LES CONSULTANTS
CONSEIL & FORMATION

EN

AML for Payment Institutions

From Regulatory Compliance to Operational Investigations

Language: English French | Regulatory context: Luxembourg and European Union.

FORMAT
Instructor-led training combining regulatory guidance, operational examples, interactive questions and payment-specific case studies.

TARGET AUDIENCE
Compliance officers, MLRO teams, KYC and onboarding analysts, transaction-monitoring investigators, risk professionals, payment operations teams, internal auditors, product teams and relevant senior managers.

BY THE END OF THE TRAINING, PARTICIPANTS WILL BE ABLE TO

Training objectives

1. Understand the Luxembourg and EU AML/CFT framework applicable to payment institutions.
2. Identify the specific money-laundering, terrorist-financing and sanctions risks associated with payment services.
3. Apply a practical risk-based approach to customers, merchants, products, payment channels and transactions.
4. Distinguish inherent risk from residual risk and assess whether mitigating controls are genuinely effective.
5. Understand the allocation of AML responsibilities across the three lines of defence.
6. Recognise relevant payment and merchant-related red flags.
7. Prioritise and investigate alerts using a structured investigation methodology.
8. Document clear, evidence-based and defensible AML decisions.
9. Escalate suspicious activity and sanctions concerns appropriately.
10. Convert investigation findings into management information and improvements to the AML control framework.

5 STAGES · 31 TOPICS

Course agenda

OPENING — Opening and regulatory context (15 minutes)

1 Introduction and learning objectives

The trainer introduces the purpose, scope and practical orientation of the course.

Topics covered:
- Why AML controls must be adapted to the payment sector.
- The relationship between regulatory requirements and operational decisions.
- The importance of decisions that are risk-based, workable and defensible.
- The three questions guiding the training: What happened? Why does it matter? What evidence supports the decision?

2 Learning journey

Presentation of the five stages of the training:

1. Regulatory foundations.
2. Governance and accountability.
3. Monitoring and detection.
4. Operational investigations.
5. Reporting, oversight and continuous improvement.

Participants are invited to identify the areas in which AML currently creates the greatest operational challenges, such as onboarding, screening, monitoring, investigation, escalation or third-party oversight.

3 Why payment institutions are different

Analysis of the characteristics that distinguish payment institutions from traditional financial institutions:
- Speed of transactions.
- High transaction volumes.
- Digital and remote distribution channels.
- Cross-border reach.
- Complex merchant, platform and processor ecosystems.
- Fragmented customer, merchant, device and beneficiary data.
- The importance of detecting patterns across multiple low-value transactions.

4 Luxembourg and EU regulatory framework

Overview of the main regulatory sources applicable to payment institutions:
- Luxembourg AML Law of 12 November 2004, as amended.
- CSSF Regulation No. 12-02.
- Luxembourg Law of 10 November 2009 on payment services.
- Relevant CSSF circulars and supervisory expectations.
- EBA money-laundering and terrorist-financing risk-factor guidelines.
- The EU AML package and the establishment of AMLA.
- Roles of the CSSF and the Luxembourg Financial Intelligence Unit, or CRF.
- Relationship between AML reporting and international financial sanctions obligations.

> **KEY TAKEAWAY**
> Regulation defines the obligation, governance assigns responsibility, procedures make the obligation executable and evidence makes the decision defensible.

MODULE 1 — Regulatory foundations (16 minutes)

5 Applying the risk-based approach

Explanation of the practical operating cycle of a risk-based AML framework:

1. Identify relevant risks.
2. Assess inherent exposure.
3. Evaluate mitigating controls.
4. Determine residual risk.
5. Apply proportionate measures.
6. Document and approve the decision.
7. Improve the framework based on experience.

Participants examine how higher-risk activities may remain acceptable where appropriate controls operate effectively and the residual risk falls within the institution's risk appetite.

6 Risk drivers specific to payment institutions

Review of the principal risk dimensions:

Product risk
- Merchant acquiring.
- Payment initiation.
- E-money and wallets.
- Remittance services.
- Card payments.
- Payment gateways.
- Stored-value products.
- Buy-now-pay-later services.

Customer and merchant risk
- Customer occupation or business activity.
- Complex ownership structures.
- High-risk merchant categories.
- Shell or recently established merchants.
- Customers whose behaviour is inconsistent with their profile.

Geographic risk
- Country of incorporation.
- Customer residence.
- Device or access location.
- Merchant location.
- Beneficiary country.
- Settlement-bank location.
- Payment-routing jurisdiction.
- Sanctions nexus.

Channel risk
- Remote onboarding.
- Mobile applications.
- Agents and distributors.
- Application programming interfaces.
- Outsourced KYC arrangements.
- Platform-based distribution.

Transaction risk
- High velocity.
- Structuring.
- Round amounts.
- Rapid movement of funds.
- Sudden volume increases.
- Repeated failed attempts.
- Unusual beneficiaries or corridors.

Third-party risk
- Processors.
- Correspondent or settlement banks.
- Platforms.
- Agents.
- Technology providers.
- Outsourced compliance providers.

7 Inherent risk and residual risk

Participants learn to distinguish:
- Inherent risk: exposure before controls are considered.
- Residual risk: exposure remaining after relevant and effective controls are applied.

The session explains why the existence of a policy, procedure or screening system does not automatically reduce risk. A control must be relevant, timely, reliable, properly owned and supported by evidence.

8 AML obligations throughout the customer lifecycle

Overview of AML responsibilities at each stage:

Before onboarding
- Identification and verification.
- Beneficial-ownership assessment.
- Understanding the purpose of the relationship.
- Expected transaction profile.
- Screening.
- Risk classification.
- Approval.

During the relationship
- Ongoing monitoring.
- Periodic reviews.
- Event-driven reviews.
- Transaction monitoring.
- Rescreening.
- Review of changes in ownership, geography or activity.

When unusual activity is identified
- Alert investigation.
- Collection of evidence.
- Escalation.
- Restriction or enhanced monitoring.
- Remediation.
- Exit or external reporting.

At termination
- Management of remaining funds.
- Record retention.
- Reporting considerations.
- Prevention of tipping off.
- Documentation of the exit rationale.

9 Impact of the EU AML package

Discussion of the expected operational consequences of the European AML reforms:
- Greater harmonisation of AML requirements.
- More comparable supervisory information.
- Increased focus on data quality and data lineage.
- Stronger evidence of control effectiveness.
- Consistent definitions across onboarding, monitoring and reporting.
- Preparation for AMLA supervision and enhanced supervisory convergence.

MODULE 2 — Governance and accountability (18 minutes)

10 Governance from the Board to the alert handler

Explanation of responsibilities across the organisation:

Board and authorised management
- Approve the AML risk appetite.
- Approve the overall AML framework.
- Ensure adequate resources.
- Review material AML risks and deficiencies.

Senior management
- Implement the framework.
- Assign responsibilities.
- Ensure systems and controls operate effectively.
- Oversee remediation.

AML compliance function
- Establish standards.
- Advise and challenge the business.
- Monitor control performance.
- Support escalation.
- Conduct quality assurance.

MLRO or Luxembourg responsible person
- Assess suspicion.
- Decide whether external reporting is required.
- Protect the independence and confidentiality of reporting decisions.

Operational teams and investigators
- Perform controls.
- Review alerts.
- Gather and analyse evidence.
- Document conclusions.
- Escalate unresolved concerns.

Internal audit
- Provide independent assurance.
- Test control design and operating effectiveness.
- Review governance, data, timeliness, documentation and remediation.

11 The three lines of defence

Application of the three-lines model to payment activities:
- First line: owns and manages operational AML risk.
- Second line: establishes the framework and provides independent challenge.
- Third line: provides independent assurance.

The module addresses the common misconception that AML belongs exclusively to the compliance function.

12 From policy to evidence

Presentation of the control chain:

Policy → Procedure → Control → Evidence → Assurance

Participants learn to test each material AML obligation by asking:
- What must happen?
- Who performs the action?
- How often is it performed?
- What evidence proves that it occurred?
- What happens when the expected result is not achieved?
- Who reviews and challenges the outcome?

13 Customer and merchant onboarding lifecycle

Detailed review of the onboarding process:
- Collection of identity and corporate information.
- Identification of beneficial owners and controllers.
- Understanding business activity and expected flows.
- Verification through reliable and independent sources.
- Sanctions, PEP and adverse-media screening.
- Risk scoring.
- Enhanced due diligence where required.
- Approval and activation.
- Assignment of limits, monitoring profiles and review dates.

The session also explains dynamic onboarding, under which the level of questioning and verification is adapted to the customer's risk characteristics.

14 Simplified, standard and enhanced due diligence

Clarification of the differences between:

Simplified due diligence
Used only where lower risk is demonstrated and no mandatory enhanced-due-diligence factor applies.

Standard customer due diligence
Covers identity, beneficial ownership, purpose, expected activity, relevant source-of-funds information, screening and ongoing monitoring.

Enhanced due diligence
May include:
- Additional independent verification.
- Senior-management approval.
- Source-of-funds or source-of-wealth analysis.
- Deeper ownership analysis.
- More restrictive transaction limits.
- Targeted monitoring.
- More frequent reviews.
- Additional controls over high-risk jurisdictions or merchant sectors.

> **KEY TAKEAWAY**
> Enhanced due diligence is not simply the collection of more documents. It must resolve the specific risk concern.

15 Sanctions and screening operating model

Review of four operational questions:

Who should be screened?
- Customers.
- Beneficial owners.
- Directors.
- Merchants.
- Agents and distributors.
- Relevant counterparties.
- Settlement beneficiaries.

When should screening occur?
- At onboarding.
- Before activation.
- Following list updates.
- Periodically.
- At relevant trigger events.
- Before transaction execution or settlement where required.

What information should be screened?
- Sanctions.
- PEP status.
- Relevant adverse media.
- Law-enforcement information.
- Internal blacklists.

How should alerts be reviewed?
- Use of reliable identifiers.
- Name variations and transliteration.
- Fuzzy matching.
- Dates of birth.
- Nationality and geography.
- Ownership and control.
- Documented false-positive reasoning.
- Immediate escalation of potential sanctions exposure.

MODULE 3 — Monitoring and detection (19.5 minutes)

16 Transaction-monitoring architecture

Presentation of the five connected layers of an effective monitoring framework:

1. Data.
2. Rules and scenarios.
3. Alerts.
4. Cases.
5. Feedback and improvement.

Topics covered:
- Customer and merchant data.
- Transaction data.
- Devices and IP addresses.
- Beneficiaries and funding instruments.
- Geographic data.
- Historical alerts and investigations.
- Data completeness, validity and timeliness.
- Reconciliation between source systems and case-management tools.

17 Monitoring-scenario governance

Each monitoring scenario should include:
- A defined risk typology.
- Documented data inputs.
- A threshold rationale.
- A designated owner.
- Validation and testing.
- Review frequency.
- Change history.
- Performance metrics.
- Feedback from investigations.

Participants learn why high alert volumes do not necessarily demonstrate effective monitoring.

18 Alert triage and prioritisation

Explanation of risk-based triage criteria:
- Potential sanctions exposure.
- Active fraud.
- High-risk corridors.
- Rapid dissipation of funds.
- Law-enforcement requests.
- Links to previous serious cases.
- High-value or high-velocity activity.
- Multiple linked customers or merchants.

A triage decision should record:
- Alert severity.
- Reason for prioritisation.
- Assigned owner.
- Investigation deadline.
- Immediate preventive or protective action.

19 Red flags involving payment accounts and cards

Examples include:
- Rapid incoming and outgoing payments.
- Pass-through activity.
- Structured or split payments.
- Sudden activity on a dormant account.
- Transactions inconsistent with the customer profile.
- Multiple customers using the same device or IP address.
- Shared telephone numbers, addresses or beneficiaries.
- Repeated failed transactions.
- Attempts to modify names or routing details after rejection.
- Generic or repeated payment references.

Participants are reminded that red flags are indicators requiring analysis, not automatic proof of suspicious activity.

20 Red flags involving remittance, e-money and wallets

Topics include:
- Repeated payments to high-risk corridors.
- Several senders transferring funds to one beneficiary.
- Frequent beneficiary changes.
- Rapid top-up and withdrawal.
- Limited genuine spending activity.
- Circular transfers.
- Multiple wallets linked to one device.
- Frequent changes of funding instruments.
- Voucher or cash-like activity inconsistent with the customer profile.

The module emphasises network and cluster analysis rather than isolated account review.

21 Merchant and platform risk

Detailed analysis of merchant-related risks:
- Merchant laundering.
- Shell or fictitious merchants.
- Prohibited or restricted products.
- Undisclosed sub-merchants.
- Nested payment activity.
- Misleading merchant-category codes.
- Unusual refunds and chargebacks.
- Rapid or unexplained growth.
- Changes in settlement accounts.
- Inconsistency between the merchant's website and transaction activity.
- Business-model drift after onboarding.

Participants learn to compare the merchant's declared business with its actual payment behaviour.

MODULE 4 — Operational investigations (33.5 minutes)

22 Five-step investigation workflow

Step 1 — Scope
Define:
- The subject of the investigation.
- The relevant alert.
- The review period.
- Products involved.
- Linked accounts, merchants or counterparties.
- The precise risk question to be answered.

Step 2 — Gather
Collect relevant information:
- KYC and beneficial-ownership data.
- Expected activity.
- Transaction history.
- Screening results.
- Prior alerts and investigations.
- Device and IP information.
- Merchant information.
- Reliable open-source intelligence.

Step 3 — Analyse
- Compare expected and actual activity.
- Build a transaction timeline.
- Identify counterparties and jurisdictions.
- Analyse velocity and concentration.
- Identify network links.
- Test relevant typologies.
- Consider credible legitimate explanations.

Step 4 — Conclude
Possible outcomes include:
- No further concern.
- Continued or enhanced monitoring.
- Request for additional information.
- Remediation.
- Account or transaction restriction.
- Customer exit.
- Sanctions escalation.
- Suspicious activity reporting.

Step 5 — Record
- Prepare a concise narrative.
- Attach relevant evidence.
- Record the decision maker.
- Obtain review and approval.
- Assign follow-up actions.
- Preserve the complete audit trail.

23 Investigation-pack checklist

A complete investigation file should include:
- Subject profile.
- Beneficial-ownership information.
- Risk rating.
- Expected activity.
- Relevant timeline.
- Transaction amounts and counterparties.
- Jurisdictions involved.
- Linked accounts and devices.
- Screening results.
- Plausibility assessment.
- Source-of-funds or source-of-value analysis where relevant.
- Clear decision and rationale.
- Reviewer and approver.
- Follow-up actions.
- Dated and traceable evidence.

24 Case study 1 — Mule-account network

Participants analyse a network of retail customers receiving transfers from unrelated third parties and rapidly forwarding the funds to common beneficiaries.

The exercise covers:
- Identification of the most relevant facts.
- Shared devices and IP addresses.
- Common beneficiaries.
- Rapid movement of funds.
- Distinction between facts and hypotheses.
- Possible account takeover or mule recruitment.
- Cluster-based investigation.
- Immediate protective measures.
- Escalation to the MLRO or responsible person.

> **MAIN LESSON**
> The appropriate investigative unit may be the network rather than the individual account.

25 Case study 2 — Merchant laundering

Participants investigate a recently onboarded merchant displaying:
- Rapid growth in payment volume.
- Unusual refund activity.
- Repeated settlement-instruction changes.
- Payments to different bank accounts.

The investigation is divided into three areas:

1. Business reality.
2. Transaction logic.
3. Control of settlement beneficiaries.

The case also considers undisclosed sub-merchants, fraud indicators, enhanced monitoring, restrictions, remediation, exit and suspicious reporting.

> **MAIN LESSON**
> Merchant due diligence continues after onboarding because transaction data continuously tests whether the declared business remains credible.

26 Case study 3 — Sanctions circumvention

Participants review a payment involving:
- A partial name match.
- A high-risk destination.
- Intermediaries.
- Repeated changes to payment details.
- Potential indirect ownership or control by a listed person.

The exercise covers:
- Immediate sanctions handling.
- Blocking or freezing considerations.
- Identity and ownership verification.
- Intermediary and routing analysis.
- Fragmentation and altered spellings.
- Documentation of the decision timeline.
- Distinction between sanctions notifications and suspicious activity reporting.

> **MAIN LESSON**
> Sanctions investigations are time-sensitive and extend beyond direct name matching.

27 Drafting a defensible investigation rationale

Participants learn a four-part writing method:

Facts
Who, what, when, where, how much and through which channels?

Inconsistency
Why does the activity not fit the expected profile or a credible legitimate purpose?

Typology
Which relevant pattern is present, such as mule activity, structuring, merchant laundering or sanctions circumvention?

Decision
Why is the matter being closed, monitored, restricted, exited or reported?

The trainer explains how to separate objective facts from professional inference and avoid unsupported conclusions.

MODULE 5 — Escalation, oversight and continuous improvement (18 minutes)

28 Internal escalation and external reporting

Review of the escalation chain:

1. Alert identification.
2. Initial investigation.
3. Quality or compliance review.
4. MLRO or responsible-person assessment.
5. External reporting where appropriate.

Topics covered:
- Suspicion threshold.
- Reporting without undue delay.
- CRF reporting through the applicable channel.
- Structure and content of a useful suspicious activity report.
- Confidentiality.
- Prohibition of tipping off.
- Coordination of customer communication and restrictions.
- Separate handling of international financial sanctions notifications.

29 Oversight of agents, distributors and outsourced providers

The module explains that delegation does not transfer AML accountability.

Initial due diligence
- Competence and integrity.
- Ownership.
- Jurisdictions.
- Control environment.
- Technology and data security.
- Subcontracting arrangements.

Contractual safeguards
- Scope of AML responsibilities.
- Service levels.
- Incident reporting.
- Access to records.
- Audit rights.
- Record retention.
- Remediation.
- Termination rights.

Ongoing oversight
- Quality sampling.
- Missing evidence.
- Alert-resolution quality.
- Screening delays.
- Geographic anomalies.
- Customer complaints.
- Remediation monitoring.
- Concentration and business-continuity risk.

Particular attention is given to the continued responsibility of the Luxembourg entity when group or outsourced arrangements are used.

30 AML Committee reporting and management information

Participants learn to design decision-useful AML dashboards covering:

Volume indicators
- Number of alerts.
- Number of cases.
- Number of customer reviews.

Risk indicators
- Sanctions alerts.
- High-risk jurisdictions.
- Merchant-risk cases.
- Network-related investigations.
- Escalations.

Quality indicators
- Missing evidence.
- Quality-assurance failure rate.
- Overturned alert closures.
- Repeat deficiencies.
- Incomplete investigations.

Capacity indicators
- Backlog.
- Alert ageing.
- Resource constraints.
- Cases outside service-level agreements.

Effectiveness indicators
- True-hit rates.
- Conversion of alerts into meaningful cases.
- Scenario coverage.
- Detection gaps.
- Results of scenario tuning.

The module explains why metrics must be supported by trends, thresholds, root causes and management actions.

31 Final takeaways and action planning

The training concludes with three core principles:

1. Design AML controls for the payment environment.
2. Evidence every material decision.
3. Use investigations to improve the wider control framework.

Participants are invited to identify one practical improvement that could be implemented within the following 30 days, such as:
- A clearer investigation template.
- A stronger escalation trigger.
- A new data-quality control.
- An improved merchant-monitoring indicator.
- A more effective AML Committee dashboard.