



KYCAML — Certificate Examination in Anti-Money Laundering & Know Your Customer

Complete Book | Table of Contents | 16 chapters + 7 sections

Module A — Anti-Money Laundering

CH-1	Money Laundering and Terrorism Financing	2
CH-2	Money Laundering - Some Methods	5
CH-3	Money Laundering - Global Measures	9
CH-4	International Guidelines and Standards	12
CH-5	AML/CFT Legislation in Major Countries and Regions	17
CH-6	AML CFT Legislation in India	20
CH-7	AML/CFT Organisation Structure in India	26
CH-8	Money Laundering and Correspondent Banking	30
CH-9	Country Risk	33
CH-10	Transaction Monitoring and Reporting	37

Module B — Know Your Customer

CH-1	KYC Policy and Customer Acceptance Policy	43
CH-2	Customer Identification Procedure and Risk Management	46
CH-3	KYC Specific Requirements	50
CH-4	Organisational Set Up for KYC AML	56
CH-5	Topical Issues Related to KYC AML	59
CH-6	Training and Awareness	63

Additional Resources

—	Case Studies — Module A: Anti-Money Laundering	65
—	Case Studies — Module B: Know Your Customer	79
—	Mega Tests — Mega Test 1 — 100 Questions (Full Syllabus)	87
—	Mega Tests — Mega Test 2 — 100 Questions (Full Syllabus)	96
—	Mega Tests — Mega Test 3 — 100 Questions (Full Syllabus)	106
—	Mega Tests — Mega Test 4 — 100 Questions (Full Syllabus)	115
—	Mega Tests — Mega Test 5 — 100 Questions (Full Syllabus)	125

CH-1

Money Laundering and Terrorism Financing

Topic 1 — Money Laundering and Its Origin

- **Meaning** — Money laundering is the processing of **criminal proceeds** to **disguise their illegal origin**.
- **Washing** — Dirty money is “washed” through financial transactions until it appears clean.
- **Limit** — Laundering changes only the **appearance** of the funds.
- **No legal cure** — It never makes criminal money **legally earned**.

Typical sources of “dirty money”	Common laundering routes
Drug trafficking	Investment in real estate and luxury businesses
Illegal arms sales	Mixing illicit cash with genuine business receipts
Smuggling and extortion	Trade manipulation – false invoices, prices, fake movement of goods
Gambling and bootlegging	Offshore accounts and onward investment in businesses

- **History is not law** — The history of the term does **not** define the legal offence.
- **Apply the law** — Apply the **relevant law** to the actual conduct and proceeds.
- **Trade cases** — Check **invoices, prices and genuine movement of goods**.
- **Section 3, PMLA** — In India the offence is defined in **Section 3, Prevention of Money-laundering Act, 2002 (PMLA)**.
- **See** — Module A Ch 6 (p. 20) for the full Section 3 offence and the Section 4 punishment.
- **Three stages** — Placement, layering and integration.
- **Analytical stages** — These are **analytical stages**; a case need not pass through three separate steps.
- **See** — Module A Ch 2 (p. 5) for what happens at each stage and how banks detect it.

Example: Illicit cash is mixed with genuine shop receipts, moved through linked companies and used to buy property. The clean-looking records explain the appearance, not legal ownership of the criminal proceeds.

Remember this

- Laundering hides the **source**; the money stays **proceeds of crime**.
- PMLA Sec 4: **3–7 years** RI + fine; up to **10 years** for NDPS-linked proceeds.

Topic 2 — Impact on the Economy, Society and Politics

Money laundering supports **criminal networks**, **destabilises financial systems** and breeds **corruption and fraud**.

Area	Effect	Illustration
Economic – unfair competition	Illegal businesses outcompete honest ones	Front firm sells below cost using laundered cash
Economic – price distortion	Laundered money inflates real estate and markets	Corrupt politician buys high-end property; prices rise artificially

Area	Effect	Illustration
Economic – slowdown	Legitimate businesses struggle to compete	Honest traders exit the market
Economic – exchange rates	Cross-border illegal funds affect currency values	Sudden unexplained capital flows
Social	More corruption; organised crime (drugs, terrorism, fraud) grows; “safe haven” for criminals	Official launders bribes offshore and escapes justice
Political	Criminals gain political power; democratic institutions weaken; bribery rises	Cartel funds politicians to gain legal protection

Topic 3 — Size of the Money Laundering Problem

- **Only estimates** — Laundering is hidden, so only **estimates** exist.
- **Compare with care** — Estimates differ in **scope, population and method**.
- **No verified total** — No historical estimate establishes a verified current annual total.

Study	Measure	Estimate
J. Walker model	Global laundering (particular model)	USD 2.85 trillion; about 9.5% of GDP
IMF consensus range	Global laundering, rough range	2%–5% of global GDP
UNODC, 20 OECD countries	Organised-crime turnover – not global laundering	USD 614 billion; about 1.8% of their GDP
UNODC study	Funds available for laundering	USD 1.6 trillion ; 2.7% of global GDP (range 2.1%–4.0%)

The IMF figure is a **range with substantial uncertainty**, not an audited fixed amount or a fixed 5% rate. The OECD row measures crime turnover, not laundering.

Topic 4 — Impact on the Financial System and Banks

Why banks and financial institutions are vulnerable

- **Public money** — They handle **public money**.
- **Many services** — They offer loans, deposits, remittances and other services.
- **Hard to trace** — They work in a **globalised, technology-driven** environment that makes tracing difficult.

Without prevention	Reputation impact	Regulatory consequences
Reputation risk – loss of public trust	Laundering links banks to criminals	Heavy penalties and fines
More financial frauds	Low-regulation locations attract illegal money	Loss of banking licence
Weaker economic stability	Confidence is lost when banks figure in scandals	Increased government scrutiny

Banks must operate under strict **legal, professional and ethical standards**. Prevention rests on **trained staff, automated (AI-based) transaction monitoring** and robust **KYC and AML measures**.

Topic 5 — International Definitions of Money Laundering

Institution	Definition
United Nations (UNODC)	Method by which criminals disguise the illegal origin of wealth to avoid suspicion and prevent a trail of evidence
International Monetary Fund (IMF)	Process by which proceeds of criminal activity are disguised to conceal their illicit origin
Financial Action Task Force (FATF)	Processing of criminal proceeds to disguise their illegal origin
Interpol	Any act to conceal or disguise illegally obtained proceeds so that they appear legitimate
EU Directive 91/308	Disguising the true nature, source or ownership of property derived from serious crime
Office of the Comptroller of the Currency (USA)	Concealing criminal activity linked to tax evasion or drug trafficking

- **Common thread** — Concealing the illegal origin of proceeds so that they appear legitimate.
- **Offshore leaks** — Leaked offshore-records cases showed politicians, celebrities and businesses hiding wealth in **offshore accounts**.

Topic 6 — Case Studies and Lessons for Banks

Case	What went wrong	Outcome / lesson
BCCI (operated in 70+ countries)	Complex structures – shell companies, subsidiaries; offshore centres used to evade regulation; racketeering, fraud and laundering charges	Closed by regulators; vet correspondent banks, major shareholders and foreign banks
European Union Bank, Antigua	Offshore bank advertising strong bank secrecy ; weak offshore supervision	Collapsed; monitor offshore banks and online banking platforms
Riggs Bank – Pinochet	Helped conceal the former Chilean ruler's assets; hidden beneficial interests and transfers kept from US regulators	USD 16 million criminal fine and severe reputational damage; ensure transparent KYC and report suspicious activity
Riggs Bank – Mbasogo	Equatorial Guinea ruler's funds: USD 11 million cash received and USD 26.4 million wires without required reporting	Assess PEP risk , apply enhanced monitoring, report when tests are met
HSBC	AML control failures	USD 1.256 billion forfeiture plus USD 665 million civil penalties
Deutsche Bank	AML control failures	USD 425 million New York DFS fine; separate UK FCA penalty of GBP 163,076,224
Bank of Baroda (Ashok Vihar branch)	Irregular outward import remittances reported by the bank itself	CBI and ED cases, charge sheet; monitor large outward remittances and verify import documents

Teaching illustration	Control failure	Lesson
Forged cheques and false accounts	Accounts opened in false identities to cash stolen cheques, drafts, postal orders	Strict KYC at onboarding; transaction monitoring
Fraudulent overdraft against FDs	Forged FD records used to raise overdrafts	Independently verify FD-linked loans; detect unusual withdrawals
Fake imports across multiple accounts	Fictitious accounts, fake companies and invoices; amounts split to avoid detection	Flag multiple accounts under one identity or common control; pattern analysis

These unnamed illustrations are teaching cases, not verified penalty orders. Global regulators are **stricter**, penalties include **criminal action**, and **individual bankers** can be fined or imprisoned.

Topic 7 — Current Controls for Banks

Key issue	Action required
KYC violations	Strict identity verification and background checks
Unusual transactions	Automated monitoring with real-time alerts
High-risk customers (PEPs, offshore accounts)	Enhanced due diligence for politically exposed persons
Shell companies and fake imports	Verify corporate accounts and import-export invoices
Cross-border transactions	Stronger oversight of forex transfers and wire transactions

Foreign PEPs under the RBI (Commercial Banks – Know Your Customer) Directions, 2025

- **Foreign PEP** — Identify PEP status (including family members and close associates), establish source of funds / wealth, obtain senior-management approval and apply enhanced ongoing monitoring.
- **Not automatic** — PEP status alone does not make every transaction reportable.
- **See** — Module B Ch 3 (p. 50) for PEP due diligence.
- **Walk-in customers** — Identify and verify for transactions of ₹50,000 or more, single or connected.
- **See** — Module A Ch 10 (p. 37) for CTR and STR thresholds and timelines, and Module B Ch 3 (p. 50) for walk-in customers.

Do **not** restrict an account merely because an STR was filed. Keep reporting **confidential** (no tipping-off) and escalate supported concerns through the bank's **Principal Officer**.

Remember this

- CTR: above ₹10 lakh, by the 15th of next month · STR: no minimum, 7 working days.

Topic 8 — Terrorist Financing

- **Meaning** — Terrorist financing is mobilising funds for terrorist acts or organisations.
- **Sources** — Funds may come from **legal or illegal** sources.
- **Key difference** — Money laundering conceals the **source** of funds; terrorist financing conceals their **purpose**.

Offence under Article 2, UN International Convention for the Suppression of the Financing of Terrorism

- **Act** — The **unlawful and wilful** provision or collection of funds, directly or indirectly.
- **Mental element** — With the **intention or knowledge** that the funds will be used, in whole or part, for a listed purpose.
- **Purpose (a)** — Offences under the listed counter-terrorism treaties.
- **Purpose (b)** — Acts intended to cause **death or serious injury** to civilians or other protected persons.
- **Aim of (b)** — To **intimidate a population or compel a government or international organisation**.
- The funds need **not actually be used** for the terrorist act – but the required **intent or knowledge** must still be established.
- An unwitting courier is not automatically guilty; ordinary charity or an unusual payment alone does not establish the offence.

- In India, raising funds for a terrorist act is punishable under **Section 17, Unlawful Activities (Prevention) Act, 1967** – imprisonment of **not less than 5 years**, extendable to **life**, and fine.

“Terrorism” is defined differently across countries; political, religious and regional factors matter. A group may be called **rebels** by one nation and **terrorists** by another.

Example: A charitable NGO collects donations as a front and secretly passes them to a terrorist group – lawful-source money diverted to a terrorist purpose.

Topic 9 — Money Laundering vs Terrorist Financing

Aspect	Money laundering	Terrorist financing
Source of funds	Always illegal (crime, fraud, drugs)	Legal or illegal (donations, smuggling, fraud)
Use of funds	Made to appear lawful through assets or businesses	Criminal or violent activities (attacks, propaganda)
Main goal	Hide the source	Hide the purpose
Common techniques	Shell companies, offshore accounts, fake invoices	Fake charities, cash couriers, trade-based transfers
Typical amounts	Usually large	Can be small or large

The two are **linked**: both misuse financial institutions, both use **trade-based** movement (fake invoicing, cross-border remittances) and criminal funds can be **diverted to terrorism**.

Example: A cybercriminal hacks bank accounts and sends the stolen money to a terrorist group abroad – proceeds of crime used for terrorist financing.

KYCAML | Module A | CH-1 | MCQs

Q1. A trader mixes cash from narcotics sales with genuine shop receipts and buys property with the combined funds. Which statement is correct? [Ref: Topic 1, p. 2]

- The property becomes lawfully owned once taxes are paid
- Laundering changes only the appearance; the funds remain proceeds of crime
- No offence arises because genuine receipts are mixed in
- It is terrorist financing because funds are concealed

Q2. The core difference between money laundering and terrorist financing is that terrorist financing primarily conceals the: [Ref: Topic 9, p. 4]

- Purpose of the funds
- Source of the funds
- Size of the funds
- Currency of the funds

Q3. A customer donates money from his salary to a front NGO knowing it will fund an attack, but the attack never takes place. Under Article 2 of the UN financing convention: [Ref: Topic 8, p. 4]

- No offence, as the funds were not used
- No offence, as the source was lawful
- Offence only if the NGO is a listed entity
- Offence is complete if the required intent or knowledge is established

Q4. Which international estimate measures organised-crime turnover rather than global money laundering? [Ref: Topic 3, p. 2]

- (a) IMF consensus range
- (b) UNODC estimate for 20 OECD countries
- (c) UNODC funds-available-for-laundering estimate
- (d) Walker model

Q5. Laundered money pours into luxury housing in a city and prices rise artificially. This is an example of the: [Ref: Topic 2, p. 2]

- (a) Political effect
- (b) Social effect
- (c) Economic effect of price distortion
- (d) Exchange-rate effect

Q6. Which definition of money laundering specifically refers to property derived from serious crime and its true nature, source or ownership? [Ref: Topic 5, p. 3]

- (a) Interpol
- (b) FATF
- (c) IMF
- (d) EU Directive 91/308

Q7. In the Riggs Bank–Mbasogo case, the core failure was: [Ref: Topic 6, p. 3]

- (a) Receiving large cash and wire flows of a PEP without required reporting
- (b) Lending to a sovereign without collateral
- (c) Forged cheques of walk-in customers
- (d) Excessive forex positions

Q8. A bank opens an account for a senior official of a foreign government. Which step is NOT required under RBI KYC Directions? [Ref: Topic 7, p. 4]

- (a) Senior-management approval
- (b) Reasonable measures to establish source of funds or wealth
- (c) Filing an STR for every transaction of the customer
- (d) Enhanced ongoing monitoring

Q9. A branch files an STR on a customer. The correct next step is to: [Ref: Topic 7, p. 4]

- (a) Freeze the account immediately
- (b) Inform the customer so he can explain
- (c) Close the account within 7 days
- (d) Keep the report confidential and continue risk-based monitoring

Q10. A customer deposits cash of ₹4 lakh, ₹3.5 lakh and ₹3 lakh in one month in integrally connected transactions. CTR treatment: [Ref: Topic 7, p. 4]

- (a) Not reportable, each is below ₹10 lakh
- (b) Reportable, as the monthly aggregate of ₹10.5 lakh exceeds ₹10 lakh
- (c) Reportable only if an STR is filed
- (d) Reportable only if any single deposit exceeds ₹5 lakh

Q11. A walk-in customer seeks a demand draft against cash of ₹50,000. The bank must: [Ref: Topic 7, p. 4]

- (a) Identify and verify the customer
- (b) Issue without identification as he has no account
- (c) File a CTR
- (d) Refuse the transaction

Q12. Under Section 17 of UAPA, raising funds for a terrorist act attracts imprisonment of: [Ref: Topic 8, p. 4]

- (a) Up to 3 years
- (b) Not less than 5 years, extendable to life
- (c) 3 to 7 years
- (d) Up to 10 years only

Q13. Which technique is more typical of terrorist financing than of money laundering? [Ref: Topic 9, p. 4]

- (a) Over-invoiced imports to shift profits
- (b) Shell companies in tax havens
- (c) Front charities and cash couriers
- (d) Purchase of luxury hotels

Q14. Banks are especially vulnerable to money laundering mainly because they: [Ref: Topic 4, p. 2]

- (a) Are owned by governments
- (b) Charge high interest
- (c) Deal only in cash
- (d) Handle public money and offer many services in a globalised, technology-driven system

Q15. The three-stage model of placement, layering and integration is best understood as: [Ref: Topic 1, p. 2]

- (a) An analytical model; a case may combine or omit stages
- (b) A legal requirement for the offence
- (c) A strict sequence every case follows
- (d) Applicable only to terrorist financing

Answer key

Q	Ans	Q	Ans	Q	Ans	Q	Ans	Q	Ans
1	b	4	b	7	a	10	b	13	c
2	a	5	c	8	c	11	a	14	d
3	d	6	d	9	d	12	b	15	a

CH-2

Money Laundering - Some Methods

Topic 1 — Nature of the Money Laundering Process

- **Evolving** — Money laundering is **complex and constantly evolving**.
- **Many stages** — Criminals use financial institutions at **multiple stages**.
- **Choice of method** — It depends on the **source and amount** of illegal funds.
- **Other factors** — The **geographic scope** and the **sophistication** of the techniques also matter.

Stage	What happens	Methods	Bank detection measures
1. Placement	Illicit proceeds enter the financial system	Many small cash deposits; cash smuggling across borders; casinos, betting, cash-based businesses	Large or unusual cash deposits; repeated transactions just below CDD thresholds; customers reluctant to give KYC details
2. Layering	Origin obscured by complex transactions	Multiple transfers across accounts and countries; fake import/export invoices; shell companies and offshore accounts; crypto conversions	Frequent international transfers with no clear business purpose; high-value flows from unknown sources; unusual buys of art, jewellery, real estate