AML in 90 Minutes:
What Every Professional Should Know

Study Guide

Contents

Aim of the Course

The aim of this course is to provide a clear, practical introduction to how Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) is applied in organisations through a risk-based approach (RBA), how to recognise and interpret common warning signs (“Red Flags”), and how governance arrangements allocate accountability for effective compliance. This course is designed to support consistent, defensible decision-making, appropriate documentation, and timely escalation of concerns in professional settings. It consists of three modules, including: Module 1: Governance & Accountability in AML/CTF, Module 2: Risk-Based Approach in AML/CTF, and Module 3: Common Red Flags in AML/CTF.

Learning Objectives

By the end of this module, you should be able to:

- Explain the risk-based approach (RBA) to AML/CFT at a high level and why it underpins modern compliance.
- Identify common red flags in customer behaviour, transactional activity, and documentation.
- Describe governance and accountability in AML/CFT (key roles, responsibilities, and escalation pathways).
- Apply these concepts to short scenarios to select appropriate next steps (e.g., proceed, request evidence, escalate).

Subject-Specific Knowledge

On successfully completing the module you will be able to:

- Explain what “risk-based approach” means in AML/CFT and distinguish inherent risk vs. residual risk at a basic level.
- Identify the main components of an AML/CFT RBA (e.g., risk identification, risk assessment, controls, monitoring, and review).
- Define what an AML “red flag” is and differentiate indicators from evidence.
- Describe core governance concepts, including accountability, oversight, independence, and effective escalation, including typical role expectations.

Practical And Transferable Skills

On successfully completing the module you will be able to:

- Apply structured thinking to assess whether activity appears inconsistent with expected patterns given a basic customer/context profile.
- Record observations clearly using neutral, factual language and minimum documentation standards (what happened, why it matters, what was checked, what is outstanding).
- Select proportionate actions aligned to the RBA (e.g., request clarification, seek additional documentation, increase monitoring, escalate).
- Follow escalation pathways appropriately, maintaining confidentiality and avoiding inappropriate disclosure.

Core Topics

- High-level risk-based approach
- Common red flags.
- AML/CFT Governance and accountability.

Assessment Description

Assessment is delivered through an open-book online knowledge check designed to confirm your understanding of the core anti-money laundering concepts and your ability to apply them in straightforward work-based situations.

- Format: 10-question online quiz (multiple choice) for each module
- Focus: tests your theoretical knowledge and your practical understanding of how to apply key concepts (for example, recognising red flags and selecting appropriate next steps)
- Pass threshold: 70% (minimum)
- Completion outcome: If you achieve the threshold, you will unlock a simple completion badge and certificate through SwapED.

Module 1: Governance and Accountability

Learning Outcomes:

After completing this learning experience, you will be able to:

- Describe the purpose of the Three Lines of Defence (3LoD) model in an AML control environment.
- Explain the roles and responsibilities of each line in managing and overseeing AML controls.
- Distinguish between operational ownership of controls, compliance oversight and challenge, and independent assurance.

- Map common AML activities to the appropriate line of defence.
- Describe how the three lines interact through escalation, reporting, and assurance.

Introduction: Why 3LoD Matters in AML

Anti-Money Laundering and Combating the Financing of Terrorism governance is the framework that operationalises financial crime compliance. It defines who owns Anti-Money Laundering and Combating the Financing of Terrorism. risk, who sets and oversees the control standards, how issues are escalated, and how senior management and the board receive assurance that controls are effective in practice. It provides clear role definitions and a built-in check-and-challenge process that helps prevent gaps, duplication, and unmanaged risk exposure. Without clear governance and accountability, Anti-Money Laundering becomes inconsistent, reactive, and difficult to evidence to supervisors, auditors, banks, and business partners.

The Three Lines of Defence model is relevant to Anti-Money Laundering and the Combating of the Financing of Terrorism because it structures accountability across the organisation and reduces blind spots. It clarifies that the first line is responsible for day-to-day control execution and risk ownership, the second line provides specialist oversight, sets requirements, and challenges effectiveness, and the third line independently tests whether the governance and controls actually work. This separation supports objectivity. The business implements controls and compliance measures and monitors them. The internal audit provides independent assurance. This separation is essential because Anti-Money Laundering and Combating the Financing of Terrorism risk changes over time, and firms need continuous oversight, escalation routes, and independent assurance, not one-off checks.

In an Anti-Financial Crime programme, this module fits as a core governance component. It connects the “what” of Anti-Money Laundering controls, such as

Customer Due Diligence, screening, transaction monitoring, investigations, and reporting, to the “who” and “how” of accountability, ensuring responsibilities are clear, decisions are documented, and control effectiveness can be demonstrated. In practice, it helps firms translate policies into consistent execution, reliable escalation, and defensible outcomes.

Key points include:

- Governance defines ownership, escalation, reporting, and assurance for Anti-Money Laundering and Combating the Financing of Terrorism.
- 3 Lines of Defence clarifies responsibilities: execute, oversee/challenge, and independently assure.
- Strong 3 Lines of Defence support regulatory expectations and demonstrate the effectiveness of control.
- It integrates directly with wider anti-financial crime controls and the operating model.

The 3 Lines of Defence Model

Line 1 consists of the business and operational teams that interact with customers, process activities, and execute controls. They own the day-to-day Anti-Money Laundering tasks like gathering and maintaining customer due diligence information, following onboarding requirements, escalating concerns, and keeping records. Depending on the organisation’s size, complexity, and operating model, transaction monitoring and alert disposition may sit in the first or second line. Line 2 is the Anti-Money Laundering compliance function, typically including the Money Laundering Reporting Officer. Line 2 sets the framework, including the policies, procedures, guidance, training, and provides oversight, monitoring, and challenge to Line 1. Line 2 also supports governance by aligning the organisation’s Anti-Money Laundering risk appetite and control standards with regulatory expectations. Line 3 is an internal audit, independent of Lines 1 and 2, that evaluates whether the overall Anti-Money Laundering control

environment is designed and operating effectively. The key idea is the separation of roles. Ownership, oversight, and independent assurance work together, but they are not the same job.

Applying 3 Lines of Defence Model in A VASP

Assume a VARA licensed custodial exchange in Dubai that offers AED deposits and USDT purchases. A new corporate customer applies to ABCD Trading LLC. The stated purpose is treasury management and the payment of overseas suppliers in USDT.

Line 1 executes the controls. Onboarding and KYC operations and relationship teams collect corporate documents, confirm ownership and control, identify and verify the ultimate beneficial owner, run sanctions and Politically Exposed Person screening, and apply the firm's risk rating methodology. Line 1 is expected to recognise, document, and escalate red flags, including complex ownership, inconsistent business activity, weak source-of-funds evidence, or higher-risk jurisdictional connections. Where enhanced due diligence is triggered, Line 1 compiles the evidence, documents the rationale, and escalates the case through the defined approval route.

Line 2 provides Anti-Money Laundering compliance oversight and challenge, typically including the Money Laundering Reporting Officer function. Line 2 defines what high risk means for corporate customers, sets enhanced due diligence standards, establishes approval thresholds, and provides guidance to support consistent decision-making. Line 2 conducts compliance monitoring and testing to assess the quality and consistency of first-line execution through file sampling, thematic reviews, and management information analysis. Where weaknesses are identified, Line 2 records findings, sets corrective actions, and tracks remediation to closure.

Line 3 provides independent assurance through internal audit. Audit reviews whether the control framework is appropriately designed for the firm's risk profile and whether controls are operating effectively in practice. Audit selects samples of corporate onboarding files to test whether evidence supports the risk rating, whether approvals occurred at the correct level, and whether screening and record-keeping requirements were met. Audit reports significant findings through an independent route to ensure appropriate senior oversight.

Quality Control Vs Quality Assurance in AML

Quality in Anti-Money Laundering is not only about having policies. It is about delivering consistent, defensible outcomes that are evidence-based.

Quality control focuses on whether the output is correct and complete. In Anti-Money Laundering, outputs include onboarding files, enhanced due diligence packs, alert investigation notes, and escalation records. A quality control check verifies that required evidence is present, screening outcomes are recorded, risk ratings are supported by the facts, rationales are clear, and approvals are properly documented. Quality control is typically applied at the file level to identify errors early and ensure minimum standards are met.

Quality assurance focuses on whether the process works consistently over time. It tests whether the organisation is applying standards reliably across teams and cases. Quality assurance asks whether high-risk triggers are applied consistently, whether enhanced due diligence is used when required, whether escalation happens at the right threshold, whether timeliness standards are met, and whether decisions are defensible across the business. Quality assurance uses sampling and trend analysis to identify recurring weaknesses such as documentation gaps, inconsistent risk ratings, repeated alert-closure reasons, or delays that weaken control effectiveness. Quality assurance supports continuous improvement by identifying patterns that require process change, training, or control redesign.

In simple terms, quality control checks the output and quality assurance checks the process. Both are needed. Quality control reduces individual errors, and quality assurance identifies systemic weaknesses that require remediation.

Line 2 in Practice: AML Compliance Monitoring & Testing

The second line of defence is the Anti-Money Laundering compliance function, typically including the Money Laundering Reporting Officer. Its purpose is to establish and maintain the Anti-Money Laundering framework and oversee whether first-line controls are implemented effectively.

Compliance monitoring provides ongoing oversight to confirm that teams follow internal requirements and applicable expectations. Testing provides structured reviews to assess whether controls are operating as designed and whether they are effective in practice. The second line does not replace the first line. It independently reviews the quality, consistency, and effectiveness of first-line work.

Monitoring and testing should produce clear, documented findings and corrective actions. Where weaknesses are identified, the organisation should define what failed, why it failed, who owns remediation, and how effectiveness will be confirmed after changes are implemented.

MLRO Role And Escalation Route

The Money Laundering Reporting Officer sits within the second line of defence and plays a central role in governance and escalation. The role ensures that suspicions are escalated appropriately, decisions are taken consistently, and reporting obligations are met. The Money Laundering Reporting Officer also provides senior visibility of material Anti-Money Laundering risks, control weaknesses, and emerging issues.

Escalation should be disciplined and evidence-led. The first line escalates concerns that cannot be reasonably resolved, supported by a documented rationale and an evidence pack. The second line reviews and challenges the case to ensure that standards have been applied correctly and that the escalation threshold has been met. Where suspicion is formed or cannot be ruled out, the case is escalated to the Money Laundering Reporting Officer for decision-making and governance of the reporting pathway. Material risk issues and repeated control weaknesses should be escalated through management reporting to senior management and, where appropriate, the board or relevant committee.

Let us look at an example escalation scenario. A VARA-licensed custodial exchange in Dubai onboards a corporate customer approved for an expected activity profile.

Two weeks later, the activity deviates from what was expected. The customer deposits a large amount of AED, buys USDT rapidly, and attempts to withdraw most of it shortly after. The destination wallet is flagged by blockchain analytics as high-risk, and the customer’s explanation and supporting documents do not credibly support the transaction's purpose.

First-line escalation involves opening a case, documenting the transaction timeline, recording on-chain indicators and customer profile details, capturing communications, applying internal procedures, and escalating when suspicion cannot be reasonably ruled out.

Second-line review and challenge involves checking the completeness and quality of the evidence, challenging gaps in the rationale or documentation, confirming the escalation threshold, and routing the case to the Money Laundering Reporting Officer.

The Money Laundering Reporting Officer's decision involves reviewing the full evidence pack, determining whether the suspicion threshold is met, documenting the decision, and governing the reporting pathway in line with requirements.

Senior escalation applies where the value or risk exposure is material. The matter is summarised for senior management and, where appropriate, the board or relevant committee, with a focus on risk implications, control weaknesses, and remediation actions.

Line 3: Internal Audit

The third line of defence is the internal audit. It is independent from both the first and second lines and provides objective assurance on the effectiveness of risk management, governance, and control systems within the organisation’s anti-financial crime framework.

Internal audit does not operate controls or supervise daily compliance activities. Its role is to independently assess whether the controls designed and operated by the first and second lines are appropriate for the organisation’s risk profile and whether those controls are functioning effectively.

Independence is essential for credibility. For this reason, the independent audit function typically reports to the audit committee or the board of directors, ensuring that significant control weaknesses are appropriately escalated and not influenced by operational priorities.

Internal audit provides assurance through planned audits that evaluate the design and effectiveness of key controls, assess whether processes align with required standards, and communicate deficiencies for remediation. Where an organisation does not have sufficient internal resources, the independent audit function may be performed by external auditors, provided the work remains objective and sufficiently competent to evaluate the anti-money laundering and counter-terrorist financing programme.

How The 3 Lines Interact

The Three Lines of Defence model is most effective when treated as an operating system rather than an organisational chart.

The first line executes controls and creates evidence, including customer information, screening results, investigation notes, decision rationales, and escalation records. When issues cannot be resolved operationally, the first line escalates them through the defined pathways.

The second line converts risk expectations into practical requirements and oversight. It sets minimum standards, provides guidance, challenges first-line decisions when evidence is weak, and consolidates monitoring results into management information that supports decision-making and remediation tracking.

The third line independently evaluates whether governance and controls are effective across the organisation. It assesses the overall control environment, including whether the first and second lines are fulfilling their responsibilities, and whether remediation is effective over time.

When the interaction is clear, responsibilities are not duplicated unnecessarily, control gaps are reduced, and escalation becomes more reliable. This strengthens governance, supports defensible decision-making, and improves operational resilience.

AML Activity Map: Who Does What

An anti-money laundering activity map is a structured way to allocate core anti-money laundering tasks across the Three Lines of Defence. Its purpose is to translate the model from a governance concept into operational clarity by showing, for each activity, who executes the task, who provides oversight and challenge, and who provides independent assurance. It is a practical tool for

documenting accountability and supporting consistent execution of controls across teams.

In practice, the map helps prevent two common failures. Gaps in which critical activities are not clearly owned, and duplication in which multiple functions perform the same task without clear accountability. By clarifying ownership and escalation routes, it strengthens governance and supports defensible decision-making. It also supports effective governance by ensuring that responsibilities align with each line's intended role.

The first line of defence owns and performs day-to-day Anti-Money Laundering controls. This typically includes conducting customer due diligence, applying screening steps, handling alerts and investigations in accordance with procedure, documenting decisions, and escalating concerns. The first line is responsible for creating the evidence trail that shows how Anti-Money Laundering decisions were made.

The second line of defence establishes and maintains the Anti-Money Laundering framework and provides oversight and challenge, including the Money Laundering Reporting Officer function. This includes setting policies and standards, advising and challenging the first line, setting training expectations, conducting monitoring and testing, analysing management information, and ensuring escalation and reporting governance operates correctly. The second line assesses whether first-line controls are applied consistently and whether remediation is implemented effectively when weaknesses are found.

The third line of defence provides independent assurance over governance, risk management, and control effectiveness. This includes evaluating whether controls are appropriately designed and operating effectively over time, and reporting findings through an independent route, typically to the audit committee or board. The third line provides objective assurance that oversight arrangements

are credible and that control weaknesses are identified and escalated appropriately.

A well-designed activity map is commonly presented as a table showing activities against lines of defence and may be supported by a responsibility assignment approach that clarifies who is responsible, accountable, consulted, and informed. The result is a usable reference that improves coordination, reduces ambiguity, and supports consistent, auditable Anti-Money Laundering outcomes.

Common Gaps & Consequences

A frequent gap is when the first line does not truly own controls and assumes compliance will catch problems. This leads to inconsistent execution, weak evidence trails, and late escalation. Another gap is inconsistent escalation thresholds and poor documentation, which makes decisions difficult to defend and makes patterns harder to detect. A further gap occurs when monitoring identifies issues, but remediation is weak, leading to actions that are not clearly owned, deadlines that slip, and problems that persist. Finally, repeated audit findings across cycles indicate that governance is not translating into operational improvement. These issues typically signal unclear accountability and ineffective control assurance.

The consequences are predictable: control weaknesses, higher exposure to financial crime risk, more serious regulatory findings, and a greater likelihood of enforcement outcomes. In parallel, reputational harm and operational disruption increase. The value of the Three Lines of Defence is that it reduces these outcomes by clarifying ownership, strengthening oversight, and ensuring independent assurance. It strengthens accountability by making ownership and challenge visible and testable.

Boundaries: What Each Line Should Not Do

The Three Lines of Defence work only when the boundaries are respected. Boundaries do not reduce cooperation. They protect accountability. Clear boundaries prevent conflicts of interest and reduce the risk that oversight functions end up reviewing their own work.

The first line should not treat anti-money laundering as someone else's job. It must own control execution and evidence creation. If the first line shifts responsibility to the second line, control becomes inconsistent, and escalation is delayed.

The second line should not become the operational owner of routine onboarding decisions or routine alert handling. Its role is to set requirements, guide, monitor, test, and challenge. If it takes over routine operations, accountability blurs, bottlenecks grow, and oversight becomes less credible because the second line begins reviewing work it has performed. This weakens oversight independence and reduces the reliability of monitoring outcomes.

The third line should not design controls, run monitoring, or manage remediation execution. Internal audit must remain independent so that its assurance is objective. If an audit designs or operates controls, it weakens independence and undermines trust in audit conclusions. Audit should evaluate, not operate.

Escalation & Reporting Flow

Showing how information and decisions move through the Three Lines of Defence is essential. An effective anti-money laundering programme depends on timely escalation, clear decision-making, and reliable reporting. Escalation routes should be defined, consistently applied, and supported by documented evidence.

Concerns typically originate in the first line of defence, for example, unusual customer behaviour, inconsistent information, a screening match, or an alert

outcome that cannot be reasonably explained. The first line documents the issue, compiles supporting evidence, records the rationale, and escalates the matter through the defined route when it cannot be resolved operationally. This ensures risk ownership begins at the point of origination.

The second line of defence provides oversight and challenge. It reviews the case to confirm that requirements have been applied correctly, assesses the quality and consistency of the first-line analysis, and determines whether further escalation is required. Where suspicion is identified or cannot be ruled out, the case is escalated to the Money Laundering Reporting Officer for decision-making and governance of the reporting pathway. The second line also ensures that outcomes, issues, and remediation are reflected in management reporting.

In parallel, the internal audit provides independent assurance that escalation and reporting mechanisms are appropriately designed and functioning effectively. Audit reporting is delivered to the audit committee or board to preserve independence. Together, this creates a closed loop: execution, oversight, escalation, reporting, and independent assurance. This interaction strengthens accountability and helps ensure that weaknesses are identified, escalated, and corrected.

Defining The Governance And Accountability In Practice

Case Study:

ABCD Trading LLC is a corporate customer onboarding remotely with a VARA-licensed exchange in Dubai, stating it will use the platform to pay overseas suppliers in USDT. Although the customer is rated medium risk, the account is approved with weak documentation. Within days, a large AED deposit is converted to USDT and withdrawn to a new external wallet, and an alert is closed as “explained” with minimal recorded rationale. When compliance requests the case file, the evidence pack is incomplete, and compliance begins redoing

onboarding checks and rewriting the rationale, indicating unclear ownership and weak governance across the Three Lines of Defence.

- Which issues in this scenario indicate poor governance or blurred accountability across the three lines?
- What should Line 1 have done differently at Day 1 and Day 4?
- What is the correct role of Line 2 at Day 6 and Day 7, and what should it avoid doing?
- What should Line 3 assess at Day 10, and what evidence should it expect to see?
- Create a short AML activity map for this case: list the key activities and assign them to Line 1, Line 2, or Line 3.

The first line approved onboarding with weak documentation and later closed an alert with minimal rationale, undermining the evidence trail and making decisions hard to defend. The inability to produce a complete evidence pack when requested shows weak recordkeeping and unclear ownership. Compliance then starts redoing onboarding checks and rewriting the rationale, blurring the separation between operational execution and oversight, and creating a self-review risk for the second line.

On Day 1, Line 1 should ensure that onboarding requirements are met before approval, including complete Know-Your-Customer and ownership evidence, a supported risk rating, and clear documentation of the rationale and approvals. If evidence was insufficient, it should have held the case, applied Enhanced Due Diligence if triggered, or escalated through the defined route. On Day 4, Line 1 should have investigated the alert against the expected profile, documented the checks performed and the conclusion, and escalated if the activity could not be reasonably explained, rather than closing it with a minimal rationale.

At Day 6, Line 2 should review and challenge the first line's work by assessing whether standards were applied, whether the risk rating and alert closure were

supported by evidence, and whether escalation thresholds were met. It should raise findings, require corrective actions, and set remediation deadlines. At Day 7, Line 2 should avoid re-performing routine onboarding checks or rewriting the first line's rationale as the operational owner. Instead, it should require Line 1 to remediate the file, strengthen documentation, and re-assess the case under supervision, while Line 2 validates the outcome through oversight.

Line 3 should assess whether the control environment and governance are functioning as designed, including whether onboarding and alert-handling controls are consistently executed, whether escalation routes are working, and whether Line 2 oversight remains independent. It should expect to see complete onboarding files, risk assessment rationale, alert investigation notes, decision records, escalation logs where applicable, compliance monitoring or testing results, documented findings, and evidence that remediation actions were owned, time-bound, and verified.

Line 1 should own onboarding execution, risk rating application, screening and alert investigation, documentation of rationale and approvals, and escalation when unresolved. Line 2 should own policy and standards-setting, oversight, and challenge of onboarding and alert quality; monitoring and testing; findings and remediation tracking; and Money Laundering Reporting Officer governance for suspicion and reporting decisions, where required. Line 3 should own independent audits of onboarding, monitoring, escalation, and reporting effectiveness, and report significant issues to senior governance through an independent route.

Key Takeaways

Effective AML programmes depend on clear accountability. The first line executes controls and creates the evidence trail. The second line sets standards and provides oversight and challenge, including Money Laundering Reporting Officer escalation and reporting governance. The third line independently tests

whether controls and governance work in practice. It also highlights the value of an Anti-Money Laundering activity map to allocate responsibilities and prevent gaps or duplication, and emphasises that the model only works when boundaries are respected, and escalation and reporting are evidence-led.

Module 2: The Risk Based Approach in AML/CTF

Learning Outcomes:

After completing this learning experience, you will be able to:

- Explain what the risk-based approach means in AML and CFT.
- Describe why financial crime risk is not uniform and why controls must be proportionate to risk.
- Distinguish between inherent risk, the effectiveness of controls, and residual risk.
- Explain the role of risk appetite and senior governance in setting boundaries and control expectations.
- Identify key risk drivers, including customer risk, product and service risk, geographic risk, and delivery channel risk.
- Describe how risk level influences due diligence measures, monitoring intensity, and escalation expectations.

Introduction: Why Risk-Based Approach (RBA)?

The risk-based approach exists because exposure to money laundering and terrorist financing risk is not uniform. Some customers, products, services, and transactions are relatively straightforward, transparent, and predictable. Others involve complexity, speed, opacity, or geographic exposure, which increase the likelihood of misuse.

If an organisation applies identical controls with identical intensity to every case, two outcomes follow. First, resources are consumed on lower-risk activities that do not require heightened scrutiny. Second, higher-risk areas may be under control, making red flags more likely to be missed and escalation too late. This is not only an efficiency issue. It is a risk management and governance issue.

The risk-based approach addresses this by aligning the strength of controls with the level of risk. It supports consistent decision-making, clearer escalation expectations, and more effective allocation of monitoring and oversight efforts. It also strengthens the organisation’s ability to explain and evidence why a particular level of due diligence, monitoring, restriction, or approval was applied in a given case.

In this module, we focus on risk assessment as the foundation of an effective AML and CFT programme. We will examine what a risk assessment is, the main types used in practice, and the fundamental components that regulators expect to see. We will explore inherent risk, assess the effectiveness of control measures, and determine residual risk to understand how risk changes once controls are applied.

By assessing risk levels and threats in a structured way, organisations improve decision-making, allocate resources more effectively, and demonstrate that their AML and CFT controls are proportionate and defensible. The risk assessment process is the backbone of a strong anti-financial crime risk management programme, and it directly informs customer due diligence, monitoring intensity, escalation thresholds, and senior governance boundaries.

What The Risk-Based Approach Means For AML/CTF

The risk-based approach in Anti-Money Laundering and Countering the Financing of Terrorism involves identifying where money laundering and terrorist financing risks are higher or lower, and applying controls that are proportionate to

those risks. Due to the fact that risk is not uniform across customers, products, services, and transactions, the approach focuses resources on higher-risk areas through stronger due diligence, enhanced monitoring, and clearer escalation, while applying simpler measures where risk is lower. It also ensures that decisions are consistent and defensible by documenting the rationale for the level of scrutiny or restriction applied in each case.

Risk Appetite & Governance

The risk-based approach begins with governance, and a central governance concept is risk appetite. Risk appetite is the level and type of money laundering and terrorist financing risk that an organisation is willing to accept in pursuit of its objectives, within the boundaries of applicable law and regulatory expectations. It is not a generic statement of intent. It is a strategic position that defines what the organisation will do, what it will not do, and what it will do only under enhanced conditions, such as tighter controls, additional approvals, and closer monitoring.

Risk appetite should be visible in policies, procedures, and day-to-day operating decisions. In practice, it shapes customer acceptance criteria and onboarding restrictions, including which sectors, jurisdictions, and customer types are prohibited, restricted, or subject to enhanced due diligence. It also influences escalation thresholds and approval requirements, such as when a relationship must be escalated to compliance or the MLRO, when senior management approval is required, and what conditions must be met before a higher-risk customer can be onboarded or retained. Risk appetite further informs product and channel design, including whether certain services are offered at all, what transactional limits apply, which delivery channels require additional verification, and how monitoring scenarios and alert priorities are calibrated.

This is why senior management and board oversight are essential. A risk-based approach cannot be effective if it exists only as a compliance statement or a document created for audit purposes. It must be embedded in governance and

decision-making, including how the organisation allocates resources to controls, how it measures control effectiveness, and how it reports risk exposure, breaches, and remediation progress upward. Effective oversight ensures accountability for the risk appetite, challenges whether it remains appropriate as risks evolve, and confirms that operational practice aligns with the organisation's stated risk boundaries.

Risk Equation: Inherent Risk, Controls, & Residual Risk

Risk assessment in Anti-Money Laundering and Combating the Financing of Terrorism can be summarised with a simple equation. Inherent risk is the baseline exposure before any controls are applied. It is driven by factors such as customer profile, products and services used, geographic exposure, and delivery channel.

Controls are the measures the organisation uses to reduce that baseline risk. Control effectiveness is not just whether a control exists on paper, but whether it is appropriately designed, consistently applied, and proven to work in practice. Examples include customer due diligence and enhanced due diligence, sanctions and Politically Exposed Persons (PEPs) screening, transaction monitoring, alert investigation, escalation, and suspicious reporting when required.

Residual risk is what remains after controls are applied. This is the risk level the organisation must actively manage and, where appropriate, accept within its risk appetite. If residual risk is above the organisation's risk appetite, the response must change. That may mean applying stronger due diligence, increasing monitoring intensity, imposing limits or restrictions, requiring higher-level approvals, or exiting the relationship.

The key point is that AML decisions should be anchored in residual risk, as it reflects both exposure and the actual effectiveness of controls. Risk assessment in Anti-Money Laundering and Combating the Financing of Terrorism can be

summarised with a simple equation. Inherent risk is the baseline exposure before any controls are applied. It is driven by factors such as customer profile, products and services used, geographic exposure, and delivery channel.

Controls are the measures the organisation uses to reduce that baseline risk. Control effectiveness is not just whether a control exists on paper, but whether it is appropriately designed, consistently applied, and proven to work in practice. Examples include customer due diligence and enhanced due diligence, sanctions and Politically Exposed Persons (PEPs) screening, transaction monitoring, alert investigation, escalation, and suspicious reporting when required.

Residual risk is what remains after controls are applied. This is the risk level the organisation must actively manage and, where appropriate, accept within its risk appetite. If residual risk is above the organisation's risk appetite, the response must change. That may mean applying stronger due diligence, increasing monitoring intensity, imposing limits or restrictions, requiring higher-level approvals, or exiting the relationship.

The key point is that AML decisions should be anchored in residual risk, as it reflects both exposure and the actual effectiveness of controls.

Risk Decisions: Accept, Mitigate, Avoid

Risk decisions are the practical outcome of a risk-based approach. Once inherent risk has been assessed, controls have been evaluated, and residual risk has been determined, the organisation must make a clear decision that aligns with its risk appetite and regulatory expectations. In Anti-Money Laundering and Combating the Financing of Terrorism, there are three core decision paths: accept, mitigate, or avoid.

Accept means the organisation proceeds because the residual risk is within its risk appetite and the control environment is assessed as effective. Acceptance is not passive. It requires documentation of the rationale, clear ownership of

ongoing monitoring, and defined triggers for reassessment if the risk profile changes.

Mitigate means the organisation proceeds only if additional measures reduce residual risk to an acceptable level. In practice, mitigation may include enhanced due diligence, stronger evidence of source of funds and source of wealth, tighter transaction limits, increased monitoring intensity, additional approvals, more frequent reviews, or specific restrictions on products, jurisdictions, or counterparties. The decision to mitigate should specify which measures are required, who is accountable, and how effectiveness will be verified.

Avoid means the organisation does not proceed, or exits an existing relationship, because the risk cannot be reduced to within risk appetite, the required evidence cannot be obtained, the customer's behaviour is inconsistent or non-transparent, or the exposure is prohibited by policy or law. Avoid also applies where control effectiveness is insufficient to manage the risk, or where repeated issues indicate that the relationship cannot be safely maintained.

The core discipline is that these decisions must be consistent, evidence-based, and escalated at the appropriate level. Where residual risk is higher, decisions should be subject to stronger governance, clearer documentation, and more senior approval.

Proportionate Controls: What Changes When Risk Is Higher

Proportionate controls are the practical expression of the risk-based approach. Once risk has been assessed, the organisation should adjust the strength of its controls so that higher-risk exposures receive stronger measures and lower-risk exposures are managed through standard measures that remain compliant and effective.

Where risk is higher, organisations apply enhanced controls. This typically includes enhanced due diligence, deeper verification of ownership and control,

stronger evidence of sources of funds and wealth where relevant, more stringent approval requirements, and tighter restrictions on certain products, jurisdictions, counterparties, or transaction types. Ongoing monitoring also becomes more intensive, meaning closer scrutiny of activity against the expected profile, more frequent reviews, and clearer escalation triggers when activity is unusual or inconsistent.

Where risk is lower, organisations still apply required controls, but the depth and frequency of checks are proportionate to the risk profile. Lower risk does not mean no controls. It means standard due diligence and routine monitoring may be sufficient where the relationship is transparent, the expected activity is clear, and behaviour remains consistent over time.

Proportionality must remain defensible. The organisation should be able to explain and evidence why a particular level of due diligence, monitoring intensity, and restriction was applied in a given case. This is also where escalation expectations become clearer. As risk increases, escalation thresholds tighten, approval levels become more senior, and documentation standards become more important because decisions must be credible, consistent, and auditable.

Key Risk Drivers in AML

To apply a risk-based approach in Anti-Money Laundering and Combating the Financing of Terrorism, learners need a clear understanding of the common drivers of financial crime risk. Risk is not random. It increases when transparency is lower, structures are more complex, activity is faster, and exposure is more cross-border.

Customer risk relates primarily to transparency and behaviour. It includes who the customer is, how clearly ownership and control can be verified, whether the relationship's purpose is credible, and whether expected activity aligns with observed activity. Higher customer risk often appears where ownership

structures are complex or opaque, information is inconsistent, the customer is reluctant to provide evidence, or behaviour changes without a clear explanation.

Product and service risk reflects how a product can be misused. Services that enable rapid value movement, high transaction volumes, frequent third-party transfers, or limited transparency increase exposure when controls are weak. In practical terms, products that support quick conversion, layering, or cross-border value movement often require stronger monitoring, tighter limits, and clearer escalation standards.

Jurisdiction risk reflects where the customer is based and where value flows to and from. Geographic exposure matters because jurisdictions vary in the level of financial crime threat, sanctions exposure, regulatory maturity, and law enforcement cooperation. Risk increases where funds move through higher risk corridors, where beneficial ownership transparency is weaker, or where there are elevated sanctions, corruption, or organised crime concerns.

Delivery channel risk reflects how the service is accessed. Non-face-to-face onboarding, remote transactions, and reliance on introducers or intermediaries can increase impersonation risk and reduce verification quality unless robust controls are in place. Strong channel controls typically include effective identity verification, liveness and fraud checks where appropriate, device and behavioural signals, and stronger controls around account changes and withdrawals.

The goal is not to memorise lists. The objective is to understand the logic behind risk-based thinking. As transparency decreases and complexity, speed, or cross-border exposure increases, controls must become more robust, monitoring more targeted, and escalation more disciplined.

Types of Risk Assessments

A risk-based approach operates across interconnected levels of assessment. Risk does not exist only at the level of an individual customer. It also exists at the organisational, sectoral, and jurisdictional levels at which the organisation operates. Effective AML and CFT programmes align these layers so that strategic risk priorities are reflected in day-to-day control decisions.

At the enterprise-wide level, an enterprise-wide risk assessment evaluates the organisation's overall exposure across customer types, products and services, geographies, and delivery channels. This assessment supports programme design and governance. It informs where stronger controls are required, how monitoring should be prioritised, where resources and expertise should be strengthened, and how risk appetite should be operationalised through policies, limits, and approval thresholds. In a mature programme, the enterprise-wide view follows a risk logic that establishes inherent risk, assesses control effectiveness, determines residual risk, and translates results into a clear action plan for mitigation and continuous improvement.

At the customer level, customer risk assessment applies the same logic to each relationship. The organisation assigns a customer risk rating based on relevant risk drivers and the expected activity profile. That rating determines the level of due diligence required, whether enhanced due diligence is needed, the intensity of ongoing monitoring, the frequency of periodic reviews, and the escalation and approval requirements for onboarding and ongoing activity. Customer level assessments ensure that controls are proportionate and consistently applied.

These levels should be informed by wider external risk signals. National risk assessments identify jurisdiction-level money laundering and terrorist financing threats and highlight higher-risk sectors and typologies. Sectoral risk assessments analyse industry-specific risks and vulnerabilities. Enterprise-wide risk assessment should consider these external assessments for any jurisdiction

or sector in which the organisation operates or plans to operate, so that internal controls are calibrated to real-world exposure and supervisory expectations.

The core concept is alignment. Enterprise-wide assessment sets the organisation's priorities, control standards, and resource allocation. Customer level assessment determines how those standards are applied in practice. When the two are misaligned, organisations either under- or over-control higher-risk exposure, or over-control lower-risk activity, without improving outcomes. When they are aligned, firms can allocate resources efficiently, apply targeted measures in higher-risk areas, and demonstrate a defensible risk-based programme that meets regulatory expectations.

Keeping Risk Assessments Up-To-Date

A risk-based approach is not a one-time decision. Money laundering and terrorist financing risks evolve as the business model evolves and external threats, typologies, and regulatory expectations develop. This means organisations need periodic reassessment and reassessment when there is a material change that could alter exposure.

Material change can include launching a new product or service, entering a new geography, introducing new delivery channels such as remote onboarding, changing key controls or systems, onboarding new customer segments, using new intermediaries, or experiencing significant shifts in transaction volumes, patterns, or counterparties. External change can include new legal or supervisory expectations, changes in sanctions regimes or enforcement intensity, updated national or sectoral risk assessments, and emerging financial crime typologies that affect the organisation's products or customer base.

When risk shifts, controls should adjust accordingly. Risk appetite boundaries and acceptance criteria may need to be clarified; due diligence standards may need to be strengthened or refined; monitoring scenarios and thresholds may

need to be recalibrated; and escalation triggers and approval requirements may need to be updated. Governance reporting should also reflect changes in exposure, control performance, and remediation progress so that senior management can challenge and resource the programme appropriately.

The core message is continuous alignment. A risk-based approach remains credible only when it stays connected to real exposure, is supported by current evidence, and is updated promptly when circumstances change.

Assurance & Effectiveness

Assurance is how an organisation demonstrates that its risk-based approach works in practice. A risk-based programme requires more than written policies and control steps. It requires evidence that controls are operating effectively, that weaknesses are identified early, and that remediation is implemented and verified.

Effectiveness should be assessed through routine oversight. Monitoring and testing help confirm whether controls operate as intended across the customer lifecycle. This includes reviewing whether risk ratings and due diligence decisions are consistent and supported by evidence, whether enhanced due diligence is applied when required, whether screening outcomes are handled appropriately, whether alerts are investigated to an acceptable standard, and whether escalation occurs when it should. Oversight also examines timeliness, backlogs, and recurring defects that signal control weakness or resourcing constraints.

Assurance must also cover outcomes, not only processes. Organisations should be able to demonstrate that controls produce defensible results, for example, that higher risk cases receive stronger measures, that unusual activity is detected and escalated, and that decisions are documented in a way that is auditable and consistent with policy. Where issues are identified, remediation should be clearly

owned, time-bound, and tracked to closure, with follow-up testing to confirm the weakness has been addressed.

Independent assurance strengthens credibility. Internal audit, or an equivalent independent function, provides an objective evaluation of governance and control effectiveness across the first and second lines. This independence is important for senior management and board reporting because it reduces reliance on self-assessment and provides confidence that significant weaknesses will be escalated and addressed.

The core message is that the risk-based approach is sustainable only when it is supported by evidence, oversight, independent assurance, and continuous improvement.

RBA in Practice

Case Study:

ABCD LLC is a corporate customer applying to a VARA-licensed exchange in Dubai through remote, direct onboarding. The customer states that it will use the platform to pay overseas suppliers in USDT, with expected monthly activity of around AED 1,500,000 and a simple pattern of two transfers per month to two named suppliers. Based on this information, the customer is initially rated medium risk.

During the first week, the activity deviates from the stated plan. On day 1, the customer requests higher withdrawal limits immediately after activation. On day 2, it deposits AED 1,400,000 from a UAE bank account that was not disclosed as an expected funding source, converts to USDT, and sends it to a wallet address not shown on the supplier invoice. On day 4, a second deposit of AED 1,600,000 arrives from a different UAE account, is converted, and is withdrawn the same day to a new external wallet.

By day 6 and day 7, documentation and monitoring signals reinforce the mismatch. The invoices provided do not align with the wallet beneficiary details previously provided, and monitoring alerts are triggered due to rapid in-and-out behaviour and counterparty inconsistencies.

- What should the updated risk rating be now, and why?
- Would you accept, mitigate, or avoid at this stage, and what proportionate steps would you apply immediately?

The updated risk rating should be high. The customer's observed behaviour is inconsistent with the declared purpose and expected activity profile. Specifically, the customer stated that USDT payments would be made to two named suppliers, yet the withdrawals were sent to wallet addresses that do not appear on the supplier invoices. In parallel, the funding pattern shifted immediately, with large deposits coming from different UAE bank accounts, including at least one account that was not disclosed as an expected funding source. Combined with rapid same-day conversion, external withdrawals, and early requests for higher limits, the overall risk profile increases materially.

The correct decision path at this stage is mitigate, on a strictly conditional basis. The firm should not accept the relationship as is, as the residual risk is not yet within appetite due to counterparty and funding inconsistencies. Equally, an immediate avoidance decision is not always necessary if the firm can apply additional controls to bring the risk back within acceptable boundaries, provided the customer can promptly provide credible evidence.

Mitigation should be practical and targeted to the red flags. The firm should pause any limit increase and restrict external withdrawals until key points are verified. Enhanced due diligence should focus on establishing a defensible link between the declared suppliers and the destination wallets, and on explaining and evidencing the use of multiple funding accounts. Monitoring should be intensified, and all rationale clearly documented. The case should be formally

escalated to compliance or the Money Laundering Reporting Officer (MLRO) for review, including consideration under the firm's internal Suspicious Transaction Report (STR) or Suspicious Activity Report (SAR) decisioning process. If the customer cannot resolve the inconsistencies quickly and convincingly, the appropriate outcome is avoidance, meaning decline of onboarding or exit from the relationship.

Key Takeaways

The risk-based approach means you do not treat every case the same. You apply stronger controls where Money Laundering / Terrorism Financing risk is higher and standard controls where risk is lower. You have to follow a clear risk logic. Start with inherent risk, assess how adequate your controls are in practice, then determine residual risk. Residual risk is what you actually manage day to day. Let risk appetite guide decisions. Risk appetite sets the boundaries for what the organisation will accept, restrict, or avoid. Senior leadership oversight is needed so these boundaries show up in real onboarding, monitoring, escalation, and approval decisions. Know the main risk drivers. Higher risk usually stems from lower transparency, greater complexity, speed, or cross-border exposure. The core drivers are customer risk, product and service risk, jurisdiction risk, and delivery channel risk. Turn risk into action. The risk assessment must lead to a clear outcome: proceed, proceed with additional mitigation, or do not proceed. As risk increases, due diligence, monitoring, documentation, and approval levels should increase too. Keep it current and prove it works. Risks change, so assessments and controls need regular review and updates after material changes. Assurance then checks that controls are working, that issues are fixed, and that outcomes are auditable, including an independent review where needed.

Module 3: Common Red Flags in AML/CTF

After completing this learning experience, you will be able to:

- Define what a red flag is in Anti-Money Laundering and Counter-Terrorist Financing
- Identify common red flags across customers and transactions
- Explain why a red flag is a trigger for action, not a conclusion
- Describe the expected response: document, review, escalate, and report where required

Introduction: What is a Red Flag?

A red flag is a warning sign of an observed behaviour, transaction, or pattern that is inconsistent with what is known about the customer, the stated purpose of the relationship, or the expected activity profile. Red flags exist to prompt proportionate review because financial crime often first appears as inconsistency, unusual patterns, or avoidance of transparency.
A single red flag may have a legitimate explanation. Risk increases when red flags accumulate, documentation is weak, explanations are inconsistent, or the customer resists reasonable verification.

Where Red Flags Typically Occur

Red flags typically appear at predictable points in the customer and transaction lifecycle. They are rarely isolated events. They usually emerge when there is a mismatch between who the customer is, what they say they will do, and what actually happens in behaviour, payments, or documentation.

Common points where red flags occur include:

- Customer onboarding and identity verification when information is inconsistent, incomplete, or difficult to verify
- Beneficial ownership and control assessment when structures are complex, or transparency is limited

- Source of funds and source of wealth assessment when funding is unclear, disproportionate, or inconsistent with the profile
- First transactions after onboarding, when activity deviates from the expected purpose or pattern
- Ongoing monitoring when transaction volume, velocity, counterparties, or geographies shift without a credible explanation
- Payment and transfer instructions when information is missing, altered, or designed to reduce transparency
- Use of intermediaries and third parties when the true originator or beneficiary is unclear
- Account and profile maintenance when sudden changes occur in address, device, contact details, or ownership without a clear rationale
- Escalation and investigation stages when the customer applies pressure, secrecy, or urgency and resists reasonable questions

Using Red Flags Responsibly

Red flags should drive consistent action, not assumptions.

A disciplined approach is:

- Confirm facts and context against the expected activity profile and history.
- Obtain targeted clarification and relevant supporting evidence where permitted.
- Document what was observed, what checks were completed, and the rationale for the outcome.
- Escalate when concerns cannot be reasonably resolved, or suspicion is formed.
- Maintain confidentiality and avoid tipping off at all stages.

Recognizing Higher Risk

A practical way to recognise higher Anti-Money Laundering and Combating the Financing of Terrorism risk is to look for misalignment, weak transparency, and patterns that reduce traceability.

Start with misalignment. If an activity does not fit the customer's profile, stated purpose, income, or business model, it constitutes a profile mismatch. A related indicator is an unexplained change in behaviour, where volumes, corridors, counterparties, or product use shift suddenly without a credible, evidenced reason.

Next is funding transparency. An unclear or unsupported source of funds means the origin of funds cannot be consistently explained or supported to a reasonable standard. Cash intensity without a rationale increases concern because cash is harder to trace, and high or frequent cash activity should be consistent with the customer profile and stated activity.

Then consider who controls the relationship. Ownership or control opacity arises when the ultimate beneficial owner cannot be identified or verified due to shells, nominees, or layered entities. Avoidance behaviour strengthens concern when the customer resists reasonable questions, provides evasive answers, or withholds information.

Finally, focus on transaction patterns that reduce traceability. Higher-risk jurisdiction exposure increases risk when customers, counterparties, or flows link to corridors with elevated financial crime or sanctions risk. Transaction structuring involves splitting activity into smaller movements to avoid thresholds or detection. Rapid movement of funds involves inflows and outflows, quick conversion, and fast withdrawals that resemble layering. Payment transparency gaps include missing or inconsistent originator or beneficiary information or instructions that obscure who is involved.

The professional response is always evidence-led: confirm facts, request targeted clarification where permitted, document the rationale, and escalate when issues cannot be resolved, or suspicion is formed.

Common Red Flags in AML/CTF

Fraud Red Flags

Fraud red flags are indicators that a person or entity may be attempting to obtain funds through deception rather than legitimate economic activity. In many fraud typologies, the objective is not to move illicit proceeds through complex structures, but to persuade the victim to transfer money quickly and with minimal scrutiny. For this reason, fraud indicators often appear in the language used, the sales approach, and the conditions attached to the offer.

Common fraud red flags include:

- Something sounds too good to be true
- Promised high returns for low investment or limited risk
- Requests for upfront payments before services, access, or returns are delivered
- Artificial scarcity is created to push commitment, such as limited slots or exclusive access
- Secrecy, including requests not to share details or to avoid “formal channels”
- Urgency, including deadlines framed as penalties or missed opportunities
- Pressure to act immediately, discouraging verification or independent advice

Sanctions Evasion Red Flags

Sanctions evasion red flags are indicators that a person or entity may be attempting to bypass sanctions restrictions by obscuring who is involved in a transaction, where goods or value are moving, or who ultimately owns or controls the relevant party. Unlike many financial crimes that focus on profit, sanctions evasion often prioritises concealment and misdirection to avoid screening, interdiction, or regulatory detection. The common pattern is a deliberate reduction of transparency across payments, trade documentation, and ownership information.

Common sanctions evasion red flags include:

- Identifying details were removed or altered in payment instructions to avoid effective screening
- Use of nested and payable accounts that reduce visibility of underlying parties
- Shell companies are used to conceal sanctioned ownership, control, or counterparties
- Transshipment tactics, including rerouting through opaque transit points or switching cargo at sea, to disguise the true origin or destination
- Complex ownership structures using proxies or bearer shares to obscure beneficial ownership and designated party links

Terrorist Financing Typology Red Flags

Terrorist financing risk involves the movement or use of funds to support terrorist activity, individuals, or networks. Unlike many money laundering cases that involve large proceeds from crime, terrorist financing can involve smaller amounts, fragmented transfers, and the use of multiple methods to move value across borders while reducing visibility. The objective is typically to enable operational capability while avoiding detection, often by exploiting low

transparency channels, third-party movement, and rapid conversion or cash-out mechanisms.

Common terrorist financing typology red flags include:

- Nested transaction patterns that route value to unrelated third parties
- Multiple prepaid cards purchased under false identities or loaded using illicit cash
- Numerous unrelated crypto deposits rapidly converted to stablecoins or fiat and withdrawn via a VASP
- Cash out activity via jurisdictions with weak anti-financial crime controls
- Repeated deposits in one jurisdiction followed by immediate ATM withdrawals in another jurisdiction

Charities & NGO Red Flags

Charities and non-governmental organisations can operate in complex environments, including conflict zones and high-risk jurisdictions, and may rely on cross-border transfers, intermediaries, and rapid distribution of funds. These features can create vulnerabilities to misuse, including the diversion of funds, the abuse of charitable status, or the concealment of the true beneficiaries. The presence of a charitable mission does not remove financial crime risk. It increases the importance of governance, transparency, and demonstrable control over how funds are collected, moved, and applied.

Common red flags for charities and non-governmental organisations include:

- Cross-border operations moving significant funds with limited transparency or weak documentation
- Elevated exposure to politically exposed persons or public officials in governance, beneficiaries, or counterparties
- Links to groups associated with terrorist financing or sanctioned activity, including through partners or local affiliates

- Exploitation of weak regulatory oversight in certain jurisdictions, including reliance on informal networks or poorly controlled intermediaries

Offshore Red Flags

Offshore financial centres can serve legitimate purposes, such as international structuring, investment holding, and cross-border commerce. However, they can also increase financial crime risk by enabling secrecy, obscuring beneficial ownership, or complicating the tracing of funds across entities and jurisdictions. The risk is not the use of an offshore centre in itself. The risk arises when the structure or behaviour reduces transparency, weakens accountability, or appears designed to frustrate due diligence and monitoring.

Common offshore financial centre red flags include:

- Complex ownership structures that make beneficial ownership difficult to verify
  Use of shell companies primarily for holding assets without a clear economic rationale
- Limited transparency, including reluctance or inability to provide ownership and control documentation
- Unusual transaction patterns, including sudden large flows of funds and round-tripping, where funds move out and back in without a credible purpose
- Rapid asset transfers between offshore entities, particularly without supporting documentation or a commercial rationale
- Use of cash-intensive businesses by a customer registered in an offshore financial centre creates inconsistency between the business model and the jurisdiction choice
- Transactions involving politically exposed persons, where opacity increases corruption and misuse risks

Special Purpose Vehicles Red Flags

Special-purpose vehicles are commonly used for legitimate purposes, such as ring-fencing assets, financing specific projects, securitisation, and structured transactions. However, special-purpose vehicles can also create a higher financial crime risk when they are designed or used in ways that reduce transparency and make it difficult to identify beneficial ownership, understand the economic rationale, or trace the origin and destination of funds. The risk increases where the special-purpose vehicle appears to exist primarily to obscure ownership or to layer funds through complex transaction flows.

Special-purpose vehicles may be misused to obscure the source of illicit funds by routing value through a series of transactions across multiple special-purpose vehicles and related entities. This can create a complex trail that makes tracing and accountability more difficult, particularly when ownership, governance, and counterparties are not clearly disclosed.

Common special purpose vehicles red flags include:

- Complex ownership structures involving multiple layers of companies
- Limited transparency around ownership, control, and governance
- Unclear or inconsistent purpose, including an economic rationale that cannot be adequately explained
- Transaction flows that appear circular, unnecessary, or inconsistent with the stated purpose of the special-purpose vehicle

Wire Transfers Red Flags

Wire transfers are a core mechanism for moving funds quickly across borders and between institutions. Because they provide speed, reach, and the ability to route value through multiple intermediaries, they can be misused to support financial crime. Common misuse includes concealing or moving proceeds of crime, facilitating fraud, breaching sanctions restrictions, and supporting terrorist

financing. The risk increases where there is limited transparency about the originator, beneficiary, purpose, or the route funds take.

Common wire transfer red flags include:

- Transfers involving high-risk jurisdictions
- Transfers involving sanctioned individuals or entities
- Unusual wire transfer activity, including unusual volume or amount, unusual timing, or complex transaction paths
- Unusual transfer instructions, such as sequences of instructions or inclusion of unrelated party names in the payment narrative
- Attempts to conceal information, including incomplete or inadequate beneficiary information

Mergers & Acquisitions Red Flags

Mergers and acquisitions involve the consolidation of companies, business lines, or assets through transactions that are often high-value, time-sensitive, and structurally complex. This complexity can create opportunities for money laundering and related financial crime by making it harder to trace the true source of funds, the ultimate beneficial owners, and the economic rationale for the transaction. Criminals may seek to acquire legitimate businesses to blend illicit proceeds into apparently lawful revenue streams, or to gain access to corporate accounts, payment rails, and trade activity that provide cover for further laundering.

Mergers and acquisitions activity can also increase exposure to broader misconduct risk. A target entity may have previously been involved in money laundering, sanctions breaches, fraud, corruption, or other serious compliance failures. If these risks are not identified through due diligence, an acquirer or adviser may inadvertently facilitate the movement of illicit funds or inherit significant regulatory and reputational liabilities.

Common Mergers and acquisitions red flags include:

- Complex deal structures or ownership arrangements that obscure ultimate beneficial ownership or control
- Use of shell companies, nominee arrangements, or layered holding structures without a clear economic rationale
- Cross border transactions involving multiple jurisdictions with uneven regulatory oversight or elevated financial crime risk
- Source of funds that cannot be clearly evidenced, is inconsistent with the buyer profile, or relies on opaque funding routes
- Time pressure to complete the transaction that limits due diligence, discourages questions, or restricts access to records
- Target entities with indicators of past compliance misconduct, including exposure to money laundering, sanctions evasion, fraud, or bribery and corruption laws

Money Services Businesses Red Flags

Money services businesses often provide high-volume, fast-moving payment and value transfer services, including remittances, currency exchange, and other transfer mechanisms. These services are attractive for legitimate use, but they can also be exploited to move illicit funds quickly, fragment transactions to avoid detection, and transfer value across borders into higher-risk corridors. In money services businesses, red flags commonly appear in customer behaviour and transaction patterns, as criminals may prioritise speed and anonymity over transparency.

Common money services businesses red flags include:

- Unusual customer behaviour, such as reluctance to provide accurate information, avoidance of reasonable questions, or submission of falsified data

- Unusual or suspicious transaction patterns, including large, round dollar amounts, rapid fund movements, or transaction sizes inconsistent with the customer profile
- Transactions involving high-risk jurisdictions, including frequent transfers to or from countries associated with weak AML controls or higher financial crime exposure
- Structuring or smurfing, where larger amounts are broken into smaller transactions to avoid thresholds, monitoring triggers, or reporting requirements

Cryptoassets Activity Red Flags

Cryptoassets activity can increase financial crime exposure because value can be moved quickly, across borders, and through services that vary significantly in the strength of their controls. While blockchain records transactions, risk can still arise when customers use cryptoassets to obscure the source of funds, bypass screening, rapidly cash out, or move value through jurisdictions with weak supervision. Cryptoasset red flags often involve wallet risk indicators, unusual velocity, and inconsistencies between activity and the customer's known profile.

Common cryptoassets red flags include:

- Transactions involving wallet addresses that are sanctioned or linked to illegal activity
- Large purchases made within a 24-hour period, followed by fiat withdrawals through multiple small transactions
- Repeated transfers to fiat currency exchanges in jurisdictions with weak regulatory enforcement
- A customer purchasing cryptoassets with funds that significantly exceed their known wealth or a credible source of funds

What To Do When You Detect A Red Flag

When a red flag is detected, the correct response is procedural and evidence-led. The objective is to determine whether the activity can be reasonably explained and evidenced, or whether it requires escalation and potential reporting.

Confirm the facts and establish context. Check what is known about the customer and the expected activity profile, then compare it to what has occurred. Verify basic details (amounts, timing, counterparties, products used, locations, account history) to ensure the concern is not driven by incomplete or incorrect information.

Conduct proportionate additional review. Where internal procedures allow, obtain clarification and supporting documentation that addresses the specific inconsistency. The focus should be on relevance: documentation should directly explain the behaviour (the purpose of the transaction, the relationship with counterparties, the source of funds, where relevant) rather than generating unnecessary information.

Document clearly and contemporaneously. Record what triggered concern, what checks were performed, what information was obtained, and how conclusions were reached. Documentation should be sufficient for a third party to understand the decision-making without relying on personal memory.

Apply escalation rules consistently. If the red flag cannot be reasonably resolved, if explanations are inconsistent, or if multiple indicators accumulate, escalate through the organisation’s defined route. This typically means escalation from the operational team to the compliance function and, where suspicion is formed or cannot be ruled out, to the Money Laundering Reporting Officer for decision-making and governance of the reporting pathway.

Maintain confidentiality and avoid tipping off. Reviews, escalations, and any reporting decisions must be handled discreetly and in line with internal policies. Communications with the customer should remain professional and neutral and must not reveal that the activity is under suspicion or that a report may be made.

This approach ensures red flags are treated neither as automatic proof nor as something to dismiss. They become a structured trigger for verification, evidence, escalation, and, where required, reporting.

Identifying Red Flags in AML/CTF

Case Study:

ABCD Relief Fund, a United Kingdom-registered charity, applies for a business account with a regulated payment institution through remote onboarding. The charity states that it will collect donations and make overseas payments for medical aid, and it is initially assessed as a medium-risk charity. During onboarding, a key individual's residential address cannot be independently verified, and the customer pushes for urgent approval while requesting that communication avoid email. The account is nevertheless approved with limited supporting evidence on overseas partners and operational controls. Within days, the charity receives a large incoming "grant" from an offshore company with minimal documentation explaining the origin and purpose of the funds. Shortly afterwards, it instructs a rapid outbound transfer to a United Arab Emirates trading company for "medical kits," supported only by a pro-forma invoice rather than robust procurement and delivery evidence. When compliance requests sought clarification, including information on end beneficiaries and stronger supporting documents, the customer refused to provide beneficiary details and continued to insist on urgency. The accumulation of transparency gaps, offshore

funding, rapid pass-through payments, and avoidance behaviour leads compliance to escalate the case for enhanced review.

- List the red flags you see.
- Does the risk stay medium or move higher? State the new rating and why.
- Write 4 specific questions you would ask to resolve the main gaps.
- What should compliance do now: proceed, pause for evidence, or escalate? Briefly justify.

The case presents multiple red flags that elevate the risk from medium to high: a key individual's address cannot be independently verified, the customer applies urgency and asks to avoid formal communication, and the onboarding file lacks robust evidence on overseas partners and operational controls. Shortly after approval, a large "grant" arrives from an offshore company with minimal supporting documentation, followed by a rapid outbound transfer to a United Arab Emirates trading firm supported only by a pro-forma invoice, which weakens assurance over the commercial rationale and end use of funds. The customer then refuses to provide end-beneficiary information or meaningful beneficiary controls, limiting transparency and traceability. The appropriate response is to pause further processing where policy permits and escalate for enhanced review, while seeking targeted clarification and evidence: the contractual relationship and any ownership links with the United Arab Emirates counterparty, the grant agreement and credible explanation of the offshore funder and source of funds, itemised procurement and delivery documentation for the "medical kits," and evidence of beneficiary controls such as distribution records, partner oversight, and an audit trail.

Key Takeaways

A red flag in Anti-Money Laundering and Combating the Financing of Terrorism is a warning sign that a customer's behaviour, transactions, or documentation does not align with what is known about them, their stated purpose, or their expected activity profile. Red flags are not conclusions; they are triggers for a consistent, evidence-led response, and risk increases when multiple indicators accumulate, explanations are inconsistent, or transparency is resisted. They tend to arise at predictable points in the lifecycle, especially during onboarding and identity checks, beneficial ownership review, source of funds or wealth assessment, early post-onboarding activity, and ongoing monitoring when patterns shift without a credible rationale. The correct approach is to verify facts and context, obtain targeted clarification and relevant evidence where permitted, document what was observed and how decisions were reached, escalate when concerns cannot be resolved, or suspicion cannot be ruled out, and maintain confidentiality throughout to avoid tipping off.