Enterprise-Wide Risk Assessment: Methodology and Procedures

The Enterprise-Wide Risk Assessment (“EWRA”) is the foundation of the Firm’s AML program. It determines where the Firm’s money-laundering and terrorist-financing risk actually sits, how well that risk is controlled, and what the Firm proposes to do about what remains. Every downstream decision — how many investigators to fund, which scenarios to run, which thresholds to set, who gets trained on what, and what Internal Audit tests — must be traceable back to it. This document specifies the methodology, the data, the scoring, the challenge process and the calendar by which the EWRA is produced.

Document control	Detail
Document title	Enterprise-Wide Risk Assessment: Methodology and Procedures
Classification	Level 2 — Standard (issued under the Global AML Policy v9.0)
Version	5.0 (supersedes 4.2; methodology change — see § 14 for the restatement of prior-year comparatives)
Owner	Head of Financial Crimes Risk and Control
Approved by	Global Head of FCC (BSA/AML Officer); methodology validated by Model Risk Management; EWRA output approved by the Board
Assessment cadence	Annual, with a mid-year refresh of inherent-risk data; event-driven refresh on material change (§ 13)
Cycle dates	Data as at 30 June · Fieldwork July–August · Challenge September · Board approval November · Actions cascaded into the following year’s plan and budget
Assessment units	9 business lines × 4 regions × 14 legal entities = 61 reportable assessment units, aggregated to 1 enterprise view
Related documents	Global AML Policy (L1); AML Control Framework and RCM (L2); Global AML Operating Procedures (L3); Country Risk Methodology; Model Risk Management Policy; Enterprise Risk Appetite Statement

Illustrative training specimen. “Northgate Financial Group, Inc.” is a fictional institution created for instructional use. This document is modelled on the structure, register and technical content of a US Category I bank holding company financial-crime document set and is not the document of any real firm. Thresholds, cycle times and tolerances shown are representative and must not be read as regulatory minimums except where a statutory citation is given.

Contents

1. Purpose, regulatory basis and what the EWRA is for

The Firm is required to maintain an AML program that is **risk-based** and **effective**. Neither is possible without first establishing, on evidence, what the Firm's risks actually are. The EWRA is that establishment. It is the document an examiner reads first, because everything else in the program either follows from it or is unjustified.

1.1 Regulatory basis

Source	What it requires of the EWRA
31 CFR § 1020.210	A program reasonably designed to assure and monitor compliance, commensurate with the risks posed by the location, size, nature and volume of the Firm's services.
Anti-Money Laundering Act of 2020	Programs must be risk-based, must prioritise resources against the highest risks, must be **effective** rather than merely documented, and must incorporate the AML/CFT national priorities published by FinCEN.
FFIEC BSA/AML Examination Manual	A well-developed risk assessment that identifies ML/TF/OFAC risk within the specific banking operations of the institution; examiners use it to scope the examination, and will develop their own if the Firm's is inadequate.
FATF Recommendation 1	Identify, assess and understand ML/TF risks; apply a risk-based approach with enhanced measures for higher risk and simplified measures only where risk is demonstrably lower.

The examiner's first move

If the Firm's risk assessment is judged inadequate, the examiner does not simply raise a finding on the risk assessment. The examiner constructs their own view of the Firm's risk and scopes the entire examination against it — which means the Firm is then defending a control environment that was calibrated to a risk picture the examiner has rejected. Every subsequent finding compounds. A weak EWRA is not one finding; it is the reason for all of them.

1.2 What the EWRA is not

- It is not a compliance artefact produced to satisfy a requirement. If the EWRA does not change what the Firm does, it has failed, regardless of how well it is written.
- It is not a control inventory. Listing controls is not assessing whether they work.
- It is not an aggregation of business self-assessments. Businesses provide input; FCC owns the conclusion and must be willing to disagree with the business in writing.
- It is not a score. The score is a means of comparison and prioritisation. The **analysis** is the deliverable; a heat map with no narrative explaining why a cell is red is decorative.

2. Governance, ownership and the challenge process

Party	Role in the EWRA	Explicit limits
Business Risk Officer (1LOD)	Provides business data, product and client inventories, control operation evidence, and a self-assessment of inherent risk and control effectiveness for their assessment unit. Signs an attestation as to completeness and accuracy of what they submitted.	Does not set the final inherent-risk score, the control-effectiveness rating, or the residual risk. Cannot decline to submit data.
FCC Risk and Control (2LOD)	Owns the methodology, the data model, the scoring, the challenge, the conclusion and the report. Independently derives every score. Documents every point of disagreement with the business and its resolution.	May not adopt a business self-assessment without independent testing of it.
BSA/AML Officer	Approves the methodology and the final EWRA. Owns the conclusion in front of the Board and the regulator. Determines which residual risks are outside appetite.	May not be directed by any business, or by any executive, as to the score.
Model Risk Management	Validates the methodology as a model: conceptual soundness, data quality, calibration, sensitivity, outcomes analysis. Issues findings.	Does not set risk scores.
Financial Crimes Risk Committee	Reviews the draft EWRA, challenges the conclusions, approves the action plans and the owners and dates attached to them.	May not amend a score. It may require FCC to re-examine one, with reasons minuted.
Internal Audit (3LOD)	Audits the EWRA process: methodology application, data integrity, challenge evidence, and whether the outputs actually drove the program.	Does not participate in producing the EWRA.
Board of Directors	Approves the EWRA. Approves the risk appetite against which residual risk is compared. Holds management to the action plan.	—

2.1 The challenge process

Challenge is a documented, adversarial step — not a review meeting at which a presentation is noted. For every assessment unit, FCC must record: what the business asserted; what FCC independently found; where they differ; what evidence resolved the difference; and what the final position is. Where the business does not accept the final position, its dissent is recorded verbatim in the EWRA and reported to the Financial Crimes Risk Committee. An

EWRA in which the business and FCC agreed on everything is not evidence of a healthy control environment; it is evidence that challenge did not occur, and Internal Audit tests it on that basis.

3. Scope and the assessment-unit structure

Risk is assessed at the level at which it is actually managed. Assessing at too high a level averages a severe risk in a small business into invisibility; assessing at too low a level produces hundreds of units nobody reads.

3.1 The assessment unit

An assessment unit is the intersection of a **business line**, a **region** and a **legal entity**. Each unit is assessed independently and then aggregated. A unit is reportable in its own right where it exceeds any of the materiality triggers in § 3.3.

Dimension	Values
Business lines (9)	Consumer and Community Banking; Small Business Banking; Commercial Banking; Corporate and Investment Banking; Markets; Private Banking and Wealth Management; Asset Management; Payments and Treasury Services (incl. correspondent banking); Digital Assets.
Regions (4)	North America; EMEA; APAC; LATAM.
Legal entities (14)	Northgate Bank, N.A. (OCC); Northgate Securities LLC (SEC/FINRA); Northgate Trust Company, N.A.; Northgate Bank London Branch (PRA/FCA); Northgate Bank Singapore Branch (MAS); Northgate Bank Hong Kong Branch (HKMA); Northgate Bank Frankfurt GmbH (BaFin); Northgate Bank Dubai (DFSA); plus 6 further subsidiaries listed in the AML Program document.

3.2 What must be in scope, and what is frequently missed

- Every product and service, including those in run-off, those offered to a single client, and those launched mid-cycle. A product launched in August is in scope for the assessment as at 30 June only if it was live — but it must appear in the mid-year refresh and in the new-product risk assessment.
- Every channel, including branch, digital, API, agent, white-label, introduced and intermediated.
- Every legal entity, including dormant entities that hold accounts, and entities acquired during the cycle.
- Non-controlled joint ventures and minority investments — assessed for the Firm’s own exposure, even though the Policy does not directly bind them.
- Activity conducted through third parties and outsourced providers on the Firm’s behalf.
- **Discontinued and exited activity within the assessment period**, because the risk existed for part of the year and the records and reporting obligations survive the exit.

3.3 Materiality triggers for separate reporting

An assessment unit is separately reported to the Board where any of the following is true: it holds more than 2% of the Firm’s customers or revenues; it carries more than 5% of the Firm’s High-risk customers; it accounts for more than 5% of SARs filed; it conducts correspondent banking, private banking or digital-asset activity in any volume; it operates in a jurisdiction rated High; or its residual risk is High or Very High irrespective of size.

4. The methodology in one page

Step	What happens	Output
1. Define the unit	Confirm the business line / region / entity inventory against Finance and Legal Entity Control. A unit that exists in the general ledger and not in the EWRA is a scope failure.	Confirmed assessment-unit inventory
2. Score inherent risk	Score each of the five factor categories (§ 5) using the anchors in Appendix A, against the data in § 7. Weight and aggregate.	Inherent risk score 1.00–5.00 and band
3. Assess control effectiveness	Assess the design and operating effectiveness of the controls in the RCM that are mapped to the risks present in that unit, adjusted for open issues, audit and examination findings, and testing results (§ 8).	Control effectiveness rating: Strong / Satisfactory / Needs Improvement / Weak
4. Derive residual risk	Apply the residual-risk matrix (§ 9). Residual risk is **derived**, never entered. No participant may propose a residual score directly.	Residual risk band, per unit and aggregated
5. Compare to appetite	Compare residual risk to the Board-approved appetite for that unit and for the Firm (§ 10).	Within appetite / Outside appetite
6. Act	Every residual risk outside appetite requires a mitigation plan with a named owner, a date, a funding source and an interim compensating control. ‘Accept’ is available only to the BSA/AML Officer with Board notification.	Action plan; risk acceptances register
7. Trace	Demonstrate that the conclusions changed the program: resourcing, scenarios and thresholds, training, testing scope, appetite metrics (§ 12).	Traceability matrix

Residual risk is derived, not negotiated

The single most common way a risk assessment is corrupted is that someone decides the answer first — usually ‘Medium’, because Medium requires no action — and then reasons backwards to inherent and control scores that produce it. The methodology prevents this structurally: residual is a formula output, the inherent score is anchored to observable data, and the control rating is anchored to testing evidence and open issues. Anyone proposing a residual score directly has misunderstood the exercise, and the submission is rejected.

5. Inherent risk: the five factor categories

Inherent risk is the risk that exists **before any control is considered**. It is a function of what the business does, for whom, where, and how — not of how well it is managed. Analysts must resist the near-universal instinct to reduce an inherent score because "we have a good control for that". That is what the control-effectiveness step is for, and conflating the two is the second most common EWRA failure.

Category	Weight	What is assessed
1. Customers and entities	25%	Volume and proportion of higher-risk customer types: PEPs and their associates; cash-intensive businesses; money services businesses; virtual-asset service providers; non-resident and non-face-to-face customers; complex or offshore structures; trusts and foundations; charities and NPOs; embassies and foreign missions; correspondent respondents; gatekeepers (lawyers, accountants, company formation agents); politically or reputationally sensitive names; customers previously exited by the Firm or by peers.
2. Products and services	20%	Products that permit anonymity, rapid movement, cross-border reach, third-party funding or value transfer outside the banking system: cash; international wires; correspondent and payable-through accounts; trade finance; private banking; custody and omnibus accounts; prepaid and stored value; virtual assets; pooled investment vehicles; trade and pre-paid cards; cheque cashing; remote deposit capture.
3. Geographies	20%	Countries of incorporation, operation, beneficial ownership, counterparty and payment corridor. Scored against the FCC Country Risk List, which is built from FATF listings, sanctions exposure, corruption and secrecy indices, narcotics and trafficking exposure, conflict and terrorism exposure, and Northgate's own SAR and exit experience. Both **where the customer is** and **where the money goes** are scored; a domestic customer paying exclusively into a high-risk corridor is not a domestic risk.
4. Delivery channels	15%	Face-to-face; digital non-face-to-face; introduced by an agent, broker or intermediary; white-labelled; API and embedded finance; third-party onboarding; correspondent (i.e. the customer of a customer).
5. Transactions and activity	20%	Actual observed activity: cash volume and value; wire volume, value and corridors; cross-border proportion; third-party payment proportion; velocity; alert volume; alert-to-SAR conversion; SAR volume and typology mix; law-enforcement enquiry and subpoena volume; 314(a) match volume; exits for financial-crime cause.

> **Transactions are inherent risk, not control performance**
>
> SAR volume, alert volume and subpoena volume appear in the inherent-risk score because they measure the criminal attention the business attracts — not how well the Firm responds to it. A business that files many SARs is not thereby lower risk; it is demonstrating that it is exposed. It may simultaneously have strong controls. The two questions are answered separately, and they are combined only in § 9.

6. Inherent risk: scoring anchors and weighting

6.1 The 1–5 scale

Score	Band	Meaning
1	Low	The risk factor is effectively absent, or present at a volume that could not material affect the Firm.
2	Low-Moderate	Present but limited; well within the ordinary experience of a US commercial bank.
3	Moderate	Materially present. This is the default for a mainstream banking activity and must be justified like any other score, not used as a resting place.

Score	Band	Meaning
4	High	Present at volume, or present in a form known to be actively exploited for laundering.
5	Very High	Concentrated exposure to a factor that features prominently in enforcement actions, FATF listings or the national priorities.

Every score must cite the data that produced it (§ 7). A score without a data citation is rejected in challenge. Scoring anchors — the observable thresholds that map data to a 1–5 score for each individual risk factor — are in Appendix A and are binding.

6.2 Aggregation

Within a category, individual factor scores are aggregated as a weighted mean, with the factor weights set in Appendix A. Category scores are then aggregated to a unit inherent-risk score using the category weights in § 5.

- **Override rule (upward only).** Where any individual factor scores 5 and represents concentrated exposure, the unit inherent score is floored at 4.0 regardless of the weighted mean. Averaging must never allow one severe exposure to be diluted by a large volume of benign business. This is the single most important arithmetic rule in the methodology.
- **No downward override exists.** There is no mechanism to reduce an inherent score below the anchored data.
- **Volume and severity are both scored.** A single correspondent respondent in a jurisdiction under a FATF call for action is a 5. Ten thousand low-value retail current accounts are not.

6.3 Bands

Inherent score	Band
1.00 – 1.79	Low
1.80 – 2.59	Low-Moderate
2.60 – 3.39	Moderate
3.40 – 4.19	High
4.20 – 5.00	Very High

7. Data: the EWRA data dictionary and evidence standard

The EWRA is only as good as the data beneath it. Every metric below is extracted centrally by FCC Risk and Control from the systems of record on a fixed as-at date. Businesses do not supply their own numbers for these fields; they may challenge them, with evidence.

Metric	Source system	Basis
Customer count by risk band (Low / Medium / High / PEP)	NG-KYC	Point-in-time at 30 June
Count of customers by higher-risk type (MSB, VASP, cash-intensive, NPO, embassy, gatekeeper, trust, correspondent)	NG-KYC customer-type taxonomy	Point-in-time

Metric	Source system	Basis
Count and value of customers with beneficial ownership in a High-rated country	NG-KYC	Point-in-time
Cash volume and value, in and out	Core banking / branch teller	12 months to 30 June
Wire volume and value, by corridor and currency	Payments hub	12 months
Proportion of payments to or from High-rated countries	Payments hub	12 months
Correspondent respondent count; nesting indicators identified	NG-KYC / Payments hub	12 months
Trade finance transaction count and value; dual-use goods flags	Trade platform	12 months
Digital-asset transaction count and value; VASP counterparty exposure	Digital asset ledger	12 months
Alert volume; alerts per 1,000 customers; alert-to-SAR conversion	NG-DETECT / NG-CASE	12 months
SAR volume; SARs per 1,000 customers; typology mix; continuing-activity proportion	NG-FILE	12 months
CTR volume	NG-FILE	12 months
314(a) matches; subpoenas; law-enforcement enquiries; NSLs	FCC Advisory register	12 months
Exits for financial-crime cause; declined onboardings	NG-KYC / FCC register	12 months
Open AML issues by severity; overdue issues; open audit and examination findings	NG-GRC	Point-in-time
2LOD control testing results; QA error rates by grade	NG-GRC / QA	12 months
Data quality: CDE error rates; feed completeness exceptions	NG-GRC / Data Office	12 months
Training completion and assessment pass rates	Learning system	12 months
Staffing: FTE per 1,000 alerts; vacancy rate; tenure; attrition in FCC	HR / FCC Ops	Point-in-time and 12-month average

7.1 Evidence standard

- Every number in the EWRA must be reproducible from a dated, retained extract. The extract, the query, and the extraction date are stored with the working papers.
- Where a number cannot be produced from a system, it is recorded as **not available**, not estimated. A gap in data is itself a finding, and it must be raised as an issue with an owner and a date — because a risk the Firm cannot measure is a risk the Firm cannot manage.
- Manual adjustments to system data require documented rationale and approval by the Head of FC Risk and Control. Unexplained adjustments are the mechanism by which risk assessments are quietly manipulated, and they are specifically tested by Internal Audit.
- Prior-year figures are restated only where the methodology changed (§ 14), and the restatement is disclosed.

8. Control effectiveness: how it is assessed

Control effectiveness is not an opinion, and it is not the business's self-assessment. It is derived from evidence already held elsewhere in the framework — principally the RCM, the testing results and the issue register.

8.1 Inputs, in order of weight

Input	Weight	Notes
Design effectiveness of the mapped controls	25%	Are the controls in the RCM that are mapped to the risks present in this unit sufficient, in design, to mitigate them? A risk present in the unit with no Key Control mapped to it caps the rating at **Weak**, irrespective of everything else.
Operating effectiveness — 2LOD (CTM) testing results	25%	Re-performance results for the period. A Key Control tested **not effective** caps the rating at **Needs Improvement**.
Open issues, weighted by severity and age	20%	An open Critical issue caps the rating at **Weak**. Open High issues past their due date cap it at **Needs Improvement**.
Internal Audit and regulatory examination findings	15%	An open Matter Requiring Attention or equivalent supervisory finding relevant to the unit caps the rating at **Needs Improvement** until validated as closed.
QA results and operational performance	10%	QA Critical error rates; SLA attainment; backlog; overdue reviews; late filings. A single late statutory filing in the period is escalated in the narrative even if the rate is low.
Data quality and system coverage	5%	A known monitoring or screening coverage gap affecting the unit caps the rating at **Weak** for the period of the gap.

8.2 The rating scale

Rating	Definition	Effect on residual risk
Strong	Controls are well designed, tested effective with no exceptions, no open High or Critical issues, no coverage gaps, and the unit self-identifies its own issues.	Reduces inherent risk by up to two bands
Satisfactory	Controls are well designed and generally operating, with isolated, non-systemic exceptions that are being remediated on time.	Reduces inherent risk by one band
Needs Improvement	One or more Key Controls are not operating effectively; or issues are overdue; or a supervisory finding is open.	No reduction — residual equals inherent
Weak	A risk present in the unit has no control mapped to it; or a Key Control is absent, not designed, or not operating; or a Critical issue is open; or there is a coverage gap.	**Increases** residual risk by one band above inherent

Why a Weak rating pushes residual above inherent

Because an uncontrolled risk in a firm that believes it is controlled is worse than the same risk in a firm that knows it is not. A Weak rating means the Firm is exposed **and** the exposure was not visible to the people relying on the control. That is the condition in which the largest enforcement actions in this industry were incurred. The methodology reflects it arithmetically so that no one has to argue for it in a meeting.

9. Residual risk: derivation and the heat map

Residual risk = inherent risk, adjusted by control effectiveness, per the matrix below. It is computed by the model. It is never entered by hand, and there is no field in which to enter it.

Inherent ↓ / Control →	Strong	Satisfactory	Needs Improvement	Weak
Very High (5)	Moderate	High	Very High	Very High
High (4)	Low-Moderate	Moderate	High	Very High
Moderate (3)	Low	Low-Moderate	Moderate	High
Low-Moderate (2)	Low	Low	Low-Moderate	Moderate
Low (1)	Low	Low	Low	Low-Moderate

Note that a Very High inherent risk cannot be controlled down to Low. A business whose inherent risk is Very High is a business the Firm has chosen to be in, and no control environment makes that choice risk-free. The methodology refuses to pretend otherwise; the floor is Moderate. If Moderate residual risk in that activity is unacceptable to the Board, the answer is not a better control — it is to reduce or exit the activity.

9.1 Aggregation to the enterprise view

- Unit residual risks are aggregated to business line, region, legal entity and enterprise using exposure weights (customer count, revenue, transaction value — whichever is the most risk-relevant driver for that dimension, stated explicitly).
- **The enterprise residual risk is never below the highest legal-entity residual risk.** A regulated entity with High residual risk is not averaged away by the size of the group; its regulator does not supervise the group's average.
- Concentrations are reported separately from averages. A heat map showing an amber enterprise position while three units are red is a misleading heat map, and the narrative must say so on the same page.

10. Comparison to risk appetite and the action plan

The Board approves an ML/TF risk appetite as part of the Enterprise Risk Appetite Statement. The EWRA compares residual risk to that appetite, per unit and in aggregate.

Outcome	Required response
Residual risk within appetite	No action beyond continued monitoring. The unit is not thereby exempt from control testing.
Residual risk outside appetite	A mitigation plan is **mandatory**. It must state: the specific control or capability gap; the action; the named individual owner; the target residual position; the completion date; the funding source and whether it is in the approved budget; and the **interim compensating control** that operates until the plan lands. A plan without a compensating control leaves the Firm exposed for the duration of the plan, and that exposure must be stated to the Board explicitly.
Risk acceptance proposed	Available only where mitigation is not feasible or not proportionate. Requires BSA/AML Officer approval, a stated expiry date (never open-ended), Financial Crimes Risk Committee review and Board notification. Recorded in the Risk Acceptance Register and re-approved annually on its merits. An acceptance may not be rolled forward administratively.
Residual risk Very High	The activity is presented to the Board with an explicit recommendation: reduce, restrict, or exit. 'Continue and monitor' is not an available recommendation for a Very High residual position.

11. Incorporating the national AML/CFT priorities

The AML Act of 2020 requires the Firm to incorporate the AML/CFT national priorities published by FinCEN into its risk-based program. Incorporation means the priorities appear in the assessment, in the detection scenarios, in the training and in the testing — not that they are listed in an appendix.

For each published priority, the EWRA must state, on the record and by name: the Firm's exposure to it; the specific typologies through which it would manifest in the Firm's products; the detection scenarios in NG-DETECT mapped to those typologies; the SARs filed in the period against that priority; the training delivered; and the testing performed. Where the Firm assesses its exposure to a priority as immaterial, it must say so and evidence why — silence is not an assessment.

Priority area (as published)	Required EWRA treatment
Corruption	PEP population and concentration; private banking exposure; source-of-wealth corroboration failures; jurisdictions with elevated corruption exposure; detection scenarios for proceeds of foreign corruption.
Cybercrime, including virtual-asset exploitation	VASP counterparty exposure; mixer and tumbler exposure; ransomware payment typologies; business email compromise mule accounts.
Terrorist financing	Screening coverage; NPO and charity exposure in conflict zones; low-value high-frequency typologies; hawala and informal value transfer exposure.
Fraud	The predicate offence generating the largest share of the Firm's SARs; elder-fraud and mule-account typologies; the AML/fraud data-sharing interface.
Transnational criminal organisations	Trade-based laundering; funnel accounts; cash-intensive business exposure; front-company typologies.
Drug trafficking	Bulk cash; structuring; trade-based laundering; professional money laundering networks.
Human trafficking and human smuggling	Third-party cash deposits across disparate geographies; shared address and device indicators; the specific detection scenario and its performance.
Proliferation financing	Dual-use goods exposure; sanctions-evasion typologies; front and shell company procurement networks; the sanctions interface.

12. Using the EWRA: the traceability requirement

The EWRA is not complete when the report is approved. It is complete when the Firm can demonstrate that the report changed what the Firm does. FCC maintains a **traceability matrix**, tested by Internal Audit, showing for every material conclusion what changed as a result.

EWRA conclusion drives...	Evidence of use
Resourcing and budget	FCC headcount and budget submission for the following year, mapped line by line to the units with the highest residual risk. A conclusion that a unit is High residual, accompanied by no change in resourcing, must be explained.
Detection scenarios and thresholds	Scenario coverage mapped to the typologies identified; tuning of thresholds in the units identified as High; new scenarios built for newly identified typologies.
Customer due diligence calibration	Changes to the risk-rating model weights; changes to EDD triggers; changes to the Restricted Business Schedule; changes to the Country Risk List.

EWRA conclusion drives...	Evidence of use
Training	The following year's training curriculum, with role-specific modules built against the highest-residual units and the national priorities.
Independent testing scope	The 2LOD testing plan and the Internal Audit plan for the following year, risk-ranked against the EWRA output.
Risk appetite	Proposed changes to appetite metrics and thresholds presented to the Board alongside the EWRA.
Business strategy	Where residual risk in an activity is Very High, the recommendation to the Board on whether to continue in that activity.

The question that closes the loop

At the next examination, the Firm will be asked: "You concluded last year that correspondent banking in EMEA was your highest residual risk. What did you do differently?" The traceability matrix is the answer to that question. If the answer is that nothing changed, the EWRA was a document, not an assessment — and the Firm will be found to have an ineffective program, notwithstanding the quality of the report.

13. Refresh triggers and event-driven reassessment

The EWRA is refreshed annually as a minimum. It must be refreshed — in whole or for the affected units — on any of the following, without waiting for the cycle:

- A material acquisition, disposal, or entry into a new jurisdiction, business line or product.
- A material change to the customer base, such as the onboarding of a portfolio or a new distribution channel.
- A significant regulatory or enforcement development, including a change in the national priorities, a new FATF listing affecting a material corridor, or a new special measure.
- The identification of a material control failure, monitoring coverage gap, or the commencement of a lookback.
- A material adverse examination finding or supervisory action.
- A significant change in the Firm's own SAR, alert or law-enforcement enquiry experience — in either direction. A sharp **fall** in alerts or filings is as much a trigger as a sharp rise, and is more often a control failure than a genuine reduction in risk.

14. Methodology change, validation and prior-year comparability

- The methodology is a **model** and is governed as one. It is independently validated by Model Risk Management: conceptual soundness; appropriateness of factors and weights; data quality; sensitivity analysis (how much does the output move if a weight moves?); benchmarking; and outcomes analysis (did units rated Low residual subsequently produce the enforcement events, lookbacks, and audit findings that a Low rating implies they should not?).
- Any change to factors, weights, anchors or the residual matrix requires FCC approval, Model Risk validation, and disclosure in the EWRA report.
- Where the methodology changes, prior-year results are **restated** on the new basis and presented alongside the new results. Presenting a year-on-year improvement that is in fact a methodology change is a misrepresentation to the Board and is treated as such.

- Sensitivity analysis is mandatory and must be reported: the report must state which conclusions would change if the weights moved within a plausible range. A conclusion that is robust only at one exact set of weights is not a conclusion.

15. The EWRA report: mandatory contents

Section	Must contain
Executive summary	The Firm's residual ML/TF risk position; the material changes since the prior year and why; the risks outside appetite; the actions proposed; and the BSA/AML Officer's own opinion on program effectiveness, stated plainly.
Methodology and any change to it	Including restated comparatives and sensitivity analysis.
Scope and assessment units	Including any exclusions, with justification.
Inherent risk	By category and by unit, with the data that produced each score.
National priorities	Exposure, typologies, detection, training and testing, priority by priority.
Control effectiveness	By unit, with the testing evidence, open issues, audit and examination findings that drove each rating.
Residual risk	The heat map, the concentrations, and the narrative explaining every High and Very High cell.
Appetite comparison	What is outside appetite, by how much, and for how long it has been.
Action plans	Owners, dates, funding, interim compensating controls.
Risk acceptances	Every acceptance, its expiry, and its re-approval status.
Data gaps	Every metric the Firm could not produce, and the plan to produce it.
Business dissent	Recorded verbatim, where the business does not accept FCC's conclusion.
Traceability	What changed in the program as a result of the prior year's EWRA.

16. Calendar and RACI

Week	Activity	R	A	C	I
W1–W2 (July)	Confirm assessment-unit inventory against Finance and Legal Entity Control; publish the data-request pack and the as-at date.	FCC R&C;	Head FC R&C;	Finance; LEC	Business Risk Officers
W3–W5	Central data extraction; data quality validation; publication of the inherent-risk data pack to each unit.	FCC R&C;	Head FC R&C;	Data Office; FC Technology	Business
W6–W8	Business self-assessment submissions and attestations; control evidence collation.	Business Risk Officers	Business Heads	FCC R&C;	—
W9–W11 (Aug)	FCC independent scoring of inherent risk and control effectiveness; derivation of residual risk.	FCC R&C;	Head FC R&C;	CTM; Internal Audit (observer)	Business
W12–W13 (Sept)	Challenge sessions with each business; documented resolution of differences; recording of dissent.	FCC R&C;	BSA/AML Officer	Business Heads	Op Risk

Week	Activity	R	A	C	I
W14	Action plans agreed with owners, dates, funding and compensating controls.	Business Heads	BSA/AML Officer	FCC R&C;	Finance
W15 (30 Sept)	Draft EWRA to the Financial Crimes Risk Committee; challenge and approval of action plans.	FCC R&C;	BSA/AML Officer	FCRC members	Internal Audit
Oct	Model Risk validation sign-off; Internal Audit review of the process.	Model Risk	Head Model Risk	FCC R&C;	Audit Committee
Nov	EWRA to the Board Risk Committee, then to the Board for approval.	BSA/AML Officer	Board	CCO; CRO	All
Dec–Jan	Cascade into the following year’s budget, testing plan, audit plan, training curriculum and tuning schedule; traceability matrix updated.	FCC R&C;	BSA/AML Officer	Business; Internal Audit; Finance	Board

Appendix A — Risk factor library with scoring anchors

Extract. The full library contains 47 factors. Anchors are binding: an analyst who scores outside the anchor for the observed data must justify the departure in writing and it is reviewed in challenge.

Factor	Score 1	Score 3	Score 5
PEPs as a % of the unit's customer base	None	0.5–2%	> 5%, or any senior foreign political figure in private banking
Foreign correspondent respondents	None	1–10 respondents, all in low-risk jurisdictions	Any respondent in a FATF call-for-action jurisdiction, or any respondent permitting nesting
Cash volume as a % of total transaction value	< 0.5%	2–5%	> 10%
Customers in the highest-rated countries (FCC Country Risk List)	None	1–5% of the base	> 10% of the base
Cross-border payment value as a % of total	< 5%	20–40%	> 60%
MSB and VASP customers	None	Fewer than 10, all with evidenced AML programs	Any VASP without an evidenced AML program, or any exposure to anonymity-enhancing assets
Non-face-to-face onboarding proportion	< 10%, all with liveness verification	40–70%	> 90%, or any onboarding via a third party without look-through
Complex or offshore ownership structures	None	Present, all resolved to natural persons	Present, with structures the Firm could not fully resolve at onboarding
SARs per 1,000 customers, relative to peer businesses	Materially below peer with a credible explanation	In line with peer	Materially above peer — **or materially below peer with no credible explanation**
Trade finance with dual-use or sanctions-sensitive goods	None	Present, all screened and reviewed	Present in a corridor with known proliferation-financing exposure
Open Critical AML issues affecting the unit	None	—	Any (this factor also caps control effectiveness at Weak)

> **The most counter-intuitive anchor in the library**
>
> A SAR rate **materially below** peer scores 5, not 1. A business that attracts criminal money and reports none of it is not low risk — it is blind. Low filing volume is treated as a red flag against the control environment and as an inherent-risk indicator that the Firm does not understand its own book, until the business evidences a credible structural reason for it.

Appendix B — Worked example: one assessment unit

Unit: Payments and Treasury Services (correspondent banking) — EMEA — Northgate Bank London Branch.

Inherent category	Weight	Score	Evidence
Customers and entities	25%	5	38 foreign correspondent respondents; 4 in jurisdictions rated High; 2 with identified nesting exposure. Concentration triggers the § 6.2 floor.
Products and services	20%	5	Correspondent accounts; USD clearing; cover payments (MT202COV); trade finance settlement.
Geographies	20%	4	62% of payment value in cross-border corridors; 9% of value to or from High-rated countries.
Delivery channels	15%	4	The customer is a bank; the underlying parties are the customers of a customer, with no direct look-through.
Transactions and activity	20%	4	112 SARs filed (18% of the Firm's total, on 0.1% of customers); 6 subpoenas; 3 314(a) matches; alert-to-SAR conversion materially above the Firm average.

Weighted inherent score: (5×0.25) + (5×0.20) + (4×0.20) + (4×0.15) + (4×0.20) = **4.45 — Very High.**

Control effectiveness: Design assessed as sufficient (AML-CDD-009, 010; AML-TMS-001, 002). However, CTM testing found AML-CDD-010 (monthly actual-vs-expected respondent activity review) operating with exceptions in 3 of 5 months tested, and one High issue on nesting identification is 40 days past due. Result: **Needs Improvement** (capped by the overdue High issue and the Key Control exception).

Residual risk: Very High inherent × Needs Improvement = **Very High.** Outside appetite.

Required response (§ 10): Because the residual position is Very High, ‘continue and monitor’ is not available. The unit is presented to the Board with a recommendation to (a) suspend new respondent onboarding in the two nesting-exposed relationships pending remediation; (b) implement a daily, rather than monthly, actual-vs-expected review as an interim compensating control, resourced from within the existing team by deferring lower-risk work, with the deferral itself disclosed to the Board; (c) exit the two respondents unable to identify their downstream institutions; and (d) close the nesting issue within 60 days with independent validation.

> **Read the example again**
>
> Note what did **not** happen. The unit did not argue that its strong controls should reduce the inherent score. The Very High inherent score was not softened because the business is profitable and strategically important — which, in a real bank, it invariably is. The overdue issue capped the control rating arithmetically, without anyone having to win that argument in a meeting. And the interim compensating control was resourced by **stopping something else**, and that trade-off was disclosed rather than absorbed silently. This is what a functioning EWRA looks like in practice.

Appendix C — Common EWRA failures and how they are examined

Failure	How an examiner detects it
Inherent risk scored net of controls	Compare the inherent score to the raw data. A business with 38 correspondent respondents scoring Moderate inherent risk has scored net of controls, whatever the narrative says.
Everything is Moderate	A distribution of scores clustered on 3 with almost no 1s, 4s or 5s indicates scoring to avoid consequences, not scoring to measure risk.
No evidence of challenge	Request the challenge log. If the business self-assessment and the final score are identical across every unit, 2LOD did not challenge.

Failure	How an examiner detects it
The EWRA did not change anything	Compare the prior-year conclusions to the current-year budget, testing plan, audit plan and tuning schedule. This is the traceability test, and it is the one most firms fail.
Data not reproducible	Ask for the extract behind a number. If it cannot be produced, or if it was manually adjusted without documented rationale, every number in the assessment is now in question.
Coverage gaps not reflected	Compare the monitoring coverage matrix to the EWRA. A known gap that does not depress the control rating for the affected unit means the EWRA is not reading the Firm's own control information.
National priorities listed but not assessed	Search the document for each priority. If it appears only in a list, with no exposure analysis, no typologies and no scenario mapping, the statutory requirement is not met.
Prior-year comparatives not restated after a methodology change	Compare the methodology sections year on year. An unexplained improvement following a methodology change is treated as a governance failure, not an achievement.

Approval

Methodology approved by the Global Head of Financial Crimes Compliance (BSA/AML Officer) on 9 April 2026; validated by Model Risk Management (validation reference MRM-2026-0417); noted by the Financial Crimes Risk Committee on 16 April 2026. The EWRA output produced under this methodology is approved annually by the Board of Directors.

— End of Methodology —