CHARTA LEARNING · LESSON NOTES

Money Laundering and Terrorist Financing

FRM Part II

1 A story: the dots nobody joined

- A small shop's account takes in cash far beyond its trade
- Each deposit looks ordinary on its own
- Nobody asks who owns the shop, or why money goes abroad
- Calder is fined and its name is damaged
- Answer: manage ML/FT risk like any other major risk

IN THE LESSON

- Imagine a branch of Calder Bank where a small shop opens an account.
- Over the next year the account takes in cash far beyond anything a shop that size could earn, and then sends it abroad.
- Each deposit looks ordinary on its own.
- Nobody asks who really owns the shop, or why its money travels so far.
- Later the police show that the account was moving the proceeds of crime.
- Calder is fined by its supervisor, and its name is damaged with customers and other banks.
- The failure was not one transaction but the lack of any system.
- The Basel Committee's answer is that a bank must manage money laundering and terrorist financing risk like any other major risk.

2 What the two crimes are

- Money laundering (ML): make crime money look legitimate
- Classic stages: placement, layering, integration
- Terrorist financing (FT): money to support terrorism
- FT money may be clean, and the amounts small
- ML hides where money came from; FT, where it goes

IN THE LESSON

- First, the two crimes.
- Money laundering, shortened to M L, is the process of making the proceeds of crime look as if they came from a legitimate source.
- A classic description has three stages.
- Placement puts the dirty cash into the financial system, layering moves it through many transactions to blur the trail, and integration brings it back as apparently clean wealth.
- Terrorist financing, shortened to F T, is providing money to support terrorism.
- Here the money may be clean, such as a salary or a donation, and the amounts are often small.
- So a useful contrast is that money laundering hides where money came from, while terrorist financing hides where money is going.
- Banks fight both under the label A M L and C F T: anti money laundering and countering the financing of terrorism.

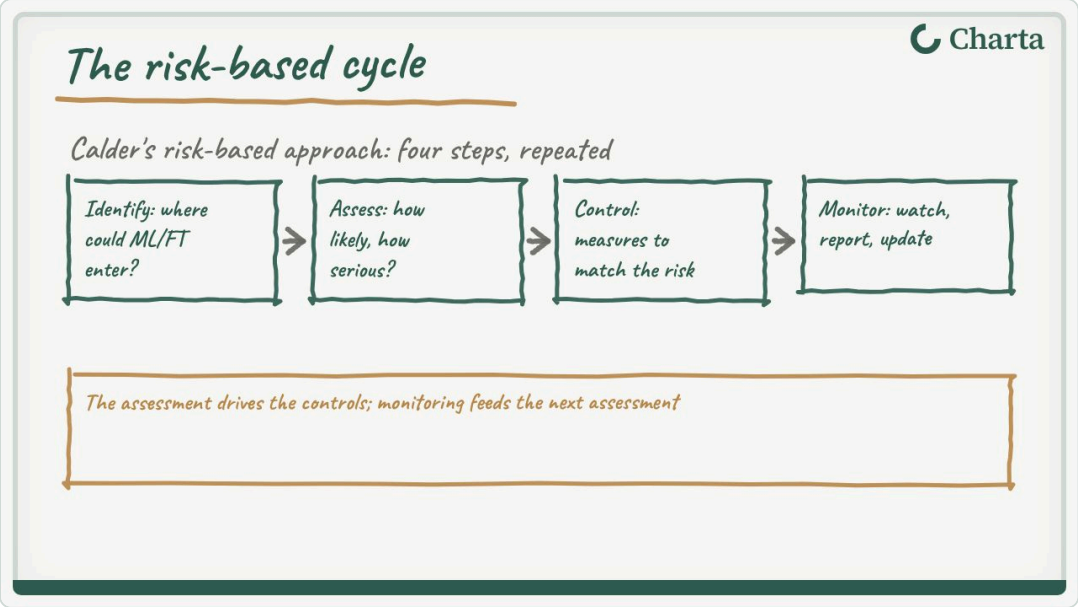
3 Why a bank must treat it as a major risk

- Reputational: customers and other banks lose trust
- Operational: weak processes and systems are exploited
- Compliance: fines and sanctions from supervisors
- Concentration: reliance on a few risky customers or funds
- Basel: identify, assess, control and monitor it

IN THE LESSON

- Why is this a risk topic and not only a legal one?
- Weak controls expose a bank to familiar risks.
- Reputational risk: once a bank is linked with crime, customers and other banks lose trust in it.
- Operational risk: criminals exploit weak processes and systems, a failure of people, processes or systems like any other operational loss.
- Compliance risk: supervisors impose fines and sanctions, and can restrict the business.
- And concentration risk, when a bank leans heavily on a few risky customers or sources of funds.
- So the Basel Committee expects a bank to identify this risk, assess it, control it and keep monitoring it, exactly as it would credit or market risk.

4 The risk-based cycle



IN THE LESSON

- Here is the Basel approach: four steps, repeated as a cycle.
- Step one, identify: where could money laundering or terrorist financing enter the bank, through which customers, products, channels and countries?
- Step two, assess: how likely is it, and how serious would it be?
- Step three, control: put in place measures that match what the assessment found.
- Step four, monitor: watch customers and transactions, report what is suspicious, and update the picture.
- This is called the risk based approach, which means the bank spends its effort where the risk is greatest instead of treating every customer the same.
- Now the key line at the bottom.
- The assessment drives the controls, and what monitoring finds feeds back into the next assessment.

5 Four places to look for risk

Calder's assessment covers four dimensions

Dimension	Higher-risk example at Calder
Customers	Cash-heavy firms, opaque ownership
Products and services	Trade finance, private banking
Delivery channels	Remote opening, intermediaries
Geographies	Weak AML rules, high corruption

IN THE LESSON

- The assessment must look across four dimensions.
- The first is customers.
- At Calder, cash heavy businesses and companies with opaque ownership score higher.
- The second is products and services.
- Trade finance can hide value in invoices, and private banking serves wealthy clients with complex affairs.
- The third is delivery channels, meaning how the bank meets its customers.
- Opening an account remotely, without ever meeting the person, or through an intermediary, makes it harder to know who you are dealing with.
- The fourth is geographies.
- Countries with weak anti money laundering rules or high corruption raise the risk of customers and transactions linked to them.
- None of these labels a customer a criminal.
- They are risk factors, combined into a rating.

6 What a sound assessment looks like

- Documented: written down, with reasons
- Regularly updated, and when new risks appear
- Covers the whole bank: customers, products, channels
- Owned and approved by senior management
- Its results set the controls and the resources

IN THE LESSON

- What makes Calder's assessment sound?
- First, it is documented: written down, with the reasoning for each rating, so a supervisor or an auditor can follow it.
- Second, it is regularly updated, on a set timetable and also whenever something changes, such as a new product, a new country or a new kind of fraud.
- Third, it covers the whole bank, all customers, products and channels.
- Fourth, senior management owns and approves it, because it decides where the bank's money and effort go.
- And fifth, its results set the controls and the resources, with more staff and tighter checks where the risk is high.
- An assessment that changes nothing in practice has failed its purpose.

7 Example 1: rating a new customer

Calder scores each dimension from 1 (low) to 3 (high) and adds them up

Customer: trading company	some cash takings	**2**
Product: trade finance	value hidden in invoices	**3**
Channel: opened remotely	owners never met	**2**
Geography: risky ports	weak AML rules	**3**
Total score	2 + 3 + 2 + 3	**10 of 12: High**

Bands: 4–6 low, 7–8 medium, 9–12 high. High: enhanced measures

IN THE LESSON

- Let us rate a new applicant, Brightwater Trading, an import and export firm.
- Calder scores each dimension from one, for low, to three, for high, and adds them up.
- The customer is a trading company with some cash takings, so it scores two.
- The product is trade finance, where value can be hidden in invoices, so three.
- The account was opened remotely, and nobody met the owners in person, so two.
- The geography is trade with ports in countries with weak anti money laundering rules, so three.
- The total is two plus three plus two plus three, which is ten out of twelve.
- Calder's bands are four to six for low, seven to eight for medium, and nine to twelve for high.
- Ten is high, so Brightwater gets enhanced measures.
- Assessment first, then controls.

8 Controls in proportion to the risk

The rating decides how deep the measures go

Risk	Measures at Calder
Higher	Enhanced: source of funds, senior sign-off
Standard	Standard due diligence and monitoring
Demonstrably lower	Simplified, but still some measures
Any situation	Never no measures at all

IN THE LESSON

- Now the controls follow, in proportion.
- Higher risk situations get enhanced measures.
- At Calder that means asking where the customer's money and wealth come from, getting a senior manager to sign off the relationship, and watching the account more closely.
- Standard risk gets standard due diligence and normal monitoring.
- Situations that are demonstrably lower risk, meaning the bank can show why, may get simplified measures, such as fewer documents at the start or less frequent reviews.
- But simplified still means some measures.
- The last row is the rule people forget: in any situation, there is never no measure at all.
- Risk based changes how deep the checks go, never whether they happen.

9 Example 2: where the review effort goes

60,000 customers. Reviews: high every year, medium every 2 years, low every 5

High: 5% of customers	3,000 ÷ 1 year	**3,000**
Medium: 25% of customers	15,000 ÷ 2 years	**7,500**
Low: 70% of customers	42,000 ÷ 5 years	**8,400**
Reviews a year in total	3,000 + 7,500 + 8,400	**18,900**
High tier's share of reviews	3,000 ÷ 18,900	**15.9%**

High: 5% of customers, 15.9% of reviews, over 3×. No tier is zero

IN THE LESSON

- Here is how ratings move real effort.
- Calder has sixty thousand customers.
- Five per cent are high risk, which is three thousand, and each is reviewed every year, so three thousand reviews.
- Twenty five per cent are medium risk, fifteen thousand customers, reviewed every two years, so seven thousand five hundred reviews a year.
- Seventy per cent are low risk, forty two thousand customers, reviewed every five years, so eight thousand four hundred a year.
- In total that is eighteen thousand nine hundred reviews a year.
- The high risk tier is only five per cent of customers, but it takes fifteen point nine per cent of the reviews, more than three times its share.
- Even the low tier is still reviewed, so no tier drops to zero.
- Effort follows risk.

10 Who owns it: the three lines of defence

Accountability stays with the board and senior management

Who	Role in AML/CFT
Board and senior management	Own the framework, approve policy
1st line: business units	Know customers, manage risk daily
2nd line: compliance	Oversee, led by a senior officer
3rd line: internal audit	Test the framework independently

IN THE LESSON

- Who is responsible?
- Accountability stays with the board and senior management.
- At the top, the board and senior management own the framework.
- They approve the policy and make sure there are enough resources.
- Below them sit the three lines of defence.
- The first line is the business units, such as Calder's branches and relationship managers.
- They meet the customers, so they must know them and manage the risk day to day.
- The second line is an independent compliance function, led by a senior A M L and C F T officer.
- It sets standards, oversees the first line and challenges it.
- The third line is internal audit, which tests independently whether the whole framework actually works.
- The exam point is that tasks can be delegated, but accountability cannot be pushed below senior management.

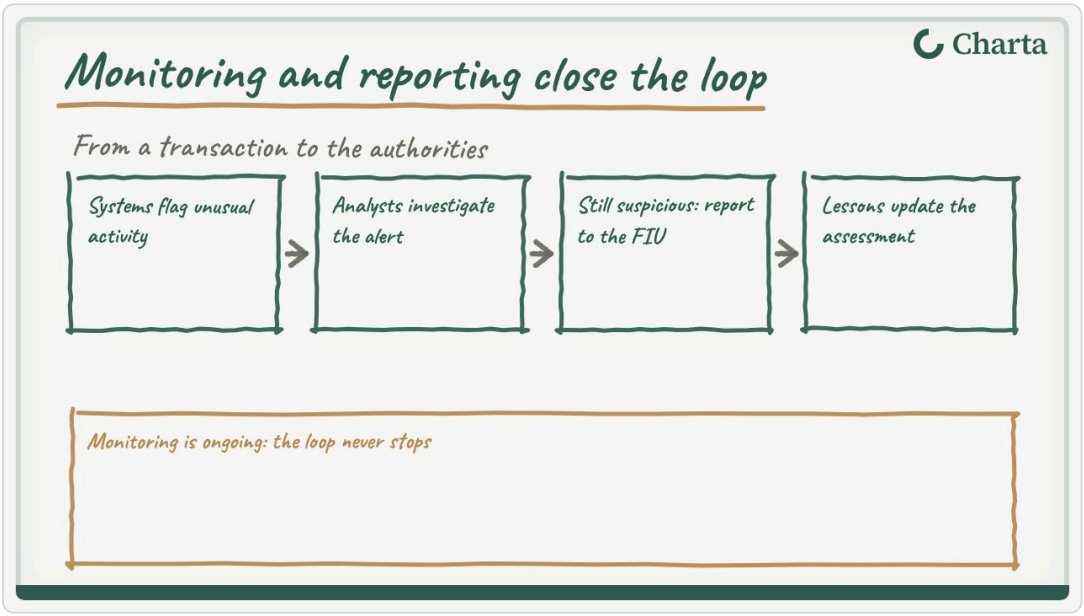
11 The AML/CFT officer

- Senior, with authority and enough resources
- Independent: no business targets to meet
- Direct access to the board
- Access to the customer and transaction information
- Escalates problems, including suspicious transactions

IN THE LESSON

- The compliance function needs a strong leader.
- Calder's A M L and C F T officer must be senior, with real authority and enough staff and systems to do the job.
- The officer must be independent, which means not carrying business targets, because someone paid for new accounts cannot be relied on to turn customers away, so the officer must not report to sales.
- The officer needs direct access to the board, so that bad news reaches the top without being filtered by the business.
- The officer needs access to the customer and transaction information required to see the risk.
- And the officer escalates problems, including suspicious transactions, rather than letting them sit.

12 Monitoring and reporting close the loop



IN THE LESSON

- The last part of the cycle is ongoing monitoring and reporting.
- First, Calder's systems flag unusual activity, such as transactions that do not fit the customer, or sudden spikes in cash.
- Second, analysts investigate each alert, looking at the customer's profile and history.
- Third, if the activity is still suspicious, the bank reports it to the financial intelligence unit, shortened to F I U.
- That is the national agency that receives these suspicious transaction reports and passes intelligence on to law enforcement.
- Fourth, what the bank learns flows back to update its risk assessment, so a product that keeps producing reports is rated higher next time.
- Monitoring is ongoing, and the loop never stops.

13 Example 3: the alert funnel

One month at Calder: the monitoring system raises 12,000 alerts

Alerts raised	by the system	**12,000**
Escalated to a case	4% × 12,000	**480**
Reported to the FIU	25% × 480	**120**
Reports per alert	120 ÷ 12,000	**1%**
Reports from prepaid cards	84 ÷ 120	**70%**

IN THE LESSON

- Let us follow one month of Calder's monitoring.
- The system raises twelve thousand alerts.
- Analysts escalate four per cent into full cases, which is four hundred and eighty.
- After investigation, twenty five per cent of those cases are still suspicious, so Calder files one hundred and twenty suspicious transaction reports with the F I U.
- That is one report for every hundred alerts, or one per cent.
- Two lessons follow.
- First, a flood of alerts is not the same as good monitoring.
- The system must be tuned so that analysts can investigate properly and report promptly.
- Second, eighty four of the one hundred and twenty reports, seventy per cent, came from prepaid cards.
- That finding goes back into the assessment, and prepaid cards are rated higher.

14 Mistakes to avoid: risk-based is not 'do less'

- Reading risk-based as permission to do less
- Letting any customer or product get no measures
- Setting controls first, then writing the assessment
- Leaving the assessment unchanged for years
- Delegating accountability below senior management

IN THE LESSON

- Here are the mistakes the exam likes.
- The biggest is reading risk based as permission to do less.
- It means doing more where the risk is high and less where it is shown to be low, not cutting effort across the board.
- Second, letting any customer or product get no measures at all.
- Third, getting the order wrong, by choosing the controls first and writing an assessment afterwards to justify them.
- The assessment must drive the controls.
- Fourth, leaving the assessment unchanged for years while products, customers and criminals change.
- And fifth, believing that accountability can be handed to the compliance officer or to a junior team.
- Work can be delegated, but the board and senior management remain answerable.

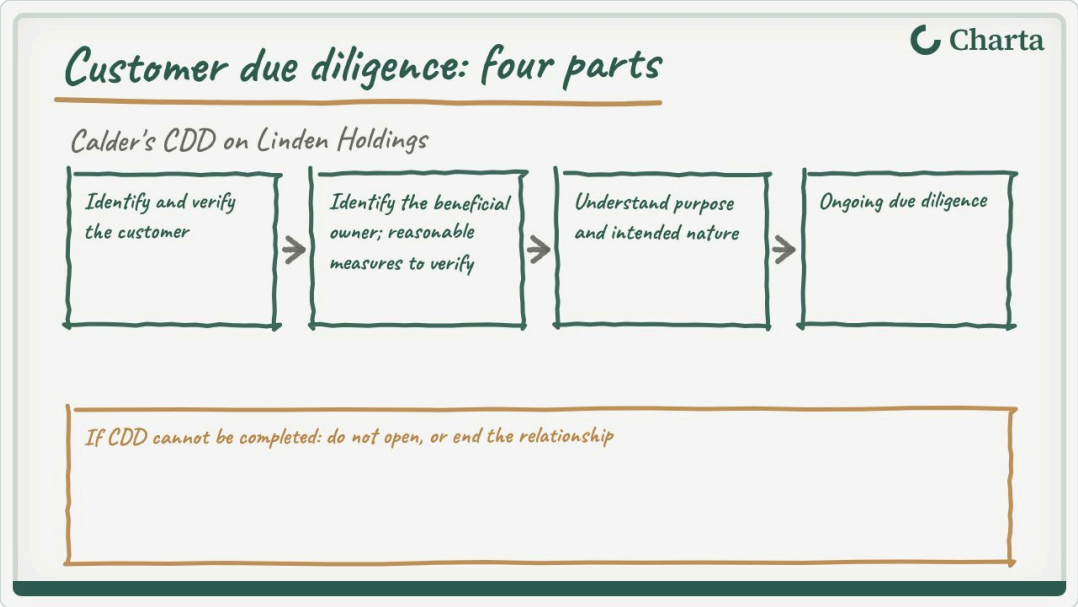
15 A new customer walks in

- Linden Holdings wants a business account
- Directors are named, but who stands behind them?
- Calder must know who it is dealing with
- The tool: customer due diligence (CDD)
- Guided by a risk-based customer acceptance policy

IN THE LESSON

- Now to the customer.
- Linden Holdings, a company, asks Calder to open a business account.
- It sends its registration papers, which name two directors.
- But the papers do not say who stands behind the directors, who really owns and controls the company, or why it needs the account.
- Before taking the money, Calder must know who it is dealing with.
- The tool for this is customer due diligence, shortened to C D D.
- It is guided by a customer acceptance policy, the bank's written rules on which customers it will take on and on what terms, and that policy is itself risk based.
- Let us see what customer due diligence requires.

16 Customer due diligence: four parts



IN THE LESSON

- Customer due diligence has four parts.
- First, identify the customer and verify that identity.
- Identify means collecting the facts; verify means checking them against reliable evidence.
- Second, identify the beneficial owner, the real person behind the customer, and take reasonable measures to verify who that is.
- Third, understand the purpose and intended nature of the relationship.
- Why does Linden want this account, and what activity should Calder expect to see?
- Fourth, ongoing due diligence, meaning the checking does not stop once the account is open.
- And underneath sits the rule that gives the whole thing teeth.
- If customer due diligence cannot be completed, the bank must not open the account, or must end the relationship.

17 Part 1: identify and verify the customer

- Identify: name, address, date of birth or registration
- Verify with reliable, independent sources
- Documents, data or information: passport, registry
- Company: directors, and who may act for it
- The customer's own say-so is not verification

IN THE LESSON

- Part one.
- To identify the customer, Calder collects the basic facts: for a person, the name, address and date of birth, and for a company, its legal name, registration number and address.
- Then it verifies them, using reliable and independent sources.
- Independent is the key word, because the evidence should come from somewhere other than the customer.
- It can be documents, data or information, for example a passport for a person, or an official company registry for a firm.
- For Linden, Calder also confirms the directors and who may act for the company.
- A form the customer filled in is identification, but it is not verification.
- The customer's own say so proves nothing.

18 Part 2: the beneficial owner

- The natural person who ultimately owns or controls
- A human being, never just another company
- Map the ownership and control structure
- Trusts and chains of companies can hide the owner
- Take reasonable measures to verify that person

IN THE LESSON

- Part two.
- The beneficial owner is the natural person who ultimately owns or controls the customer.
- Natural person means a human being.
- So if Linden is owned by another company, that company is not the answer.
- Calder must keep going up the chain until it reaches people.
- To do that, Calder must understand the ownership and control structure of the customer: who owns the shares, and who can direct the company or appoint its directors.
- Control can matter even without a large shareholding.
- Trusts and chains of companies across countries are the classic way to hide the real owner, so the structure must be mapped, not just recorded.
- Finally, the bank takes reasonable measures to verify that the person it has found really is the owner.

19 Example 4: tracing ownership through a chain

Linden: Mara 20% direct; Birch Ltd 50% (Mara 30%, Rex 70%); 30% widely held

Mara: held directly	in her own name	**20%**
Mara: through Birch Ltd	50% × 30%	**15%**
Mara: in total	20% + 15%	**35%**
Rex: through Birch Ltd	50% × 70%	**35%**
Widely held shares	no holder above 5%	**No owner**

Calder's threshold is above 25%: Mara and Rex are both beneficial owners

IN THE LESSON

- Let us map Linden.
- Mara holds twenty per cent directly.
- Birch Limited, another company, holds fifty per cent, and Birch is owned thirty per cent by Mara and seventy per cent by Rex.
- The other thirty per cent is widely held.
- Calder's policy, a common choice, treats anyone owning more than twenty five per cent as a beneficial owner, and, by convention, multiplies stakes along the chain.
- Mara's direct stake is twenty per cent.
- Through Birch she holds fifty per cent times thirty per cent, which is fifteen per cent.
- In total Mara owns twenty plus fifteen, thirty five per cent.
- Rex is not on Linden's register, yet through Birch he owns fifty per cent times seventy per cent, which is thirty five per cent.
- He also controls Birch outright, so by control he would count anyway.
- The widely held shares, with no holder above five per cent, give no owner.
- So both Mara and Rex are beneficial owners, and looking at direct holdings alone would have missed both.

20 Parts 3 and 4: purpose, then ongoing diligence

- Purpose and nature: why the account, what activity
- This sets the 'normal' that monitoring compares against
- Ongoing: scrutinise transactions against that profile
- Keep documents and information up to date
- Review higher-risk customers more often

IN THE LESSON

- Part three is understanding the purpose and intended nature of the relationship.
- Calder asks why Linden wants the account and what activity to expect: which countries it trades with, how much money will flow, and in what form.
- This sets the normal picture that monitoring compares against.
- Part four is ongoing due diligence.
- Calder scrutinises Linden's transactions against that profile, so a firm that said it sells furniture locally but starts receiving large transfers from abroad stands out.
- It keeps the documents and information up to date, for example when directors or owners change.
- And it reviews higher risk customers more often.
- Customer due diligence lasts as long as the account.
- It is not a form filled in on day one.

21 The customer acceptance policy

- Risk-based: clear criteria for which customers to take
- Higher risk, e.g. PEPs: senior management approval
- PEP: someone with a prominent public function
- Not so rigid that it shuts out the disadvantaged
- Basic lower-risk accounts support financial inclusion

IN THE LESSON

- The customer acceptance policy decides whom Calder takes on.
- It is risk based, with clear criteria for which customers are acceptable and under what conditions.
- Higher risk customers need approval from senior management, not just the branch.
- The standard example is a politically exposed person, shortened to P E P.
- That is someone who holds, or has held, a prominent public function, such as a senior politician or judge, whose position could be abused for corruption.
- Such customers are not banned, but they are accepted only with enhanced checks and senior approval.
- At the other end, the policy must not be so rigid that it shuts out people who are financially or socially disadvantaged.
- A basic, lower risk account can serve them, which supports financial inclusion.

22 Example 5: four applicants, four decisions

Calder's acceptance policy applied to four applicants

Applicant	Finding	Decision
Retired teacher	Shown to be low risk	Accept: simplified CDD
Foreign minister	PEP: higher risk	Enhanced CDD, senior sign-off
Refugee, no passport	Must not be shut out	Basic account, other reliable ID
Firm hides its owner	CDD cannot be completed	Decline; consider an STR

IN THE LESSON

- Let us apply Calder's policy to four applicants.
- A retired teacher whose local pension is paid into the account, with a simple, verified profile, is shown to be low risk, and can be accepted with simplified customer due diligence.
- A serving foreign government minister is a politically exposed person, so higher risk: enhanced due diligence, including where the money comes from, and sign off by senior management.
- A refugee with no passport must not be shut out by a rigid rule.
- Calder can offer a basic account, verified with other reliable documents the person has.
- Finally, a company that will not say who owns it cannot complete customer due diligence.
- Calder must decline it, and should consider filing a suspicious transaction report, shortened to S T R.

23 When CDD fails, and relying on others

- CDD incomplete: do not open, or end the relationship
- Consider filing a suspicious transaction report
- Applies to existing customers as well as new ones
- Reliance on a regulated third party, with conditions
- But ultimate responsibility stays with the bank

IN THE LESSON

- Two more rules.
- First, if customer due diligence cannot be completed, the bank must not open the account, and if the customer is already on the books, it must end the relationship.
- Either way, the bank should consider filing a suspicious transaction report.
- The rule covers existing customers as well as new ones, so an old client who stops answering questions during a review is treated the same way.
- Second, reliance.
- Calder may rely on a third party, such as another regulated bank that introduces a client, to perform parts of the due diligence.
- That is allowed, if the introducer is regulated and supervised, and Calder can get the information and documents promptly.
- But ultimate responsibility never moves.
- If the introducer's checks were poor, it is still Calder that answers to the supervisor.

24 Mistakes to avoid in customer due diligence

- Verifying the company but never finding the people
- Counting only direct holdings, missing chains
- Treating CDD as a one-off at account opening
- A policy so rigid it excludes the disadvantaged
- Thinking an introducer takes the responsibility

IN THE LESSON

- Here are the traps for this outcome.
- The first is verifying the company but never finding the natural persons who own or control it.
- The second is counting only direct holdings, which misses owners like Rex who sit behind a chain of companies or a trust.
- The third is treating customer due diligence as a one off at account opening, when part four makes it ongoing for the life of the relationship.
- The fourth is the opposite of laxity: an acceptance policy so rigid that it excludes the financially or socially disadvantaged, when a basic lower risk account would serve them.
- And the fifth is thinking that relying on an introducer hands over the responsibility.
- It hands over some of the work, never the accountability.

25 A story: compliant everywhere, blind overall

- Calder East and Calder West each pass local checks
- One client deposits cash in all three entities
- Each amount is below every local alert
- Nobody sees the total: nobody looks across the group
- Lesson: manage ML/FT risk for the whole group

IN THE LESSON

- Calder has grown.
- It now owns a subsidiary abroad, Calder East, and runs a branch in another country, Calder West.
- Each passes local checks.
- Yet one client is depositing cash in all three: at home, in the east and in the west.
- Each amount sits below every local alert, so each entity sees nothing odd.
- Nobody sees the total, because nobody is looking across the group.
- This is the gap the Basel Committee targets.
- Borders split information, and launderers know it.
- A group that manages the risk entity by entity can be compliant everywhere and still blind overall.
- The lesson is that money laundering and terrorist financing risk must be managed for the whole group.

26 Managing the risk on a consolidated basis

- Parent sets group-wide AML/CFT policies
- Implemented in every branch and subsidiary
- A group-level function sees the whole risk picture
- Including customers that appear in several entities
- Share customer, account, transaction data, safely

IN THE LESSON

- Basel calls this managing the risk on a consolidated basis, meaning for the group as a single whole.
- First, the parent, Calder Bank, sets group wide A M L and C F T policies and procedures.
- Second, these are implemented in every branch and subsidiary, not just sent there.
- Third, the group has a function at group level that sees the whole risk picture, so the risk assessment covers the group and not just each piece.
- Fourth, that picture includes customers who appear in several entities, like the client in our story.
- Fifth, to make this possible, the entities share the customer, account and transaction information needed for risk management.
- They do so with safeguards, such as confidentiality and data protection.

27 Example 6: one customer, three entities

Cash deposits in one month. Each entity's alert threshold: $15,000 a month

Calder Bank, home	below $15,000	**$9,000**
Calder East, subsidiary	below $15,000	**$11,000**
Calder West, branch	below $15,000	**$12,000**
Group total	9,000 + 11,000 + 12,000	**$32,000**
Against the threshold	32,000 ÷ 15,000	**2.1 times**

IN THE LESSON

- Here are the numbers.
- Calder's rule is that cash deposits above fifteen thousand dollars in a month trigger an alert.
- The client deposits nine thousand dollars at Calder Bank at home, eleven thousand at Calder East and twelve thousand at Calder West.
- Each is below fifteen thousand, so no entity raises an alert.
- Now add them up at group level.
- Nine thousand plus eleven thousand plus twelve thousand is thirty two thousand dollars, about two point one times the threshold.
- Splitting money to stay under limits is a known laundering technique called structuring, and this group was blind to it.
- Only a group function that can see the customer across entities, using shared information, would catch it.

28 Home versus host: which rule wins?

Home: the parent's country. Host: where the branch or subsidiary operates

Situation	What the foreign entity does
Host rules less strict	Group standard, as far as host law allows
Host rules stricter	Follow the host rules
Host law blocks the standard	Extra measures; tell home supervisor

IN THE LESSON

- Home means the country of the parent and its supervisor, and host means the country where the branch or subsidiary operates.
- When the host rules are less strict than the group standard, the foreign entity applies the group standard, as far as host law allows.
- When the host rules are stricter, it follows the host rules.
- So in both cases the tougher requirement wins.
- The hard case is when host law prevents the group standard from being implemented properly, for example a law that bars sending customer information abroad.
- Then the group must apply additional measures to manage the risk, and it must inform its home supervisor.
- Doing nothing is not an option.

29 Example 7: applying the rule in three countries

Group standard: keep customer records 7 years; share alerts with the group

Host A requires 5 years	less strict: group standard	**7 years**
Host B requires 10 years	stricter: host rule	**10 years**
Host C bars data transfers	law blocks the standard	**Extra measures**
Home supervisor	about Host C	**Informed**

IN THE LESSON

- Let us apply it.
- Calder's group standard is to keep customer records for seven years and to share alerts with the group function.
- In Host A, the law requires only five years.
- That is less strict, and nothing stops Calder keeping records longer, so the entity applies the group standard of seven years.
- In Host B, the law requires ten years.
- That is stricter, so the entity follows the host rule of ten years.
- In Host C, the law bans sending customer data abroad, which blocks group sharing.
- Calder must apply extra measures there, for example limiting the products it offers there, and as a last resort closing the operation.
- And the home supervisor must be informed about Host C.
- In each country, the tougher requirement that can lawfully be applied is the one that counts.

30 Mistakes to avoid across borders

- 'The subsidiary is locally compliant, so we are fine'
- Each entity watching only its own customers
- Lowering standards to the weakest host country
- Quietly accepting a host-law block
- Rule: the strictest workable standard, applied consistently

IN THE LESSON

- The common error in this outcome is the comforting sentence at the top: the subsidiary is locally compliant, so the group is fine.
- Local compliance is necessary, but the group is judged as a whole.
- Second, letting each entity watch only its own customers, which is exactly how the client in our example slipped through.
- Third, lowering the group's standard to match the weakest host country, when the group standard should apply wherever host law allows.
- Fourth, quietly accepting a host law that blocks the standard, instead of adding measures and telling the home supervisor.
- The rule to remember for the exam is the last line: the strictest workable standard, applied consistently across the whole group.

31 Try three quick questions

1. Scores 1, 2, 3, 3 on Calder's 1-to-3 scale. Rating and measures?
   Answer: Total 9 of 12: high band (9–12). Enhanced measures.
2. Owns 10% directly, and 60% of a firm owning 30%. Threshold 25%. Owner?
   Answer: 60% × 30% = 18%; 10% + 18% = 28% > 25%. Yes.
3. Host law bars sending customer data to the group. Is local compliance enough?
   Answer: No: apply additional measures, inform home supervisor.

IN THE LESSON

- Now try three quick questions.
- Pause, think, then listen.
- Question one.
- Using Calder's scale, a customer scores one for customer type, two for product, three for channel and three for geography.
- What is its rating, and what measures follow?
- The total is nine out of twelve, which is in the high band of nine to twelve, so enhanced measures.
- Question two.
- A person owns ten per cent of a customer directly, and sixty per cent of a company that owns thirty per cent of the customer.
- With a threshold of twenty five per cent, is that person a beneficial owner?
- Sixty per cent of thirty is eighteen, plus ten makes twenty eight per cent, so yes.
- Question three.
- A subsidiary's host law bars it from sending customer data to the group.
- Is local compliance enough?
- No.
- The group must apply additional measures and inform its home supervisor.