Certification Centre By Crence

T.M.M & PARTNERS ADVOCATES
LEGAL EXPERTISE, PERSONALIZED SERVICE

AML & ESG Executive Training 2025:

New Format Compliance Training Workshop on AML and ESG in Kenya

30 OCT — 01 NOV 2025

Empowering through practice

AGENDA

- From Paper to Practice: Designing a Risk-Based AML Framework that Stands Up to Audit
- Compliance in Action: Tools, Tactics & Expectations for Financial Institutions
- European experience in regulating VASPs
- Surprise Inspection: Can Your Team Pass a Mock Regulatory Review?
- Managing Emerging Risks: Crypto
- Navigating AML Expectations Across High-Risk Sectors: Real Estate, Law & More

AML Certification Centre
By Crence

Certification Centre
By Crence

From Paper to Practice: Designing a Risk-Based AML Framework that Stands Up to Audit

Andrei Sribny
CEO at AML
Certification Centre

Setting the Tone

The visible one

Effective AML system

The real one

Every effective AML system has two faces:

The visible one — policies, manuals, and procedures.

The real one — people, culture, and decision-making.

Certification Centre
By Crence

Why AML Frameworks Fail?

1. Copy-paste policies with no link to operations
2. Outdated risk assessments
3. Lack of governance ownership
4. No audit trail or measurable controls
5. Training without accountability

Certification Centre
By Crence

What ‘Risk-Based’ Really Means

Certification Centre
By Crence

RISK-BASED APPROACH

1

Governance & Oversight

2

Risk Assessment

3

Policies & Procedures

4

Monitoring & Improvement

Understanding the Risk-Based Approach

Certification Centre
By Crence

Tailored measures based on **customer risk**, evolving from “rule-based” to “complex” scenarios.

Avoid EDD for low-risk customers

Key principles

Proper measures depend on the risk profile and national assessments.

Practical example: Retail shop producing locally with electronic payments vs. retail shop importing from high-risk countries and using cash frequently.

Understanding the Risk-Based Approach

Certification Centre
By Crence

Key Considerations:

- Begin with analysing existing scenarios.
- Identify false positives, SAR investigations, and patterns.

Analyze → Refine → Integrate → Monitor

! **AI is not a panacea**; skilled AML experts are essential to train and guide AI.

Policy Development: From Template to Tailor-Made

Certification Centre
By Crence

The Difference:

An effective AML policy doesn't just describe compliance — it operationalises it.
It connects statements to people, controls, and timelines.

Policy design:

PHASE 1	Align policies with risk appetite
PHASE 2	Assign clear accountability
PHASE 3	Include measurable elements (training hours, reporting deadlines, KPIs)
PHASE 3	Keep policies auditable — trace every statement to a control

Keep in mind:

If you can't show how a policy works in practice, it doesn't exist.

Certification Centre
By Crence

Lives Only on Paper

Excerpt from a Template AML Policy

The Company shall implement appropriate measures to prevent money laundering and terrorist financing. All employees must comply with applicable AML laws and regulations. The Compliance Department shall oversee the monitoring of suspicious activity and report to the relevant authorities where nessary.

⚠ This language is compliant – but meaningless in practice

- No reference to risk levels
- No ownership or accountability
- No link to real controls or timelines

Copied, not connected.

When Compliance Lives in Practice

Excerpt from Our Tailored AML Policy

The Company applies a risk-based approach to all customers and products.

Customer risk is assessed at onboarding using a three-tier model (Low, Medium, High) managed by the Business Risk Team.

The MLRO reviews all High-Risk cases within 24 hours before account activation.

STRs must be filed within one business day of identification and recorded in the central STR Register.

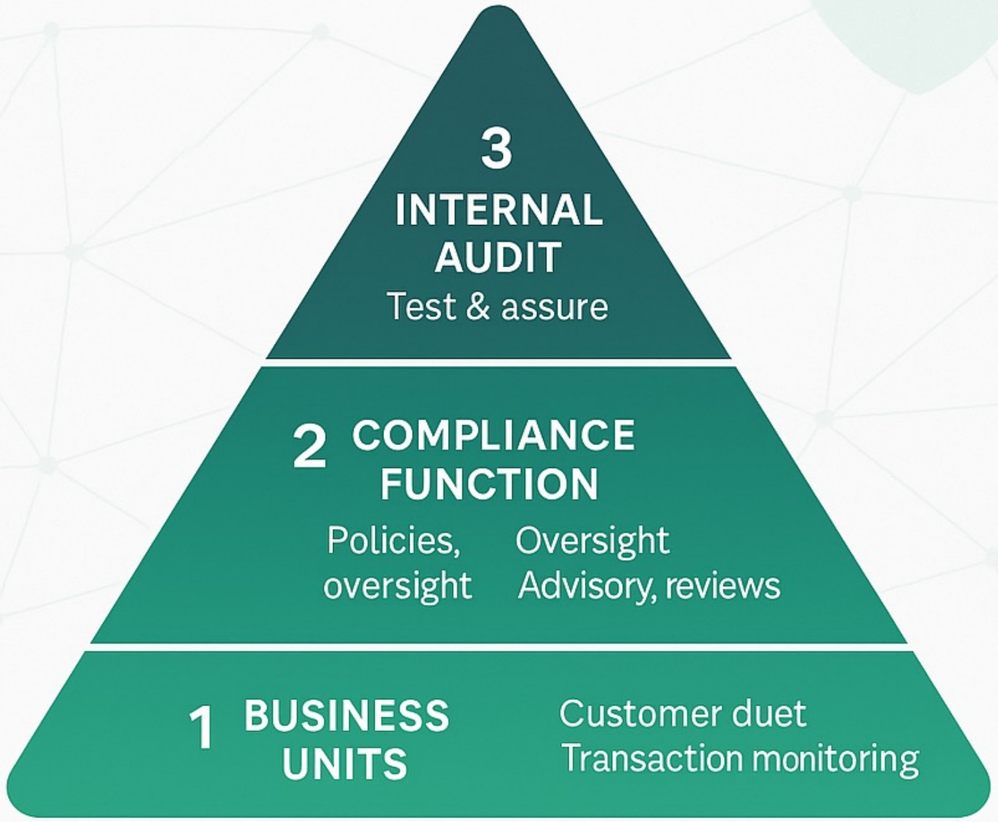
✓ This language is specific, measurable, and owned.

- Clear risk model and fiunctrame
- Named responsible functions
- Direct link to evidence and audit trail

Aligned, accountable, auditable.

Certification Centre
By Crence

THE ENGINE OF AML: THREE LINES OF DEFENCE



Every layer must understand not just *what to* do, but *why* they do it.

Certification Centre
By Crence

Core Controls Checklist

✓ CDD & ongoing monitoring	▶ Identify, verify, and update
✓ Screening (sanctions, PEPs)	▶ Before onboarding and continuously
✓ STR procedures	▶ Timely, complete, consistent
✓ Record-keeping & reporting	▶ Maintain documentation for at least 5 years
✓ Staff training	▶ Regular, role-specific, documented

Traceability: The Auditor's Lens

Certification Centre
By Crence

Audit Traceability Chain

- **Control:** The process or check you perform.
- **Evidence:** The proof it was done.
- **Report:** How you document and escalate results.
- **Review:** How management verifies effectiveness.
- **Action:** How findings are addressed and improved.

Key Updates

A control that isn't traceable is invisible to an auditor.

Once the controls and governance are in place, the next question is:

What happens when they're tested?

That's where audit findings come in — and we'll see what usually goes wrong, and how to fix it.

Applying Red Flags

Certification Centre
By Crence

Focus: Real-World Situations

- Red flags don’t appear in isolation.
- It’s not always about one big red flag.

Context: Where Red Flags May Appear

- During onboarding or when updating customer information
- When customers ask repeated questions about limits, thresholds, or how reports are filed
- Behaviour changes: becoming nervous, vague, or evasive
- Transactions that are unusually large, structured, or don’t match the profile

Approach: Think Critically

- Don’t just tick boxes — assess the full picture
- Ask yourself: “Does this make sense based on what I know about this customer?”
- If something feels off, it probably is — report it

Applying Red Flags

Certification Centre
By Crence

Case study:

Suspicious Business Client Behaviour

“A customer, listed as a small online retailer, suddenly starts sending large international payments to unrelated jurisdictions. When asked for supporting documentation, they provide vague answers and delay sending anything. They also avoid phone calls and only respond via email.”

What are the red flags?

- Change in transaction behaviour
- Lack of transparency
- Avoidance of contact

What should you do?

- Log your observations clearly
- Report to the Compliance Team immediately
- Let them assess whether to escalate further

Practical Tips for Spotting Red Flags During Interactions

Listen Actively

- **Pay close attention** to what the customer says — and how they say it.
- **Look for inconsistencies**, vague answers, or signs they're avoiding specific topics.
- **Don't rush** — give space for natural responses.

Observe Behaviour

Be aware of **non-verbal cues**:
- Nervousness, defensiveness, or unusual urgency
- Reluctance to provide standard information or documents

Trust your instincts — if something feels off, take note.

Questioning Techniques

- Use **open-ended questions** to gather more context:
- *"Can you tell me more about the purpose of this transaction?"*
- *"What's the source of these funds?"*
- Don't interrupt, they'll say more

Avoid leading or yes/no questions that limit understanding.

Documentation

- Record your observations accurately, clearly, and promptly.
- **Stick to facts** — avoid assumptions or personal interpretations.
- Good documentation is crucial for the Compliance Team's investigation.

Practical Approach to CDD

Certification Centre
By Crence

The Idea of Customer Due Diligence:

Firms must identify and verify the identities of their customers—and, where applicable, their beneficial owners—while understanding the nature and purpose of the business relationship to assess risk and enable effective ongoing monitoring.

CDD Structured:

PHASE 1	Verify identity and documentation
PHASE 2	Assess the risk level based on customer profile
PHASE 3	Monitor ongoing activities to detect changes
PHASE 3	Document findings and actions taken

Keep in mind:

The role of the first line of defence is essential in protecting the institution.

Challenges in CDD and How to Overcome Them

Certification Centre
By Crence

Problem

Customer Resistance

Customers may question the need for certain documents or feel the process is too intrusive.

Solution

Clearly explain regulatory requirements and the bank's responsibility to comply with AML laws.

Use calm, professional language and emphasise the protection of both the institution and the customer.

Data Verification Issues

Incentivise and equip employees to handle risks independently.

Use trusted and independent sources such as government registries and sanction lists.

Where needed, employ reputable third-party verification tools or service providers.

Checklist for steps.

Case Example

A customer submits a utility bill with mismatched names or unclear origin.

Response:

Politely request a valid replacement document and explain the need for consistency.

If suspicion remains, escalate the case to Compliance as per internal procedures.

Document the issue and the customer's response thoroughly.

Certification Centre
By Crence

Question

Have you experienced any challenges in CDD?

How much information is sufficient?

Certification Centre
By Crence

The Standard: Enough to Understand Risk

The level of information collected should be proportionate to the risk posed by the customer. Higher-risk customers require more detailed information and enhanced due diligence (EDD).

What Does "Sufficient" Mean in Practice?

You should be able to answer:

- Who is the customer?
- What is the source of their funds or wealth?
- Why are they using our services?
- Is there anything unusual or unclear about the relationship?

Low vs. High-Risk Profiles	
Low-risk and normal risk: **CDD or SDD** Basic ID, address, nature of business/activity.	**High-risk:** **EDD** Detailed ownership structure, source of funds/wealth, ongoing monitoring and deeper checks (e.g. PEPs, sanctions).

There's no one-size-fits-all checklist. Apply **judgement**, guided by your internal AML policies and regulatory expectations.

Certification Centre
By Crence

If you're unsure whether the information is sufficient—ask yourself:

"Would I be confident explaining this customer profile to a regulator?"

Team Responsibilities in AML Compliance

Certification Centre
By Crence

1

Frontline Staff or the **First Line of Defence**. Acts as the **first point of contact** with customers.

Responsibilities include:
- Observing customer behaviour and identifying anything unusual.
- Asking appropriate questions when something doesn't feel right.
- **Reporting suspicions promptly** to the Compliance Team — not investigating independently.

2

Compliance Team – Investigate and Escalate. Serves as the **Second Line of Defence.**

Responsibilities include:
- Reviewing reports submitted by staff.
- Conducting internal investigations and risk assessments.
- Escalating cases to the FIU or relevant authorities when needed.
- Providing guidance and training to frontline teams.

3

Management & Internal Audit (**Third Line of Defence**) – Oversee and Enforce. Ensures the AML framework is fully implemented.

Responsibilities include:
- Creating a strong compliance culture across the organisation.
- Ensuring policies, procedures, and escalation channels are in place.
- Holding teams accountable and providing sufficient resources and training.

Cross-Department Collaboration

Certification Centre
By Crence

Why Coordination Matters

- As a customer-facing team, you are often the first to spot unusual behaviour.
- Timely and accurate reporting allows the Compliance Team to act quickly and appropriately.
- Poor coordination can delay action — and that can lead to regulatory breaches or missed suspicious activity.

Best Practices to Follow

- Know your internal contacts: Be clear on who to report to and how (email, system, form, etc.).
- Report early — don’t wait for confirmation or proof.
- Ask the Compliance Team when in doubt — collaboration avoids mistakes.
- If something doesn’t feel right, flag it and let Compliance decide next steps.

> *Your role is not to investigate — it’s to **observe**, **document**, and **report**. Compliance takes it from there.*

Certification Centre
By Crence

NO TIPPING OFF!!!

Reporting Protocols

Certification Centre
By Crence

- **Accuracy:** Capture details without making assumptions
- **Completeness:** Include all relevant information and context
- **Timeliness:** Report promptly to avoid compliance gaps

If you spot **unusual customer behaviour**, unclear documents, or anything that doesn't "feel right" — **report it immediately**.

Examples include:

- Reluctance to provide information
- Transactions that don't match the customer's profile
- Signs of structuring or evading questions

Escalation Process

- Your report goes to the Compliance Team for review and potential investigation.
- If necessary, Compliance will escalate further to management or the Financial Intelligence Unit (FIU).
- You may be contacted for clarification — cooperate fully but maintain discretion.

How to Report?

Follow your internal procedure:

- Use the designated reporting form/system
- Include all relevant facts: what you saw, heard, or noticed
- Be objective — avoid assumptions or personal opinions
- Always maintain confidentiality — do not discuss the case with others.

Key Takeaways

1. Governance defines ownership; controls define execution.
2. Documentation and communication across the three lines prevent failure.
3. Traceability — not volume — is what makes an AML system auditable.
4. A risk-based AML framework is only as strong as its weakest documented control.

Certification Centre

Certification Centre
By Crence

> **Don’t wait for confirmation or proof — suspicion is enough to report.**

Certification Centre
By Crence

Compliance in Action: Tools, Tactics & Expectations for Financial Institutions

Viktor Tkatsenko
Key Expert;
Head of AML,
Citadele Bank

Chapter 1: The Compliance Imperative in Financial Services

Certification Centre
By Crence

Why Compliance Matters Now More Than Ever

Evolving Landscape

Financial institutions navigate constantly shifting regulations, sophisticated cyber threats, and intensified stakeholder scrutiny in an interconnected global economy.

High-Stakes Consequences

Non-compliance risks extend far beyond fines—legal penalties, irreparable reputational damage, customer loss, and devastating financial impacts threaten institutional survival.

AML Certification Centre By Crence

Regulatory vs. General Compliance: What's the Difference?

Regulatory Compliance

Mandatory laws and requirements enforced by government agencies with legal authority. Non-negotiable standards that carry penalties for violations.

- MiFID II securities regulations
- CRD V/CRR II banking directives
- Solvency II insurance requirements
- PSD2 payment services directive
- GDPR data protection regulation
- 6AMLD anti-money laundering directive

General Compliance

Internal policies and procedures that promote organizational ethics, operational efficiency, and comprehensive risk management beyond legal minimums.

- Code of conduct
- Internal controls
- Best practice standards
- Corporate governance

The EU Regulatory Landscape: Key Agencies & Their Roles

EBA

European Banking Authority - Ensures effective and consistent prudential regulation and supervision across the EU banking sector.

ESMA

European Securities and Markets Authority - Safeguards stability of the EU's financial system by enhancing investor protection and promoting stable and orderly financial markets.

EIOPA

European Insurance and Occupational Pensions Authority - Contributes to the stability of the financial system, transparency of markets, and protection of insurance policyholders and pension scheme members.

ECB

European Central Bank - Conducts monetary policy and supervises significant banks in the eurozone to ensure financial stability.

The Anti-Money Laundering Authority (AMLA)

The Anti-Money Laundering Authority (AMLA) is a new EU body established to centralize anti-money laundering supervision across the European Union. It will be responsible for directly overseeing high-risk cross-border financial institutions and coordinating AML efforts among member states to enhance the fight against illicit financial flows.

Direct Supervision

Oversight of high-risk cross-border financial institutions.

Coordination Hub

Harmonizing AML practices across EU member states.

Regulatory Standards

Developing consistent AML rules and guidelines.

01

Banking Supervision

Prudential oversight and systemic risk monitoring

02

Market Regulation

Securities markets and investor protection

03

Insurance Oversight

Policyholder protection and pension security

04

Monetary Policy

Price stability and financial system oversight

Chapter 2: Core Compliance Responsibilities for Financial Institutions

Certification Centre
By Crence

Compliance Officer's Mandate

Implementation & Monitoring

Develop, implement, and continuously monitor adherence to EU directives, national regulations, and internal policies across all organizational functions.

Risk Assessment & Training

Conduct comprehensive risk assessments, design targeted compliance training programs, and ensure staff understand their regulatory obligations.

Regulatory Liaison

Maintain relationships with regulatory bodies, coordinate audit responses, and manage examination processes with transparency and professionalism.

Certification Centre
By Crence

Risk Management & Controls

Risk Identification

Systematically identify operational, financial, and cyber risks across all business units and processes.

Control Establishment

Design and implement robust controls to mitigate identified risks and prevent fraud before it occurs.

Continuous Monitoring

Deploy real-time monitoring systems and establish comprehensive reporting mechanisms for proactive risk management.

Certification Centre
By Crence

Customer Due Diligence & AML Compliance

Essential AML Protocols

1 Know Your Customer (KYC)

Enforce rigorous identity verification and ongoing customer due diligence to prevent money laundering and terrorist financing.

2 Transaction Monitoring

Detect and report suspicious transactions under 6AMLD and EU AML regulations with comprehensive documentation and analysis.

3 Technology Automation

Leverage advanced technology platforms to automate monitoring, generate alerts, and streamline reporting for regulatory compliance.

Certification Centre
By Crence

Data Privacy & Cybersecurity Compliance

Regulatory Alignment

Ensure full compliance with GDPR, NIS2 Directive, DORA, and sector-specific data protection regulations governing financial information.

Data Protection

Implement encryption, access controls, and secure data handling procedures to protect sensitive financial and personally identifiable information.

Incident Response

Maintain comprehensive incident response plans and breach notification protocols to ensure rapid, compliant action during security events.

Chapter 3: Practical Audit Tools for Compliance Success

Certification Centre
By Crence

What Is a Compliance Audit?

Certification Centre
By Crence

> A compliance audit is an independent, systematic review that verifies an organization's adherence to regulatory requirements, internal policies, and industry standards.

Financial Reporting

Accuracy and transparency in financial statements and disclosures

Cybersecurity

Information security controls and data protection measures

AML Programs

Anti-money laundering procedures and suspicious activity monitoring

Operational Controls

Internal processes and risk management frameworks

Leading Compliance & Risk Management Platforms

Centralized Workflows

Consolidates audit workflows, risk assessments, and compliance activities into a unified platform for seamless collaboration.

AI-Driven Automation

Leverages intelligent automation to significantly reduce manual tasks, allowing compliance teams to focus on strategic analysis.

Robust & Reliable Solutions

Provides enterprise-grade compliance and risk management capabilities, earning widespread adoption across diverse industries.

Certification Centre
By Crence

Customizable Compliance Automation Platforms

Certification Centre
By Crence

Flexibility Meets Power

These low-code platforms enable organizations to build customized compliance workflows without extensive IT resources.

- **Custom Workflows**

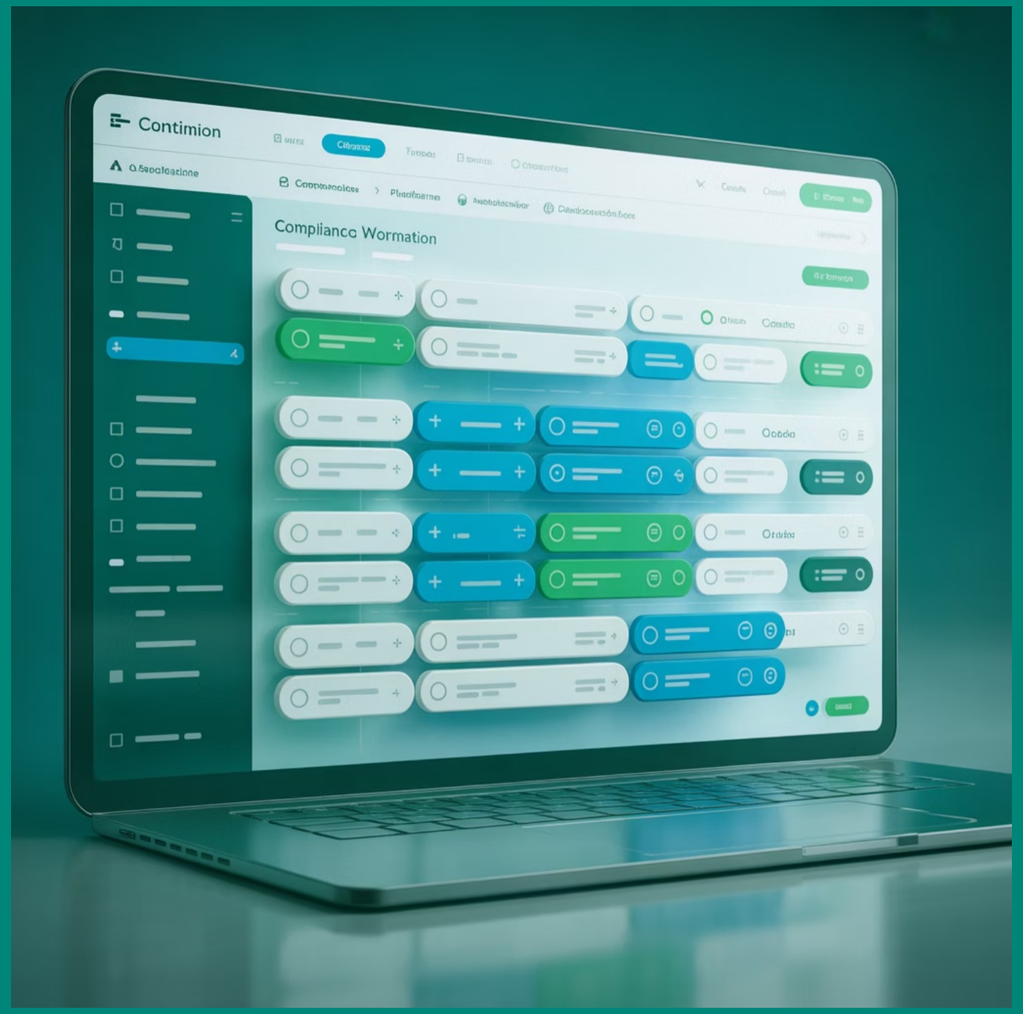
  Design tailored compliance processes matching your institution's unique regulatory requirements and organizational structure.

- **Third-Party Risk**

  Integrated vendor risk monitoring ensures supply chain compliance and identifies potential vulnerabilities.

- **Complex Environments**

  Ideal for institutions navigating multiple regulatory jurisdictions and intricate compliance frameworks.



Real-Time Compliance Tracking Systems

Automated Evidence Collection

These systems continuously gather compliance evidence from integrated platforms, significantly reducing manual documentation efforts.

Security Tool Integration

They seamlessly connect with various security tools, such as SIEMs and vulnerability scanners, to provide comprehensive visibility.

Live Status Dashboards

Offering real-time visualization of compliance posture, these systems enable proactive risk management and ensure continuous audit readiness.

Certification Centre
By Crence

Certification Centre
By Crence

Continuous Monitoring for Security Compliance Platforms

AI-Enhanced Compliance Framework Automation

Leverage advanced AI and machine learning to streamline SOC 2, ISO 27001, HIPAA, and other critical security audit preparations with continuous automated monitoring and intelligent evidence collection.

AI-Driven Alerts & Predictive Reporting

Receive instant notifications of compliance drift with AI-driven insights and generate comprehensive, predictive reports for auditors, significantly reducing preparation time.

85%

Time Reduction

Average decrease in audit preparation hours

24/7

Monitoring

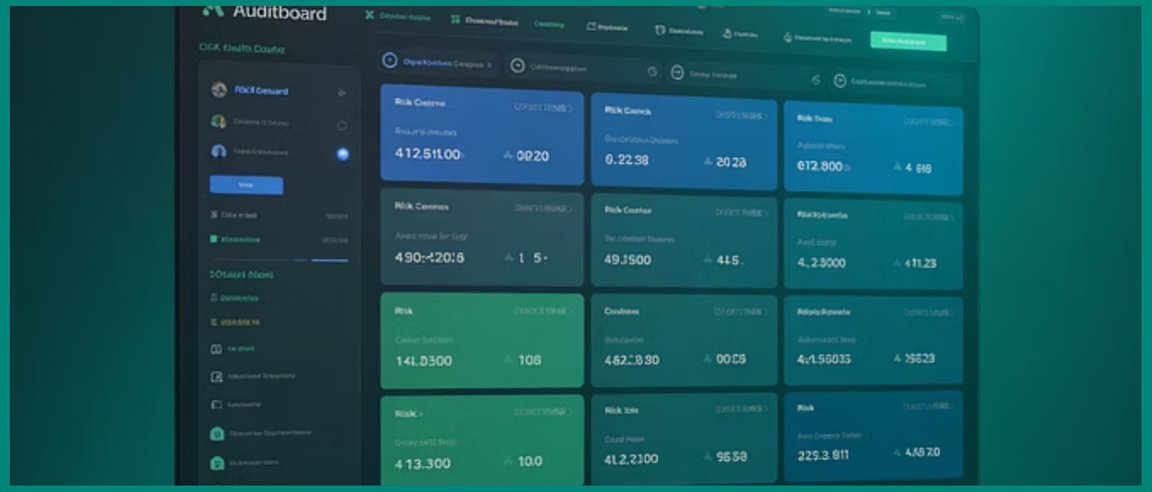
Continuous compliance surveillance

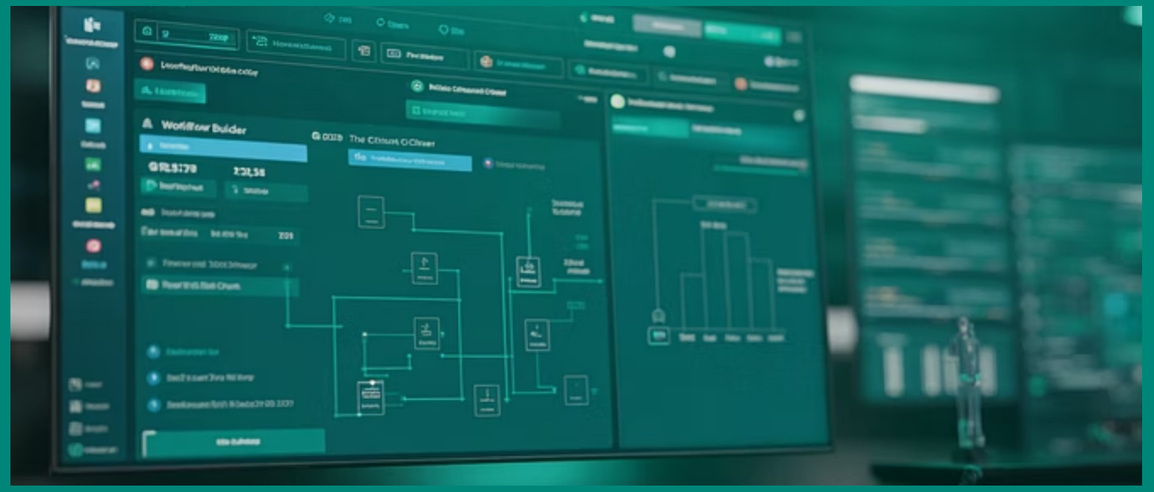
50+

Integrations

Connected security and IT tools

Certification Centre
By Crence





Modern compliance software platforms leverage intuitive dashboards, robust automation, and real-time monitoring to transform how organizations manage their regulatory obligations and ensure continuous adherence.

AI-Driven Compliance Monitoring: Next-Gen Features

Certification Centre
By Crence

Predictive Risk Insights

AI models analyze vast datasets to anticipate potential compliance breaches before they occur, enabling proactive mitigation.

Intelligent Anomaly Detection

Machine learning identifies subtle patterns and unusual activities, flagging deviations from normal behavior for immediate investigation.

Automated Reporting

Generate comprehensive, audit-ready compliance reports and documentation instantly, reducing manual effort and ensuring accuracy.

Continuous Monitoring & Alerts

Benefit from 24/7 real-time surveillance and instant alerts for any detected non-compliance or critical events.

Regulatory Text Analysis

NLP deciphers complex regulatory documents, extracting key requirements and ensuring policies are aligned with the latest mandates.

Smart Workflow Automation

Automate routine compliance tasks and integrate approval processes, enhancing efficiency and reducing human error.

Advanced Data Visualization

Transform complex compliance data into clear, actionable insights through intuitive dashboards and interactive visualizations.

Seamless System Integration

Integrate easily with existing GRC tools, ERP systems, and security platforms for a unified compliance ecosystem.

Certification Centre
By Crence

Chapter 4: Audit Tactics & Best Practices

Risk-Based Audit Planning

Certification Centre
By Crence

Strategic Prioritization

01

Identify High-Risk Areas

Focus audit resources on anti-money laundering, cybersecurity, and financial reporting—areas with greatest regulatory scrutiny and potential impact.

02

Data Analytics Integration

Leverage advanced analytics to identify anomalies, unusual patterns, and emerging trends that may indicate compliance gaps or control weaknesses.

03

Dynamic Risk Assessment

Continuously update risk profiles based on regulatory changes, internal incidents, and evolving business operations.

Certification Centre
By Crence

Evidence Collection & Documentation

1

Automated Audit Trails

Deploy tools that automatically capture and timestamp compliance activities, creating defensible documentation for regulatory examinations.

2

Standardized Checklists

Implement consistent forms and procedures across all audit activities to ensure nothing is overlooked and quality remains uniform.

3

Centralized Repository

Maintain a secure, searchable evidence database that enables rapid retrieval during audits and regulatory inquiries.

Best Practice: Establish a document retention policy aligned with regulatory requirements, typically 5-7 years for financial records.

Stakeholder Engagement & Communication

Board of Directors

Quarterly compliance updates and risk assessments

Business Units

Ongoing collaboration and control testing

Senior Management

Monthly status reports and issue escalation

Regulators

Transparent reporting and examination cooperation

External Auditors

Evidence provision and findings discussion

Effective communication ensures alignment, builds trust, and enables proactive problem-solving across all organizational levels.

AML Certification Centre By Crence

Continuous Improvement & Training

Findings Analysis

Transform audit discoveries into actionable insights, strengthening controls and closing compliance gaps systematically.

Regulatory Updates

Maintain current awareness of rule changes, enforcement trends, and industry best practices through continuous education.

Culture Building

Foster an organizational commitment to compliance excellence where every employee understands their role in risk management.

Certification Centre
By Crence

Chapter 5: Real-World Compliance Challenges & Solutions

Case Study: AML Compliance Failure & Recovery

Certification Centre
By Crence

2019: Critical Failure

Major bank fined $100M for inadequate KYC controls after missing suspicious transactions involving high-risk customers.

2020: Remediation

Implemented automated transaction monitoring system, overhauled KYC procedures, and conducted comprehensive staff retraining.

2021-2023: Success

Zero major violations in subsequent regulatory examinations, demonstrating effectiveness of enhanced controls and commitment to compliance.

1 2 3

Key Lesson: Investment in technology and training pays dividends—the bank's improved systems prevented estimated $500M in potential future penalties.

Navigating Regulatory Convergence: Data Privacy Meets Finance

The Challenge

Financial institutions face unprecedented complexity as GDPR, CCPA, and financial regulations create overlapping requirements for data handling, customer rights, and breach notification.

The Solution

Integrated Frameworks

Develop unified compliance programs addressing both privacy and financial regulations simultaneously.

Cross-Functional Teams

Establish working groups combining legal, compliance, IT, and business stakeholders.

Technology Solutions

Deploy platforms managing multiple regulatory requirements through single interfaces.

Certification Centre
By Crence

Certification Centre
By Crence

The Role of Big Four Auditors in Compliance Assurance

Deloitte

Global leader in regulatory advisory, risk management, and financial services compliance with specialized fintech expertise.

PwC

Provides comprehensive audit and assurance services with deep regulatory knowledge across banking, securities, and insurance sectors.

EY

Offers integrated compliance solutions combining audit excellence with technology-enabled risk assessment and monitoring.

KPMG

Delivers regulatory interpretation, control design, and compliance transformation services for complex financial institutions.

Compliance Audit Lifecycle

Certification Centre
By Crence

Planning

Define scope, identify risks, allocate resources

Fieldwork

Test controls, gather evidence, conduct interviews

Analysis

Evaluate findings, assess severity, identify root causes

Reporting

Document results, provide recommendations, communicate to stakeholders

Remediation

Implement corrective actions, monitor progress, validate effectiveness

Follow-Up

Verify resolution, close findings, update risk assessments

The Future of Compliance Auditing in Financial Services

AI & Machine Learning

Predictive risk analytics identifying potential compliance issues before they materialize, enabling proactive intervention and resource optimization.

Digital Operational Resilience

EU's DORA and similar frameworks emphasizing technology risk management, third-party oversight, and incident response capabilities.

Regulatory Collaboration

Enhanced partnerships between institutions and regulators through RegTech, fostering transparency and reducing examination burdens.

Building a Culture of Compliance Excellence

> "Compliance is not a destination but a continuous journey requiring vigilance, adaptability, and unwavering commitment to integrity."

Continuous Journey

Recognize that compliance evolves with regulations, technology, and business models—embrace ongoing learning and adaptation.

Modern Tools & Tactics

Leverage cutting-edge platforms, automation, and analytics to stay ahead of regulatory expectations and operational risks.

Empowered Teams

Foster a culture where integrity, customer protection, and trust are core values embraced by every employee, from front line to boardroom.

Learning by Regulating: The EU’s Crypto Journey

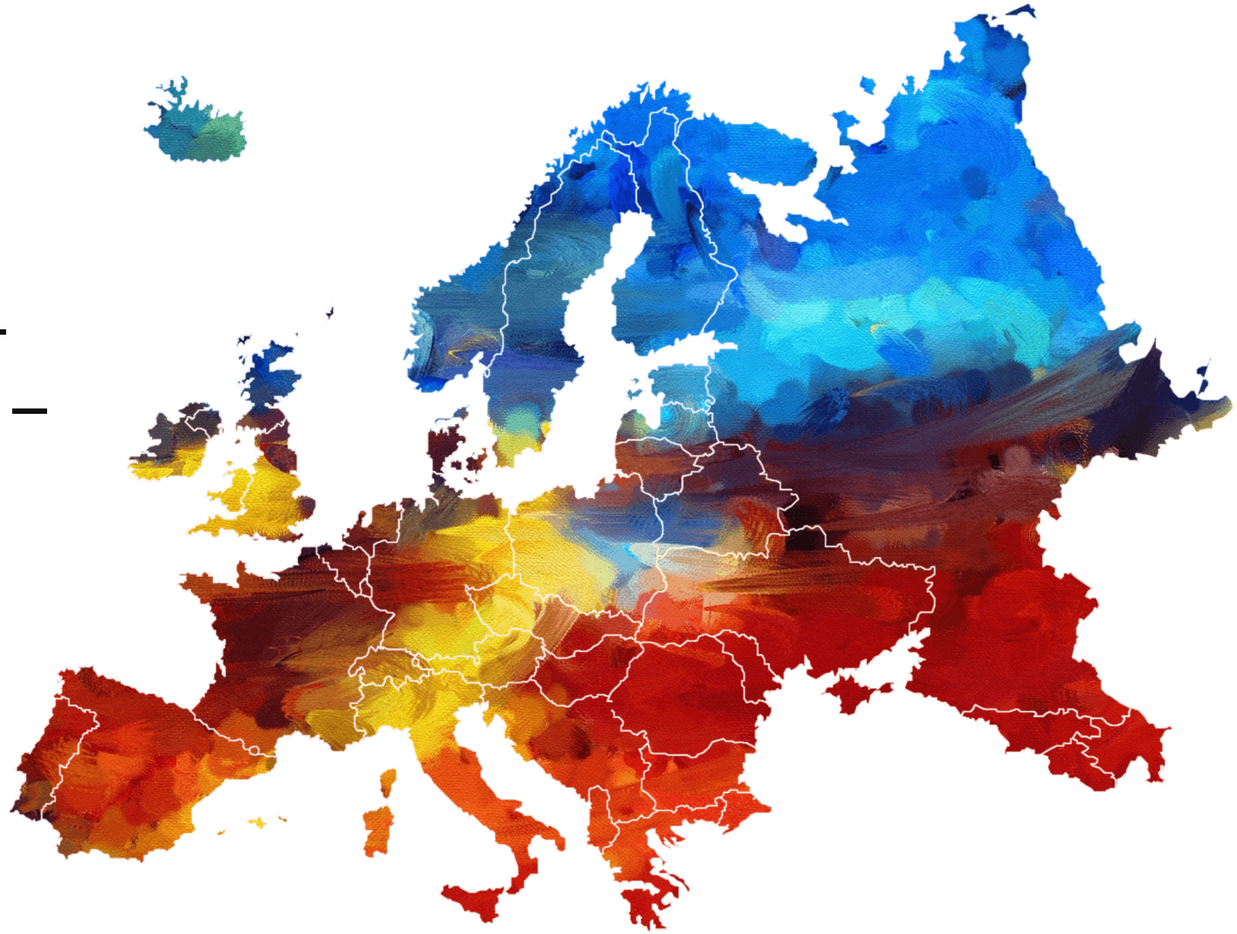
Gofaizen & Sherle

Mihhail Sherle

October, 2025

Intro

The key objective is to translate Europe's lessons on VASP regulation – from fragmentation to harmonisation – into actionable insights for Kenya.



Why this matters:

- *Crypto innovation meets AML challenge*
- *Smart regulation can turn risk into resilience.*

Gofaizen & Sherle

EU VASP Framework

Gofaizen & Sherle

Before MiCA

- **Before MiCA:** fragmented national regimes (Germany, France, Estonia, etc.)
- **Based on AML Directives:** registration with FIUs, CDD/KYC, STR reporting
- **No unified licensing:** each country defined “VASPs” differently
- **Limited cross-border recognition:** no EU passporting for services
- **MiCA introduces:** single authorization, harmonized supervision, and consistent AML alignment

Gofaizen & Sherle

Issues with AMLD and National Supervisors

⚖️ Different Qualification

Germany classified virtual currencies as **financial instruments**.

Other countries treated them as **separate asset classes**, not under MiFID.

Some had **no definition or regulation at all**.

🪪 Different Licensing Regimes

Licensing approaches varied widely: from **simple registration or notification** regimes to **full financial-institution licences**.

No consistency across EU jurisdictions.

⚙️ Technological Limitations

AMLD framework could **not adapt to emerging technologies** such as **smart contracts**, **DAOs**, **DEXs**, or **DeFi protocols**.

Result: innovation moved faster than regulation.

Gofaizen & Sherle

MiCA: Unified EU Framework

📘 Clear Definitions

• Crypto assets and its types: EMT, ART, Utility tokens
• Excludes FIs & most NFTs

🏦 CASPs as Financial Institutions

• Subject to DORA, AML & prudential rules
• Risk & governance obligations

🪪 Licensing & Passporting

• Single EU licence
• Standardised reporting

🔗 Integration & Oversight

• ESMA & EBA supervision
• Part of EU financial system

Gofaizen & Sherle

Supervision Under MiCA

ESMA: oversees significant CASPs, market integrity, cross-border activities
EBA: supervises stablecoin issuers (ARTs, EMTs), prudential rules
Jointly develop technical standards and coordinate NCAs

Authorise CASPs under MiCAR
Conduct ongoing supervision
Report to **ESMA** & **EBA**

National Competent Authorities (NCAs)

Comply with MiCAR, AML, DORA requirements
Provide reporting to **NCAs**
Subject to **ESMA/EBA** oversight for significant entities

CASPs, Issuers & Financial Institutions

Gofaizen & Sherle

Transfer of Funds Regulation (TFR)

💳 Obligation to Include Sender & Recipient Data

CASPs must attach data of both **originator** and **beneficiary** to every crypto transfer.

Data fields: name, account number (or wallet address), originator's CASP, and – when applicable – beneficiary's CASP.

🔍 Applies to All Crypto Transfers

Applies to **all** transfers involving at least one EU CASP – including **wallet-to-wallet** and **cross-border** transactions.

Minimum thresholds removed: *even small transfers must include full information.*

🔗 Supervision & Compliance

CASPs must **detect, block, and report** missing or suspicious data.

NCAs and FIUs use TFR data for **AML monitoring** and **sanctions enforcement.**

Gofaizen & Sherle

TFR: Key Challenges in Implementation

⚠️ Fragmented Infrastructure

- Lack of a **unified infrastructure** to transfer originator & beneficiary data between CASPs.
- No single standard or messaging protocol across providers.

🏦 Lessons from Traditional Payments

- In traditional finance, **SWIFT** enables standardized message exchange (MT messages).
- Crypto industry still lacks equivalent interoperability layer.

🌍 EU Response

- **EBA** coordinating with CASPs to develop **technical standards** for data transmission.
- Aim: full compatibility across EU and alignment with FATF standards.

Unlike SWIFT, crypto still lacks a universal “data rail” — TFR is the first step to build it.

Gofaizen & Sherle

EBA Guidelines: Wallet Verification

Unattended verification

via remote onboarding solutions displaying the address

Attended verification

customer performs verification step under CASP's supervision

Micro-transfer check

CASP sends or receives a minimal transaction from the wallet

Digital signature

client signs a predefined message with the private key

Gofaizen & Sherle

TFR: Unresolved Issues & Conflicts

⚙️ Verification Gaps

• Current EBA “options” for wallet verification (micro-transfers, signatures, etc.) **do not fully guarantee identity validation**.
• No standardized method across CASPs – risk of inconsistent KYC outcomes.

🌍 Cross-Border Data Transfers

• Transfers of crypto data to or from **non-EU jurisdictions** face legal uncertainty.
• Not all countries have **equivalent data protection standards**.

🧩 Regulatory Conflict (GDPR vs TFR)

• **TFR requires sharing transaction data**, while **GDPR restricts personal data flow**.
• Ongoing tension between **AML transparency** and **data privacy rights**.

Gofaizen & Sherle

EU AML Package: Unified Framework for Crypto Oversight

🧩 What's Included

AML Regulation – directly applicable, replaces national rules.
AMLD6 – harmonized directive for preventive measures.
AMLA – new central EU Anti-Money Laundering Authority.

🌍 Who It Applies To

Banks, fintechs, CASPs, and all obliged entities under AMLD.

Expands scope to **crypto service providers and platforms.**

⚖️ Why It Matters

Ensures **EU-level enforcement and consistency.**

Builds **risk-based supervision** and **cross-border data exchange.**

Gofaizen & Sherle

Same risk, same rule

- Ensures a **level playing field** across financial and crypto sectors
- **Equal regulation** for entities offering **similar services or risks**, regardless of technology
- Prevents **regulatory arbitrage** between traditional finance and crypto markets
- Promotes **consumer protection, market integrity, and financial stability**

Gofaizen & Sherle

Addressing Risks in Practice

Gofaizen & Sherle

Licensing & Oversight (MiCA + AML)

Licensing & Registration

Single **EU authorisation** for CASPs (passporting)

Fit & proper, capital & governance requirements

Documented **risk assessment** and policies

Ongoing Supervision

Periodic **reporting** (risk, volumes, incidents)

On-/off-site inspections, thematic reviews

AML controls incl. Travel Rule compliance

Coordination & Data-Sharing

NCAs: license & monitor locally

ESMA: significant CASPs;

EBA: EMT/ART issuers

FIUs: STR/SAR exchange & joint actions

Gofaizen & Sherle

Transparency & Traceability

Travel Rule Compliance

Mandatory transfer of **originator and beneficiary data** for crypto transactions

Applies to **CASPs, banks, and intermediaries**

Strengthens visibility of cross-border crypto flows

Blockchain Analytics

FIUs, Europol, and EBA use analytics to trace illicit activity

Tools such as **Chainalysis** and **TRM Labs** support investigations

Enables detection of **mixers, DeFi laundering, and ransomware flows**

Public–Private Cooperation

Exchanges, analytics firms, and law enforcement share data

Enhances **traceability** without undermining innovation

Supports the EU goal of "**no safe haven for illicit funds**"

Gofaizen & Sherle

Enforcement in Practice: Finding the Balance

⚖️ Sanctions & Licence Withdrawals

Estonia revoked over **200+ VASP licenses (2022–2023)** after stricter AML audits.

Lithuania tightened VASP licensing, suspending non-compliant operators.

BaFin (Germany) withdrew registrations for firms failing AMLD checks.

💶 Administrative Fines

Fines issued for **AML reporting gaps** and **inadequate due diligence** (e.g., in Spain & Italy).

New AMLA authority expected to centralize enforcement by **2026–2027**.

🌍 Cross-Border Cases

Europol's "Follow the Money" operations: coordinated investigations into crypto laundering via mixers and OTC brokers.

Joint actions between **FIUs**, **Europol**, and **national prosecutors** improving tracing.

Lessons from EU VASP Regulation

Gofaizen & Sherle

Proportional Enforcement

- Balance between **innovation and control** is essential.

- National audits, licence withdrawals, and fines work — but must be **coordinated EU-wide**.

Bridging Gaps

- **Privacy vs. Transparency** remains unresolved (GDPR vs. Travel Rule).
- Supervisory **capacity and crypto expertise** still uneven across Member States.
- Technology evolves faster than compliance tools.

Building Competence

- Regulation evolves — **skills must evolve too**.

- Future regulators: **data-driven, crypto-literate, adaptive**.

- Collaboration between **public and private sectors** is key to resilience.

MiCA vs Kenya VASP Bill

Gofaizen & Sherle

Criterion	EU – MiCA	Kenya – VASP Bill (2024)
Regulatory Maturity	Fully enacted, with harmonised EU standards and active supervision.	Newly introduced; operational details and supervisory tools still evolving.
Institutional Framework	Multi-layered: EU (ESMA/EBA) + national regulators coordinate.	Dual oversight by CMA and CBK; coordination mechanisms emerging.
Licensing Depth	Strong focus on internal governance, white papers, prudential requirements.	Focus on registration, capital adequacy, and disclosure - lighter on governance.
Enforcement Tools	Established penalties, licence withdrawal powers, EU-level cooperation (Europol, FIUs)	Enforcement powers defined but not yet tested; relies on national agencies.
RegTech & Data Use	Advanced blockchain analytics, supervisory data sharing.	RegTech adoption in early stages; capacity-building under way.
Privacy & Data Balance	MiCA interfaces with GDPR → mature handling of privacy vs transparency.	Data protection provisions limited; future alignment needed.

Key Similarities

- **Licensing & AML:** Both require registration, risk assessment, and compliance with FATF Rec. 15.
- **Consumer Protection:** Both aim to safeguard client assets and promote market integrity.
- **Public–Private Collaboration:** Both frameworks rely on cooperation with industry and analytics providers.

Kenya is structurally aligned with MiCA, but still developing institutional capacity, RegTech integration, and enforcement experience.

Gofaizen & Sherle

Q&A Session

About Gofaizen & Sherle

Scan

Thank you!

Deep dive into MiCA Regulation

MiCAR

Gofaizen & Sherle

Certification Centre
By Crence

Group Exercise:

Surprise Inspection

Certification Centre
By Crence

Phase 1 Notice

Your organisation has just received an unannounced inspection from the Financial Reporting Centre.

- **You don’t need real documents.**
- **Use your Document Cards to explain what each record contains.**
- **Decide who will speak to inspectors.**
- **Think about where your weaknesses might be.**

Certification Centre
By Crence

Phase 1
Notice

1. Read your institution profile.
2. Assign roles (Compliance Lead, Legal, Documentation, Analyst, Operations & Training Officer).
3. Discuss the five requested documents.
4. Identify key risks and weaknesses.
5. Prepare your inspection strategy.

Certification Centre
By Crence

Phase 2
Inspection

Explain. Justify. Evidence.

Certification Centre
By Crence

Key Inspection Areas

Quick tips:

- **Be direct and factual.**
- **Reference policy, control, or evidence.**
- **If unsure, explain process (“I’d verify through…”).**
- **Don’t improvise. Stay within your documented framework.**

Governance & Oversight	Risk & CDD	STR & Training
Accountability	Enterprise-wide risk assessment	STR process & timelines
Board oversight	High-risk customers	Staff awareness
Reporting lines	Monitoring systems	Documentation quality

Certification Centre
By Crence

Phase 3 Findings

Prepare a Management Response

1. Acknowledge each finding.
2. Explain the root cause.
3. Propose corrective actions (who, what, when).
4. Suggest preventive steps.

Announcement of the management responses

Certification Centre
By Crence

Certification Centre
By Crence

Common findings

Area	Strong Practice	Common Gap
Governance	Clear ownership	Limited Board visibility
STR	Defined chain	Weak documentation
Risk Assessment	Known method	Outdated frequency
Training	Regular sessions	Poor record traceability

Certification Centre
By Crence

NAVIGATING AML EXPECTATIONS ACROSS HIGH-RISK SECTORS

Theo Matundura

Managing Partner, T.M.M
Partners Advocates

Context

Kenya’s grey-listing by FATF highlights AML vulnerabilities among DNFBPs — real estate, legal, and accounting sectors.

Regulatory gaps persist despite amendments to POCAMLA (2009).

Certification Centre By Crence

T.M.M & PARTNERS ADVOCATES
LEGAL EXPERTISE, PERSONALIZED SERVICE

Who Are DNFBPs?

- DNFBPs: Designated Non-Financial Businesses and Professions.
- Examples: Real estate agents, lawyers, accountants, TCSPs, and casinos.
- They act as ‘gatekeepers’ to the economy.

Certification Centre By Crence × T.M.M & PARTNERS ADVOCATES
LEGAL EXPERTISE, PERSONALIZED SERVICE

Why High-Risk?

- Criminals shift to DNFBPs as banking controls tighten.
- High-value transactions, confidentiality, and weak oversight make these sectors attractive for laundering.

Real Estate Sector

Vulnerabilities:

- - High-value, cash-based deals
- - Complex ownership structures
- - Weak regulatory oversight

AML Expectations:

- - CDD/EDD & STR filing
- - Record keeping (7 years)
- - Risk assessments & compliance culture

Certification Centre By Crence

T.M.M & PARTNERS ADVOCATES
LEGAL EXPERTISE, PERSONALIZED SERVICE

Real Estate Examples

- Terror financing through property sale (2024)
- Mass non-compliance & FRC crackdowns (2025)
- Use of shell companies for property acquisition

Certification Centre By Crence

T.M.M & PARTNERS ADVOCATES
LEGAL EXPERTISE, PERSONALIZED SERVICE

Legal Professionals

Vulnerabilities:

- - Misuse of trust accounts
- - Abuse of client confidentiality
- - Company formation for concealment

AML Duties:

- - Trigger activities define obligation
- - STR filing required when suspicious
- - Internal AML policies mandatory

Certification Centre By Crence

T.M.M & PARTNERS ADVOCATES
LEGAL EXPERTISE, PERSONALIZED SERVICE

Accounting Professionals

Vulnerabilities:

- - Audit gaps & tax evasion structures
- - False bookkeeping

AML Expectations:

- - KYC beyond surface-level
- - Identify trigger activities
- - File STRs when suspicions arise

Certification Centre By Crence × T.M.M & PARTNERS ADVOCATES
LEGAL EXPERTISE, PERSONALIZED SERVICE

Cross-Cutting Challenges

- Limited awareness & training
- Weak beneficial ownership transparency
- Fear of losing clients
- Limited regulatory capacity
- Difficulty applying Risk-Based Approach (RBA)

Certification Centre By Crence

T.M.M & PARTNERS ADVOCATES
LEGAL EXPERTISE, PERSONALIZED SERVICE

Way Forward

- Invest in AML technology
- Strengthen internal policies
- Foster compliance culture from leadership
- Adopt genuine RBA
- Report suspicions promptly

Certification Centre By Crence × T.M.M & PARTNERS ADVOCATES
LEGAL EXPERTISE, PERSONALIZED SERVICE

Conclusion

- Proactive compliance = professional integrity.
- Kenya’s DNFBPs must evolve from regulatory checklists to strategic AML partners.

Certification Centre By Crence

T.M.M & PARTNERS ADVOCATES
LEGAL EXPERTISE, PERSONALIZED SERVICE

FATF Recommendations 18 & 23: Group-Wide AML/CFT Programmes

FATF Recommendation 18 requires financial and certain DNFBP groups to implement group-wide AML/CFT programmes.

This ensures consistent customer due diligence, record keeping, and internal controls across all branches and subsidiaries.

Recommendation 23 extends obligations to DNFBPs—law firms, accountants, real estate agents, TCSPs—based on their risk exposure.

These requirements aim to improve coordination, information sharing, and overall AML effectiveness.

Applying Group-Wide AML Requirements to DNFBPs

Countries have discretion to determine when to extend group-wide AML requirements to DNFBPs. Decisions should be risk-based, practical, and aligned with the goal of improving AML/CFT effectiveness.

Key considerations include:

- The ML/TF risk profile and interconnection between group entities
- Existence of a coordinating or parent entity capable of enforcing group AML policies
- Shared compliance systems (e.g., KYC tools, training, audits)
- Commonality in operations and business models across jurisdictions
- Scale and materiality of the DNFBP structure

Common DNFBP Group Structures

FATF identifies several DNFBP structural types where group-wide AML controls may apply:

- Mixed FI-DNFBP groups – e.g., TCSP or law firm under a banking group.
- Professional networks – e.g., international law or audit firms sharing compliance standards.
- Corporate conglomerates – e.g., real estate holding companies managing multiple subsidiaries.
- Franchise models – independent entities under a shared brand with limited central oversight.

The application of AML programmes depends on the risk and level of coordination within these structures.

Implementing Group-Wide Programmes: Practical Steps

To comply effectively, DNFBPs should implement:

1. Unified AML/CFT policies across entities and jurisdictions.
2. Centralized compliance oversight and designated AML officers.
3. Group-level risk assessment covering all branches.
4. Secure information-sharing systems consistent with data privacy laws.
5. Regular AML/CFT training and internal audit reviews.
6. Consistent record-keeping and suspicious activity escalation processes.

Kenyan Context: DNFBPs & FATF Expectations

Kenya’s FRC and POCAMLA regulations increasingly emphasize the role of DNFBPs in national AML/CFT frameworks.

Post-grey-listing reforms focus on:

- Enhancing beneficial ownership transparency.
- Extending AML obligations to real estate, legal, and accounting professionals.
- Mandating internal compliance officers for high-risk entities.
- Encouraging sector associations to establish group or network-level AML policies.
- Strengthening reporting, supervision, and sanctions for non-compliance.

Way Forward: Strengthening DNFBP Compliance Culture

- Adopt risk-based group-wide AML programmes consistent with FATF Rec. 18 & 23.
- Embed compliance leadership at board and partnership levels.
- Use RegTech tools for CDD, transaction monitoring, and information sharing.
- Enhance collaboration with FRC, professional bodies, and peer institutions.
- Transition from reactive compliance to proactive risk management.

Certification Centre By Crence

T.M.M & PARTNERS ADVOCATES
LEGAL EXPERTISE, PERSONALIZED SERVICE

Conclusion: Aligning Practice with Global Standards

Effective AML compliance for DNFBPs requires both institutional commitment and inter-sector collaboration.

Group-wide programmes promote consistent standards, reduce regulatory risk, and strengthen professional integrity.

By aligning with FATF Recommendations 18 and 23, Kenya's DNFBPs can demonstrate maturity, safeguard reputation, and contribute meaningfully to the integrity of the global financial system.

AML Certification Centre By Crence × T.M.M & PARTNERS ADVOCATES
LEGAL EXPERTISE, PERSONALIZED SERVICE

Q&A Session

Certification Centre
By Crence

Thank you!

Certification Centre
By Crence