the institution retains regulatory responsibility.

OVERSIGHT MECHANISMS

1. OPERATIONAL MONITORING

Frequency: Daily to weekly

Method: Real-time dashboards tracking alert backlogs, SLA compliance, processing volumes

2. COMPLIANCE COMMITTEE REVIEW

Frequency: Monthly

Method: Management review of KPIs, alert trends, high-risk cases, SLA breaches, remediation actions

3. SERVICE LEVEL AGREEMENT MONITORING

Frequency: Monthly reporting, quarterly review

Method: BPO provider submits detailed SLA compliance report. Non-compliance triggers investigation and remediation plan.

4. COMPLIANCE AUDIT

Frequency: Quarterly (internal), annually (external)

Method: Sampling review of case files, documentation quality, control compliance, audit trail integrity

5. REGULATORY EXAMINATION & RESPONSE

Frequency: As needed

Method: BPO provider prepares documentation for regulatory audits. Institution maintains final regulatory accountability.

6. ANNUAL COMPLIANCE CERTIFICATION

Frequency: Semi-annually (June 30, December 31)

Method: MLRO prepares comprehensive compliance report for Board review. Certifies control effectiveness, identifies gaps, recommends improvements.

CRITICAL GOVERNANCE PRINCIPLES

The following principles must guide the outsourcing arrangement:

Regulatory Accountability Remains: The financial institution cannot delegate regulatory responsibility to the BPO provider.

Separation of Duties: The BPO executes; the institution governs. Final authority on all compliance decisions remains with the MLRO.

Data Security: Data must be processed in secure facilities with proper encryption, access controls, and NDAs. No local data retention at BPO premises.

Audit Trail: Every decision, alert, investigation, and escalation must be fully documented with clear traceability to support regulatory examinations.

Conflict of Interest: Conflict checks must be conducted at onboarding and renewed periodically. Staff must disclose any financial crime or adverse background.

7. REPORTS GENERATED BY BPO PROVIDER

The BPO provider generates regular reports for management and board-level review. These reports serve as evidence of program effectiveness and basis for regulatory compliance certification.

MONTHLY REPORTS

Delivered: Within 5-10 business days of month-end. Audience: Compliance team, operations management

- **Transaction Monitoring Dashboard:** Alert volume, backlog by age, false positive rate, investigation turnaround, SAR filing rate
- **KYC Processing Report:** Volume processed, completion rates by risk tier, turnaround times, escalations
- **SLA Compliance Report:** Percentage of targets met, breaches, root causes, corrective actions
- **Sanctions & PEP Screening Report:** Screening volume, hits, resolution status, false positive rates

QUARTERLY REPORTS

Delivered: End of quarter. Audience: Compliance Committee, MLRO, Board

- **Quarterly Compliance Effectiveness Report:** Alert trends, rule performance, false positive analysis, emerging typologies
- **AML/CFT Control Assessment:** Control testing results, sampling audit outcomes, compliance gaps, audit readiness
- **Risk Assessment Update:** Changes to ML/TF risk profile, new typologies, effectiveness of controls
- **Training & Awareness Summary:** Staff training completion rates, topics covered, gaps identified

SEMI-ANNUAL / ANNUAL REPORTS

Delivered: June 30, December 31 (or per regulatory requirement). Audience: Board of Directors, MLRO, Regulatory Authorities

The MLRO prepares a comprehensive compliance report covering:

- Executive summary of program effectiveness
- Risk assessment methodology and key findings
- Transaction monitoring analysis (annual metrics, rule performance, SAR summary)
- KYC/CDD program effectiveness (completion rates, refresh status, quality metrics)
- Sanctions and PEP screening results
- Suspicious Activity Reporting summary (volume, issue types, timeliness)
- Compliance testing and audit findings
- Staff training completion
- Policy and procedure updates
- Identified control weaknesses and remediation plans
- Board approval and submission to regulatory authorities

8. IMPLEMENTATION ROADMAP

Establishing an effective AML outsourcing arrangement requires careful planning and phased implementation. This roadmap outlines critical steps from planning through operational execution.

PHASE 1: PLANNING & ASSESSMENT (WEEKS 1-4)

- Assess current AML operations, identify activities to outsource
- Define scope of services, functional requirements, regulatory constraints
- Establish governance framework and MLRO oversight structure
- Conduct regulatory pre-notification if required in jurisdiction

PHASE 2: VENDOR SELECTION (WEEKS 5-12)

- Issue RFP to qualified BPO providers with AML/compliance expertise
- Evaluate proposals on capability, experience, compliance track record, technology
- Conduct due diligence on finalists (audit visits, regulatory checks, references)
- Negotiate SLA, KPI targets, pricing

PHASE 3: CONTRACT & FRAMEWORK DEVELOPMENT (WEEKS 13-20)

- Finalize Master Service Agreement with clear responsibility division
- Develop detailed Operating Procedures documenting workflows and escalation paths
- Establish data security, GDPR compliance, and confidentiality protocols
- Define governance, oversight, and audit rights

PHASE 4: KNOWLEDGE TRANSFER & TRAINING (WEEKS 21-32)

- Provide historical data, customer profiles, transaction data to BPO provider
- Train BPO teams on institution's AML policies, procedures, risk standards
- Conduct conflict of interest checks and background verification for BPO staff
- Conduct dry runs for transaction monitoring and KYC processes

PHASE 5: PARALLEL OPERATIONS (WEEKS 33-44)

- Run BPO processes in parallel with internal team for validation
- Compare alert quality, KYC accuracy, processing times
- Refine thresholds, rules, and procedures based on findings

PHASE 6: GO LIVE & STABILIZATION (WEEKS 45-56)

- Cutover from internal to BPO execution
- Close monitoring of alert volumes, SLA compliance, false positives
- Establish ongoing oversight mechanism and governance cadence

PHASE 7: CONTINUOUS IMPROVEMENT (ONGOING)

- Monthly compliance committee reviews of KPIs and SLA adherence
- Quarterly thematic reviews and control assessments
- Annual compliance certification and board reporting
- Regular review of emerging risks and regulatory requirements

9. CRITICAL SUCCESS FACTORS

The following factors are essential for effective AML outsourcing:

1. CLEAR GOVERNANCE & ACCOUNTABILITY

The financial institution must maintain clear separation between execution (BPO) and governance (institution). The MLRO must have authority to make final decisions on KYC approval, SAR filing, and account actions. This cannot be delegated.

2. ROBUST OVERSIGHT

Monthly KPI reviews, quarterly control assessments, and annual audits ensure the BPO provider remains within expectations. Oversight must be systematic and documented.

3. STRONG SLA & KPI FRAMEWORK

SLAs must be specific, measurable, and enforced. Breaches should trigger investigation and remediation. KPIs should cover volume, quality, timeliness, and compliance dimensions.

4. DATA SECURITY & CONFIDENTIALITY

Customer data must be processed in secure facilities with proper encryption, access controls, and auditability. Staff must be vetted. NDAs must be mandatory.

5. COMPETENT BPO PARTNER

The BPO provider must have demonstrated AML expertise, proper compliance certifications, audit track record, and technology capability. Generalist BPOs rarely work for AML.

6. AUDIT TRAIL COMPLETENESS

Every alert, investigation, decision, and escalation must be documented with clear traceability. This documentation must be sufficient to satisfy regulatory examiners.

7. REGULATORY ALIGNMENT

The outsourcing arrangement must comply with local AML regulations, FATF recommendations, GDPR, and other applicable requirements. Regulatory pre-notification should be considered.

10. KEY RISKS & MITIGATION STRATEGIES

Outsourcing AML operations introduces several risks that must be proactively managed:

RISK: LOSS OF CONTROL & OVERSIGHT

Consequence: Poor quality decisions, missed suspicious activities, regulatory breaches

Mitigation: Establish multi-layered oversight: real-time dashboards, monthly compliance committee reviews, quarterly control audits, annual regulatory assessments. MLRO must maintain final authority over all compliance decisions.

RISK: DATA SECURITY & CONFIDENTIALITY BREACH

Consequence: Customer data leakage, regulatory fines, reputation damage, GDPR violations

Mitigation: Require ISO 27001 certification, SOC 2 audit, encrypted data storage, limited access controls, regular penetration testing. Impose strict NDAs with financial penalties. Audit compliance regularly.

RISK: SLA NON-COMPLIANCE

Consequence: Delayed alerts, missed suspicious activities, backlog of unreviewed cases

Mitigation: Set clear, achievable SLA targets with financial penalties for breach. Monitor compliance weekly. Require root cause analysis and corrective action plans for breaches.

RISK: INADEQUATE AUDIT TRAIL

Consequence: Inability to explain decisions to regulators, failed audits, regulatory criticism

Mitigation: Require BPO to maintain comprehensive audit logs. Implement 4th party audit visits at BPO premises. Conduct periodic sampling reviews to verify documentation completeness.

RISK: CONFLICT OF INTEREST OR FRAUD

Consequence: Insider threats, collusion, data theft, missed SAR reporting

Mitigation: Conduct thorough background checks and conflict of interest checks for all BPO staff. Require annual renewal. Implement segregation of duties. Conduct unannounced audits.

RISK: REGULATORY EXAMINATION OR ENFORCEMENT

Consequence: Regulatory fines, enforcement actions, license restrictions, reputational damage

Mitigation: Maintain complete regulatory readiness. Conduct internal audit self-assessments. Ensure MLRO has authority to communicate directly with regulators. Prepare annual compliance certification. Document all governance and oversight activities.

11. CONCLUSION

Outsourcing AML transaction monitoring and KYC functions to a specialized BPO provider can deliver significant operational and cost benefits while maintaining regulatory compliance, but only if the financial institution maintains clear governance, systematic oversight, and ultimate responsibility for all compliance decisions.

The key principle is this: The financial institution cannot outsource compliance responsibility. It can only outsource operational execution. The BPO provider is the first line of defense (operational execution); the institution is the second line (governance and oversight). Internal audit provides the third line (independent verification).

Success requires:

- Clear functional scope with proper SLAs and KPIs
- Multi-layered oversight mechanisms (daily monitoring, monthly reviews, quarterly audits, annual certification)
- Competent BPO partner with proven AML expertise
- Strong governance controls (data security, conflict management, audit trails)
- MLRO with clear authority and independence
- Continuous monitoring, assessment, and regulatory alignment

With these elements in place, institutions can confidently outsource operational AML functions while maintaining the control and accountability required by regulators.