AML Control Framework and Risk-Control Matrix

This Standard defines the population of AML controls the Firm relies on, what each control must achieve, who operates it, what evidence it produces, how it is tested, and what happens when it fails. It is the bridge between the Global AML Policy (which states what must be true) and the Global AML Operating Procedures (which state how the work is done). A control that is not in this framework is not relied upon; a control that is relied upon and not in this framework is a control-inventory failure.

Document control	Detail
Document title	AML Control Framework and Risk-Control Matrix
Classification	Level 2 — Standard (issued under the Global AML Policy v9.0)
Version	4.1 (supersedes 4.0, effective 1 November 2025)
Owner	Head of Financial Crimes Risk and Control
Approved by	Global Head of Financial Crimes Compliance (BSA/AML Officer); noted by the Financial Crimes Risk Committee
Effective date	1 May 2026
Review cycle	Annual; and on any change to the Policy, the enterprise risk assessment, the control environment, or the supporting systems
Control population	68 controls in the AML domain, of which 24 are designated Key Controls. Sanctions controls (SAN-*) and fraud controls (FRD-*) are governed by their own frameworks and are cross-referenced only.
Testing owners	1LOD self-testing (Control Owners); 2LOD Compliance Testing and Monitoring (CTM); 3LOD Internal Audit

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, scope and control philosophy	1
2.	Control taxonomy and naming convention	2
3.	Risk taxonomy and the risk-to-control mapping	3
4.	Control design standard: what a control must specify	4
5.	The Risk-Control Matrix (RCM)	5
6.	Key Control detail sheets	10
7.	Screening control specification	13
8.	Transaction monitoring: coverage, tuning and model governance	13
9.	Data quality controls and system coverage	15
10.	Key Risk Indicators and Key Performance Indicators	15
11.	Control testing methodology and sample sizes	16
12.	Issue management and remediation	17
13.	Control attestation and change governance	18
A.	Appendix A — Control test sample-size table	19
B.	Appendix B — Control failure severity definitions	19

1. Purpose, scope and control philosophy

The Firm does not manage money-laundering risk by having procedures. It manages it by operating controls that work, producing evidence that they worked, and testing that evidence independently. This Standard exists so that every control the Firm relies on is: **identified**, **owned** by a named individual, **designed** to mitigate a named risk, **operated** at a defined frequency, **evidenced** in a way that can be re-performed, and **tested** on a defined cycle.

1.1 Four principles

- **A control without evidence is not a control.** If the operation of a control cannot be re-performed from the artefacts it produces, the Firm cannot demonstrate it worked, and an examiner will treat it as if it did not.
- **A control without an owner is not a control.** Ownership is individual and named. “The team” owns nothing.
- **Design effectiveness and operating effectiveness are different questions.** A well-designed control operated badly and a badly designed control operated diligently both fail. Testing asks both questions separately.
- **Preventive beats detective.** Where a preventive control is feasible and proportionate, the Firm implements it in preference to detecting the failure afterwards. Detective controls that repeatedly detect the same failure indicate a missing preventive control, and are escalated as such rather than resourced indefinitely.

1.2 Scope

This Standard covers all controls that mitigate money-laundering and terrorist-financing risk across all in-scope legal entities, businesses, products and channels. Sanctions screening and blocking controls are specified in the Sanctions Control Framework; the interfaces are identified here (Section 7) but the controls are not duplicated. Fraud, anti-bribery and tax-evasion-facilitation controls are similarly cross-referenced only.

2. Control taxonomy and naming convention

2.1 Control identifier

Every control carries a permanent identifier of the form **AML-[DOMAIN]-[NNN]**. Identifiers are never reused, never renumbered and never retired silently; a withdrawn control is marked WITHDRAWN with a date and a reason, and the risk it mitigated must be re-mapped to another control or accepted through the exception process.

Domain code	Coverage
AML-CIP-nnn	Customer identification program
AML-UBO-nnn	Beneficial ownership identification and verification
AML-CDD-nnn	KYC profile, risk rating, EDD, periodic review
AML-SCR-nnn	PEP and adverse-media screening (sanctions screening: SAN-* framework)
AML-TMS-nnn	Transaction monitoring, alert handling, investigation
AML-RPT-nnn	Regulatory reporting — SAR, CTR, 314(a), 314(b)
AML-REC-nnn	Recordkeeping, funds transfer records, retention, legal hold
AML-DAT-nnn	Data completeness, accuracy, timeliness, lineage and coverage
AML-GOV-nnn	Governance, risk assessment, training, MI, model governance, third parties

2.2 Control attributes

Attribute	Permitted values	Meaning
Nature	Preventive / Detective / Corrective	Preventive stops the event. Detective identifies it after the fact. Corrective restores the position and prevents recurrence.
Execution	Automated / Manual / Hybrid (IT-dependent manual)	A hybrid control is a human decision made on a system-generated input — the most common and most fragile category, because it fails if either the system or the human fails. Testing a hybrid control must test both halves.
Designation	Key / Non-key	A Key Control is one whose failure would, alone, result in a material regulatory breach, a missed or late statutory filing, an undetected suspicion, or a prohibited relationship being onboarded. Key Controls are tested at least annually by 2LOD and are in permanent scope for 3LOD.
Frequency	Continuous / Real-time / Daily / Weekly / Monthly / Quarterly / Annual / Event-driven	The frequency at which the control operates — not the frequency at which it is tested.
Precision	High / Medium / Low	How narrowly the control would detect an error of the size that matters. A monthly review of aggregate volumes is a low-precision control and cannot be relied on alone to detect a single missed filing.

Why precision matters

A common examination finding is that a bank claims to rely on a management review to catch an error the review could never have seen. If a control is described as detecting “errors in SAR filings” but consists of a monthly look at a count of filings, it cannot detect a wrong narrative, a missed subject, or a late clock start. State what the control can actually see, and map the residual gap to another control or accept it explicitly.

3. Risk taxonomy and the risk-to-control mapping

Every control must be traceable to a Level 2 risk in the Firm’s financial-crime risk taxonomy, and every Level 2 risk must have at least one Key Control mapped to it. An unmapped risk is an accepted risk, and acceptance requires BSA/AML Officer approval and reporting to the Financial Crimes Risk Committee.

L1 risk	L2 risk	Primary controls
Onboarding risk	R1.1 The Firm onboards a customer whose identity it has not established	AML-CIP-001, 002, 004
	R1.2 The Firm onboards a legal entity without knowing who ultimately owns or controls it	AML-UBO-001, 002, 003
	R1.3 The Firm assigns a risk rating that understates the true risk	AML-CDD-002, 003, 010
	R1.4 The Firm onboards a customer in a prohibited or restricted category without the required approval	AML-CDD-005, 006
Screening risk	R2.1 A PEP is not identified at onboarding or on promotion	AML-SCR-001, 003
	R2.2 A screening match is cleared without adequate justification	AML-SCR-004, 005
	R2.3 The screening engine does not cover a population, a list, or a data field	AML-SCR-002, AML-DAT-004
Detection risk	R3.1 Suspicious activity occurs and no alert is generated	AML-TMS-001, 002, AML-DAT-001
	R3.2 An alert is generated and closed without adequate investigation	AML-TMS-004, 005, 009
	R3.3 Alert backlog causes the statutory filing clock to be missed	AML-TMS-006, 007
Reporting risk	R4.1 A SAR that should be filed is not filed	AML-RPT-001, 002, 003
	R4.2 A SAR is filed late, or the initial detection date is recorded incorrectly	AML-RPT-002, 004
	R4.3 A CTR is missed, late, or inaccurate	AML-RPT-006, 007
	R4.4 A 314(a) search is incomplete or late	AML-RPT-008
Confidentiality risk	R5.1 A customer or unauthorised person is tipped off	AML-RPT-005, AML-GOV-006
Records risk	R6.1 A required record is not retained, or is destroyed under hold	AML-REC-001, 002, 005
	R6.2 Funds-transfer records or travel-rule data are incomplete	AML-REC-003, 004
Data and model risk	R7.1 A source system is not fed to monitoring or screening (coverage gap)	AML-DAT-004, 005
	R7.2 Data fed to monitoring is incomplete, inaccurate or late	AML-DAT-001, 002, 003
	R7.3 Thresholds or scenarios are mis-calibrated and suppress detection	AML-GOV-008, 009, 010

L1 risk	L2 risk	Primary controls
Governance risk	R8.1 The risk assessment does not reflect the actual business	AML-GOV-001
	R8.2 Staff are untrained, or trained without comprehension	AML-GOV-004, 005
	R8.3 A third party performs an AML activity without oversight	AML-GOV-011

4. Control design standard: what a control must specify

A control entry that omits any of the following is incomplete and must not be relied upon in the risk assessment or presented as mitigation to a regulator.

Field	Standard	A failing example
Control objective	The single thing the control must achieve, stated as an outcome.	“Ensure compliance with BSA.” Too broad to test.
Control description	Who does what, to what population, at what frequency, using what input, applying what criterion, producing what output, and what happens on exception.	“Alerts are reviewed.” By whom? All of them? Against what standard?
Owner	A named individual and role, accountable for operation and evidence.	“KYC Operations.”
Population and completeness	How the operator knows the population is complete.	A control operated on a report whose completeness is never checked is a control over an unknown subset.
Criterion	The objective test applied — the threshold, the rule, the checklist.	“Analyst judgement.” Judgement is permitted; an unarticulated criterion is not.
Evidence	The artefact produced, where it is stored, and for how long.	“The analyst reviews it in the system.” No artefact, no control.
Exception handling	What happens when the control identifies a failure.	A control with no defined exception path detects nothing that anyone acts on.
Failure modes	The specific ways this control is known to break.	Stating failure modes is not an admission of weakness; it is the basis of the test plan.

5. The Risk-Control Matrix (RCM)

The RCM below is the authoritative control inventory. **K** denotes a Key Control. N = Nature (P preventive, D detective, C corrective); X = Execution (A automated, M manual, H hybrid).

ID	Control	K	N	X	Freq.	Owner	Evidence
AML-CIP-001	NG-KYC blocks account activation in the core banking system until CIP status = PASS or an approved deferral is flagged. No manual override exists.	K	P	A	Real-time	Head, KYC Ops	System control configuration; monthly exception report of accounts activated without PASS (target: zero)
AML-CIP-002	Four-eyes review of every CIP record before approval; preparer and reviewer recorded separately and cannot be the same user ID.	K	P	H	Per case	Head, KYC Ops	NG-KYC audit trail with both user IDs and timestamps
AML-CIP-003	Daily exception report of accounts open beyond 25 days with CIP incomplete; escalated to FCC at day 25, restricted at day 30.		D	H	Daily	Head, KYC Ops	Dated exception report with disposition and restriction confirmations
AML-CIP-004	Automated restriction of any account reaching day 30 with CIP incomplete (outbound block applied by the system, not by request).	K	P	A	Real-time	Head, KYC Ops	System restriction log; reconciliation to the day-30 population
AML-UBO-001	NG-KYC prevents approval of a legal entity customer where no control-prong individual is named and verified.	K	P	A	Real-time	Head, KYC Ops	Configuration evidence; nil-exception report
AML-UBO-002	Ownership chart obtained, certified within 12 months, and resolved to natural persons at the applicable threshold (25%, or 10% for High risk / high-risk jurisdictions / private banking).	K	P	H	Per case	Head, KYC Ops	Certified chart; look-through calculation worksheet in NG-KYC
AML-UBO-003	Beneficial-ownership certification re-affirmed on every new account and on every trigger event; system prompts and blocks on expiry.		P	H	Event	Head, KYC Ops	Certification records with version history
AML-CDD-001	KYC profile completeness check: mandatory fields (nature, purpose, expected activity, SOF, and SOW where required) cannot be left blank or populated with prohibited placeholder values.		P	A	Real-time	Head, KYC Ops	Field-validation configuration; QA sample of profile quality
AML-CDD-002	Risk rating produced solely by the validated NG-KYC model. No manual rating entry path exists.	K	P	A	Real-time	Head, FC Risk & Control	Model configuration; change log; validation report
AML-CDD-003	Downward risk-rating overrides require FCC Advisory (VP+) approval; 100% reviewed by QA; monthly override report to FCRC.	K	P	H	Per case	Head, FCC Advisory	Override register with approver, rationale and QA outcome
AML-CDD-004	EDD memorandum completed and approved at the authority level in the Procedures before High-risk / PEP onboarding.	K	P	H	Per case	Head, FCC Advisory	EDD memo with approver identity and timestamp in NG-KYC
AML-CDD-005	Restricted Business Schedule enforced at onboarding: NG-KYC routes flagged categories to the mandated approver and blocks approval by anyone else.	K	P	A	Real-time	Head, FCC Advisory	Routing configuration; approval audit trail

ID	Control	K	N	X	Freq.	Owner	Evidence
AML-CDD-006	Prohibited categories (shell bank, bearer shares, anonymous account, s.311 designation, unresolved UBO) hard-blocked; no approval path exists in any system.	K	P	A	Real-time	BSA/AML Officer	Configuration attestation; quarterly re-performance by CTM
AML-CDD-007	Periodic review scheduling: NG-KYC generates the due population from the risk band and drives outreach, escalation, restriction and exit triggers automatically.	K	D	A	Daily	Head, KYC Ops	Due/overdue ageing report; restriction log
AML-CDD-008	Periodic review compares actual activity to expected activity and documents variance; reviews cannot be closed as ‘no change’ where a variance flag is set without an investigator referral.	K	D	H	Per case	Head, KYC Ops	Review record with activity comparison; referral log
AML-CDD-009	Correspondent banking: CBDDQ, PATRIOT Act certification and s.319 process agent obtained and current; annual refresh enforced by system expiry.	K	P	H	Annual	Head, Corr. Banking Compliance	Current CBDDQ and certification on file with expiry dates
AML-CDD-010	Monthly actual-vs-expected activity review for all correspondent respondents, by corridor, currency, volume and value.	K	D	H	Monthly	Head, Corr. Banking Compliance	Signed review pack with variance explanations and escalations
AML-SCR-001	100% of customers, beneficial owners, controllers, signatories and related parties screened at onboarding and continuously thereafter.	K	P	A	Continuous	Head, Screening Ops	Screening coverage reconciliation: customer master vs screened population (target: 100%)
AML-SCR-002	List ingestion SLA: OFAC within 4 hours of publication; all other lists within 24 hours; automated alert on load failure.	K	P	A	Per update	Head, Screening Ops	List load log with publication and load timestamps; failure alerts and resolution
AML-SCR-003	PEP flags cannot be removed without FCC approval and documented evidence; removals are 100% QA reviewed.		P	H	Per case	Head, FCC Advisory	PEP removal register with evidence and approver
AML-SCR-004	Four-eyes disposition of every screening match; the clearing rationale must name the specific discriminating data points.	K	D	H	Per alert	Head, Screening Ops	Disposition record with both user IDs and the written rationale
AML-SCR-005	Quarterly fuzzy-matching threshold tuning with above-the-line and below-the-line testing; results reviewed by Model Risk.	K	D	H	Quarterly	Head, FC Risk & Control	Tuning report, ATL/BTL samples, Model Risk sign-off
AML-TMS-001	All in-scope products, entities and channels feed NG-DETECT; the coverage matrix is reconciled monthly to the product and entity inventory.	K	P	A	Monthly	Head, FC Risk & Control	Coverage matrix with sign-off; approved gap register
AML-TMS-002	Scenario inventory mapped to the typologies in the enterprise risk assessment; any typology without a detection scenario is an accepted risk requiring BSA/AML Officer sign-off.	K	D	H	Annual	Head, FC Risk & Control	Typology-to-scenario mapping with gap acceptances
AML-TMS-003	Daily batch-completion control: NG-DETECT confirms all expected source feeds were received and processed; a missing feed triggers a P1 incident and a documented replay.	K	D	A	Daily	Head, FC Technology	Batch-completion log; incident and replay records
AML-TMS-004	L1 alert closures reviewed by a second analyst; L1 cannot close an alert on a customer with a SAR filed in the last 12 months (system-enforced routing to L2).	K	P	H	Per alert	Head, Investigations	NG-CASE audit trail; routing configuration

ID	Control	K	N	X	Freq.	Owner	Evidence
AML-TMS-005	Investigation completeness check before closure: minimum 90-day lookback, counterparty screening, adverse-media search and RFI resolution all recorded, or the case cannot be closed.	K	P	H	Per case	Head, Investigations	NG-CASE mandatory-field enforcement; QA sampling results
AML-TMS-006	Daily alert-ageing control against the statutory clock: any alert whose initial-detection date is more than 20 days old and which has no SAR decision is escalated to the Head of Investigations.	K	D	H	Daily	Head, Investigations	Ageing report with named escalations and outcomes
AML-TMS-007	Backlog tolerance: alert inventory beyond SLA must not exceed the KRI amber threshold; breach triggers a documented recovery plan approved by the BSA/AML Officer.		D	H	Weekly	Head, FC Operations	Backlog MI; approved recovery plan; weekly burn-down
AML-TMS-008	Initial-detection date is a mandatory, immutable field captured at case creation; subsequent changes require supervisor approval and are logged.	K	P	A	Per case	Head, Investigations	Field audit log of all changes with approvers
AML-TMS-009	QA sampling: 5% of alert closures, 10% of EDD approvals, 10% of SAR no-file decisions, 100% of downward overrides and deferrals.	K	D	M	Monthly	Head, QA	QA scorecards, error grading, theme reporting to FCRC
AML-RPT-001	SAR Review Committee meets at least twice weekly; every FILE and NO-FILE decision minuted with reasoning; no business representative present.	K	D	M	Twice weekly	Head, Investigations	Committee minutes with attendees, cases and decisions
AML-RPT-002	Automated SAR deadline control: NG-CASE computes 30/60/120-day deadlines from the initial-detection date and escalates at T-10, T-5 and T-2 days.	K	P	A	Daily	Head, Reg. Reporting	Deadline dashboard; escalation log; late-filing report (target: zero)
AML-RPT-003	Narrative quality review against the who/what/when/where/why/how standard before filing; a second reviewer signs off.	K	P	H	Per filing	Head, Reg. Reporting	Reviewed narrative with reviewer identity; QA narrative scores
AML-RPT-004	BSA Identifier acknowledgement retrieved from BSA E-Filing and reconciled to the case within 5 business days; unreconciled acknowledgements are a reportable failure.	K	D	H	Weekly	Head, Reg. Reporting	Reconciliation report; exception log
AML-RPT-005	SAR access control: role-based restriction, access logged, quarterly access recertification; SAR data cannot be exported to shared drives or external email (DLP-enforced).	K	P	A	Continuous	Head, FC Technology	Access logs; recertification evidence; DLP block reports
AML-RPT-006	CTR aggregation performed systemically across branches, ATMs and channels by the same conductor and same beneficiary on the same business day; no manual aggregation.	K	P	A	Daily	Head, Reg. Reporting	Aggregation logic documentation; independent re-performance by CTM
AML-RPT-007	CTR 15-day filing control with automated ageing and escalation; exemptions (Phase I / II) administered centrally and reviewed annually.	K	P	A	Daily	Head, Reg. Reporting	Filing timeliness report; DOEP register with annual review evidence
AML-RPT-008	314(a) search executed against the full customer and transaction population within the prescribed scope and responded to within 14 days; search completeness independently verified.	K	D	H	Per cycle	Head, FCC Advisory	Search logs; scope attestation; response confirmations from the secure site

ID	Control	K	N	X	Freq.	Owner	Evidence
AML-REC-001	Retention schedule enforced systemically in NG-ARCHIVE; records cannot be deleted before the retention date.	K	P	A	Continuous	Head, FC Technology	Retention configuration; deletion-attempt logs
AML-REC-002	Legal hold overrides retention; held records cannot be deleted, archived out of reach or migrated without Legal approval.	K	P	A	Continuous	General Counsel	Hold register; system enforcement evidence
AML-REC-003	Travel-rule completeness control on outbound payments ≥ $3,000: payments with incomplete originator or beneficiary data are stopped before release.	K	P	A	Real-time	Head, Payments Ops	Stopped-payment log with repair and release evidence
AML-REC-004	Inbound payments with missing or meaningless originator information are identified, investigated, and — where recurrent by correspondent — escalated to relationship level, not repaired indefinitely.		D	H	Daily	Head, Payments Ops	Incomplete-data report; correspondent escalation records
AML-REC-005	Annual reconciliation of the record inventory to the retention schedule; gaps raised as issues.		D	M	Annual	Head, FC Risk & Control	Reconciliation working papers
AML-DAT-001	Daily data-completeness reconciliation: record counts and value totals from each source system reconciled to NG-DETECT; variance beyond tolerance is a P1 incident.	K	D	A	Daily	Head, FC Technology	Reconciliation report with variance and resolution
AML-DAT-002	Critical data element (CDE) accuracy testing: quarterly sample-based tracing of CDEs from source to monitoring and screening.	K	D	M	Quarterly	Head, FC Risk & Control	CDE test results with error rates by element
AML-DAT-003	Timeliness control: data must be available to NG-DETECT by 06:00 ET T+1; delays are logged, backlogged and reported.		D	A	Daily	Head, FC Technology	Feed timeliness dashboard
AML-DAT-004	System-of-record coverage attestation: each business attests annually that every product, entity and channel it operates is fed to monitoring and screening.	K	P	M	Annual	Business Heads	Signed attestations; independent reconciliation by CTM
AML-DAT-005	New system, product or migration cannot go live without an FCC-approved data coverage assessment (part of the new-product approval gate).	K	P	H	Event	Head, FC Risk & Control	Approval gate records; coverage assessment documents
AML-GOV-001	Enterprise-wide ML/TF risk assessment refreshed at least annually; conclusions traced to resourcing, control calibration, training and testing coverage.	K	D	M	Annual	BSA/AML Officer	EWRA document; traceability matrix to actions
AML-GOV-002	Business-level risk assessments completed on the enterprise methodology; no local methodologies permitted.		D	M	Annual	Business Heads	Completed BRAs with FCC review sign-off
AML-GOV-003	Financial Crimes Risk Committee meets monthly with a quorum; decisions and dissent minuted; FCC objections overruled by the business are reported to the Board Risk Committee.	K	D	M	Monthly	BSA/AML Officer	Minutes; escalation record
AML-GOV-004	Mandatory AML training assigned on joining and annually; completion system-tracked; non-completion escalates to the manager and blocks system access at day 30.	K	P	A	Annual	Head, FC Training	Completion MI; access-suspension log

ID	Control	K	N	X	Freq.	Owner	Evidence
AML-GOV-005	Role-specific training for higher-risk roles with assessed comprehension (pass mark enforced, not attendance).		P	H	Annual	Head, FC Training	Assessment results by cohort
AML-GOV-006	Tipping-off control: exit and RFI communications use approved templates only; template variation requires FCC approval; breaches are reported to the BSA/AML Officer and Legal immediately.	K	P	H	Per case	Head, FCC Advisory	Template register; approval records; breach log
AML-GOV-007	Whistleblowing and escalation channel available, anonymous, monitored by FCC independent of the business; retaliation allegations reported to the Board.	K	D	M	Continuous	General Counsel	Case log; Board reporting
AML-GOV-008	Annual threshold tuning of every monitoring scenario with ATL/BTL testing; changes require FCC and Model Risk approval and a documented detection-impact assessment.	K	D	H	Annual	Head, FC Risk & Control	Tuning packs; approvals; impact assessments
AML-GOV-009	Independent model validation of NG-DETECT and the NG-KYC rating model on the cycle set by the Model Risk Management Policy; findings tracked to closure.	K	D	M	Per cycle	Head, Model Risk	Validation reports; finding tracker
AML-GOV-010	Scenario and threshold change control: no change to detection logic may be promoted to production without FCC approval, testing evidence and a back-out plan.	K	P	H	Per change	Head, FC Technology	Change tickets with approvals and test evidence
AML-GOV-011	Third-party AML activity oversight: due diligence, contractual audit rights, SLA monitoring, and periodic QA of the vendor’s output by the accountable Firm function.	K	D	H	Quarterly	Head, FC Operations	Vendor scorecards; QA sample results; right-to-audit exercises
AML-GOV-012	Annual control attestation by every control owner (Section 13).	K	D	M	Annual	Head, FC Risk & Control	Signed attestations with exceptions declared

Controls AML-CIP-005 to 009, AML-CDD-011 to 016, AML-TMS-010 to 014, AML-RPT-009 to 012 and AML-DAT-006 to 008 are non-key supporting controls and are set out in the RCM system of record (NG-GRC). The 24 Key Controls above are the population subject to mandatory annual 2LOD testing and permanent 3LOD scope.

6. Key Control detail sheets

Every Key Control carries a detail sheet in NG-GRC. Four representative sheets are reproduced here to fix the standard; the remaining twenty follow the same template exactly.

AML-RPT-002 — SAR statutory deadline control

Attribute	Specification
Control objective	No SAR is filed after the statutory deadline, and every deadline is computed from the correct initial-detection date.
Risk mitigated	R4.2 — late filing; incorrect clock start.
Nature / execution / designation	Preventive / Automated / **Key**
Frequency	Continuous computation; daily escalation cycle at 07:00 ET.
Owner	Head of Regulatory Reporting.
Population	Every open case in NG-CASE carrying an initial-detection date. Completeness is assured because NG-CASE will not permit case creation without the field (AML-TMS-008).
Input	Initial-detection date; suspect-identified flag; prior related filing date and BSA Identifier for continuing activity.
Criterion	30 calendar days from initial detection where a suspect is identified; 60 where no suspect is identified; 120 from the prior related filing for continuing activity. Deadlines falling on a weekend or federal holiday move to the preceding business day.
Execution	The system computes the deadline, displays days remaining on every case, and generates escalations at T-10 (investigator and team lead), T-5 (Head of Investigations), and T-2 (BSA/AML Officer). A case cannot be parked, snoozed or re-queued in a way that suppresses the escalation.
Exception handling	Any case reaching T-2 without a SAR decision is escalated by name to the BSA/AML Officer and is presented at the next SAR Review Committee as a standing agenda item. Any filing made after the deadline is a Critical control failure: it is reported to the Financial Crimes Risk Committee, root-caused within five business days, and disclosed to the regulator where required.
Evidence	Deadline dashboard extract; escalation log; late-filing report (target: zero); monthly filing-timeliness MI.
Known failure modes	(a) The initial-detection date is recorded as the alert-assignment date rather than the true detection date, quietly extending the clock — tested by AML-TMS-008 and by CTM re-performance; (b) a case is closed and re-opened, resetting the clock — prevented systemically and logged; (c) continuing activity is treated as a new matter, resetting the 120-day cycle — detected by the prior-SAR linkage check.
Test procedure (CTM)	Select a sample per Appendix A across the filing population. For each: independently re-derive the initial-detection date from the underlying alert and transaction data; recompute the deadline; compare to the filing date on the BSA acknowledgement. Separately, test all initial-detection-date changes in the period against approval evidence.

AML-TMS-001 — Transaction monitoring coverage

Attribute	Specification
Control objective	Every in-scope product, entity, channel and account type is fed to NG-DETECT, so that no population of transactions is invisible to monitoring.
Risk mitigated	R3.1 / R7.1 — suspicious activity occurs and no alert can ever be generated, because the data never arrives.
Nature / execution / designation	Preventive / Automated with manual reconciliation / **Key**

Attribute	Specification
Frequency	Monthly reconciliation; event-driven on any new product, entity, system or migration.
Owner	Head of Financial Crimes Risk and Control.
Population	The full product and legal-entity inventory maintained by Finance and Product Control — not a list maintained by FCC, which would be self-referential.
Criterion	Every product/entity/channel combination in the inventory maps to at least one NG-DETECT feed and at least one applicable scenario, or appears on the approved gap register with a BSA/AML Officer risk acceptance and an expiry date.
Exception handling	An unmapped population is a Critical failure. Monitoring gaps are reported to the Financial Crimes Risk Committee immediately, a compensating manual review is put in place within five business days, and a retrospective lookback over the gap period is scoped.
Evidence	Signed coverage matrix; the gap register with approvals and expiry dates; reconciliation working papers.
Known failure modes	(a) A migration moves a product to a new source system and the feed is not re-pointed; (b) a new legal entity is booked under an existing entity code and inherits scenarios that do not fit its risk; (c) a channel (e.g. a new instant-payment rail) is launched and the coverage assessment is treated as a post-launch task.
Test procedure (CTM)	Take the product and entity inventory from Finance. Independently trace a sample end-to-end to NG-DETECT feed logs and scenario assignment. Test the gap register for expired acceptances.

AML-SCR-004 — Screening match disposition

Attribute	Specification
Control objective	No screening match is cleared unless the discriminating evidence is specific, documented and independently reviewed.
Risk mitigated	R2.2 — a true match is cleared as a false positive.
Nature / execution / designation	Detective / Hybrid / **Key**
Frequency	Per alert.
Owner	Head of Screening Operations.
Criterion	The clearing rationale must name at least one hard discriminator — date of birth, nationality, unique identifier, or an established and evidenced identity difference. Soft reasoning (‘common name’, ‘unlikely’, ‘customer is known to us’) is not a discriminator and must be rejected by the reviewer.
Exception handling	Potential sanctions true matches are escalated to the Sanctions team within two hours and are never cleared by Screening Operations. PEP and adverse-media true matches route to EDD.
Evidence	Disposition record showing both user IDs, timestamps, the list entry compared, and the written rationale.
Known failure modes	(a) Reviewer approves in bulk without opening the underlying match; (b) rationale is copied from a prior disposition on a different person; (c) the same analyst prepares and reviews using a shared or generic account — prevented by unique-ID enforcement and detected by QA.
Test procedure (CTM)	Re-perform a sample of cleared matches against the source list entry. Any match that a competent reviewer would not have cleared on the evidence recorded is a Critical exception, irrespective of whether the person turned out to be listed.

AML-CDD-003 — Downward risk-rating override

Attribute	Specification
Control objective	A customer's risk rating is never reduced below the model output without evidence and independent approval.

Attribute	Specification
Risk mitigated	R1.3 — understated risk leading to reduced diligence, longer review cycles and higher monitoring thresholds.
Nature / execution / designation	Preventive / Hybrid / **Key**
Frequency	Per case; monthly reporting.
Owner	Head of FCC Advisory.
Criterion	The override must state the specific model input believed to be wrong, the evidence that it is wrong, and why the residual risk is within appetite. A commercial reason is never a valid basis and must be rejected.
Exception handling	An override applied without approval is a Critical failure: the rating is reverted immediately, the relationship is re-reviewed, and the individual is referred to Employee Relations.
Evidence	Override register: customer, model rating, overridden rating, rationale, evidence, approver, date, QA outcome.
Known failure modes	(a) The override is applied to hit an onboarding SLA; (b) the override is applied because the customer complained about EDD requests; (c) a systemic pattern of overrides in one business indicates the model, or the business, needs investigation — which is why the rate, not just the individual case, is a KRI.
Test procedure (CTM)	100% population review by QA. CTM re-performs a sample and separately analyses the override rate by business, by analyst and by approver for concentration.

7. Screening control specification

7.1 Matching configuration

Parameter	Standard	Rationale
Algorithm	Deterministic exact match plus phonetic and fuzzy matching (edit distance and token-based), with transliteration support for Arabic, Cyrillic and Chinese name forms.	Name-based evasion is the norm, not the exception. Exact matching alone is not a control.
Sanctions match threshold	Set deliberately low (high recall, low precision). Northgate accepts a high false-positive rate on sanctions in exchange for recall.	A missed sanctions hit is a strict-liability breach. A false positive costs an analyst twenty minutes.
PEP / adverse-media threshold	Set on a risk-tiered basis, tighter for High-risk customers and jurisdictions.	These are risk-based obligations, unlike sanctions.
Fields screened	Name; alias and AKA; date of birth; place of birth; nationality; address; identifiers (passport, national ID, LEI, IMO); and for payments: originator, beneficiary, ordering and beneficiary institutions, intermediaries, free-text fields, goods, vessels and ports.	Free-text and narrative fields are a common gap and are where evasion language appears.
Tuning cadence	Quarterly ATL/BTL testing; annual full recalibration; any threshold change requires Model Risk validation and a detection-impact assessment.	Thresholds drift as the customer base and list content change.

> **Below-the-line testing is the point**
>
> Above-the-line testing samples what the engine caught and asks whether it was cleared correctly. Below-the-line testing samples what the engine did **not** catch — records scoring just under the threshold — and asks whether anything true was missed. Only BTL testing can evidence that a threshold is not set too high. A tuning exercise that reports only false-positive reduction, with no BTL evidence, is a cost-saving exercise wearing a compliance costume, and will be treated as a finding.

8. Transaction monitoring: coverage, tuning and model governance

8.1 Scenario inventory (illustrative extract)

Scenario	Typology addressed	Segmentation
Structuring — sub-threshold cash aggregation across branches, ATMs and days	Evasion of CTR reporting (31 U.S.C. § 5324)	Retail; small business; by branch footprint
Rapid movement of funds — in and out within a short window, leaving minimal balance	Layering; funnel accounts; money-mule activity	Retail; SMB; by expected balance profile
Activity inconsistent with the KYC profile — volume, value, corridor or counterparty	General laundering; account takeover; undisclosed business change	All segments; peer-group calibrated
High-risk jurisdiction exposure — unexplained flows to or from High-rated countries	Corruption; sanctions evasion; illicit trade	By customer risk band and expected corridors
Round-dollar and repeating-amount payments to unrelated third parties	Trade-based laundering; invoice fraud; shell-company payments	Corporate; SMB

Scenario	Typology addressed	Segmentation
Correspondent: originators or beneficiaries inconsistent with the respondent's stated customer base; unexpected new corridors; MT202COV inconsistent with the underlying MT103	Nesting; downstream correspondent abuse	Correspondent portfolio; by respondent
Trade finance: price, quantity or weight anomaly; circular shipping; dual-use goods; unnecessary intermediation	Trade-based money laundering; proliferation financing	Trade portfolio
Virtual assets: exposure to mixers, tumblers, high-risk exchanges or anonymity-enhancing assets	Illicit VASP exposure; darknet proceeds	Digital-asset portfolio
Human-trafficking indicators: multiple third-party cash deposits in disparate locations; transactions near motels, transport hubs; shared address or device across many accounts	Human trafficking and exploitation	Retail; by geography

8.2 Segmentation

Thresholds are applied by peer segment, not to the whole book. Segments are derived from customer type, expected activity, business size and risk band, and are re-derived annually. A segment that contains materially dissimilar customers produces thresholds that are too high for the small and too low for the large, generating noise at one end and blindness at the other. Segment homogeneity is tested as part of annual tuning.

8.3 Tuning governance

1. Define the tuning objective and the population. A tuning exercise is never framed as a target percentage reduction in alerts. That is a prohibited objective.
2. Perform ATL testing on a statistically valid sample of alerts generated in the period.
3. Perform BTL testing on records scoring immediately below the threshold, sampled across segments, to establish whether productive activity is being missed.
4. Quantify the detection impact of any proposed change: which of the last 24 months of SARs would still have been detected under the new threshold? A change that would have suppressed a filed SAR is rejected unless another scenario demonstrably catches it.
5. Obtain FCC and Model Risk approval. Document the decision, the evidence and the residual risk.
6. Promote through change control (AML-GOV-010) with a back-out plan, and monitor alert and escalation volumes for 90 days post-change.

Prohibited tuning practices

Raising a threshold because the alert volume exceeds team capacity. Disabling a scenario to clear a backlog. Narrowing a segment to exclude a noisy customer. Excluding a customer, product or corridor from monitoring by exception rather than by design. All of these convert an operational problem into a detection failure, and each has been the subject of public enforcement action against other institutions.

9. Data quality controls and system coverage

9.1 The five dimensions tested

Dimension	Question	Control
Completeness	Did every transaction that occurred arrive in the monitoring system?	AML-DAT-001 (daily count and value reconciliation, source to target)
Accuracy	Does the value in monitoring match the value in the source system?	AML-DAT-002 (quarterly CDE tracing, sample-based)
Timeliness	Did it arrive in time to be monitored on the correct cycle?	AML-DAT-003 (feed timeliness dashboard; late feeds trigger replay)
Coverage	Is the source system connected at all?	AML-DAT-004, AML-TMS-001 (annual attestation and monthly reconciliation to the product and entity inventory)
Lineage	Can the Firm demonstrate how a field travelled from source to alert?	Data lineage documentation maintained for every CDE; tested by CTM and by Internal Audit

9.2 Critical data elements

The following are designated CDEs. An error rate above tolerance in any of them is a Critical control failure, because monitoring and screening cannot work without them: customer identifier; customer risk rating; customer type; country of residence, incorporation and operation; beneficial-owner identifiers; account identifier; transaction amount; transaction currency; transaction date and time; transaction type; channel; counterparty name; counterparty account; counterparty country; originator and beneficiary name and address; ordering and beneficiary institution BIC; and payment free-text.

10. Key Risk Indicators and Key Performance Indicators

KRIs measure whether risk is increasing. KPIs measure whether the function is performing. They are not the same and must never be blended into a single dashboard that lets good performance mask rising risk. Thresholds below are illustrative of the Firm’s calibration.

Indicator	Type	Green	Amber	Red
SARs filed after the statutory deadline	KRI	0	—	≥ 1
CTRs filed after 15 calendar days	KRI	0	—	≥ 1
Accounts activated without CIP PASS or approved deferral	KRI	0	—	≥ 1
Customers with no monitoring coverage (unmapped population)	KRI	0	—	≥ 1
314(a) responses submitted after 14 days	KRI	0	—	≥ 1
Periodic reviews overdue beyond the restriction point	KRI	0	1–5	> 5
Alerts aged beyond SLA as a % of open inventory	KRI	< 5%	5–10%	> 10%
Cases open beyond 20 days from initial detection with no SAR decision	KRI	< 2%	2–5%	> 5%
Downward risk-rating override rate	KRI	< 2%	2–4%	> 4%

Indicator	Type	Green	Amber	Red
CDE accuracy error rate	KRI	< 1%	1–3%	> 3%
Screening BTL testing — true matches found below the line	KRI	0	—	≥ 1
QA Critical error rate	KRI	< 1%	1–3%	> 3%
Mandatory training completion	KPI	≥ 99%	95–99%	< 95%
Open Critical / High audit and regulatory issues past due	KRI	0	1–2	> 2
Alert-to-SAR conversion rate (monitored for unexplained movement, not targeted)	KPI	Stable	± 25% shift	± 50% shift
L1 triage SLA attainment	KPI	≥ 95%	90–95%	< 90%
Onboarding cycle time — High risk	KPI	≤ 15 days	16–25 days	> 25 days

A falling alert-to-SAR conversion rate is not a success

Conversion rate is presented as a diagnostic, never as a target. If alerts rise and filings do not, the question is whether the scenarios have become noisy — or whether investigators have become reluctant. If alerts fall and filings fall with them, the question is whether the risk fell or the thresholds rose. Any material movement in this ratio must be explained to the Financial Crimes Risk Committee with evidence, not narrated as an efficiency gain.

11. Control testing methodology and sample sizes

11.1 Who tests what

Line	Activity	Frequency	Reports to
1LOD	Control owner self-testing and self-identification of issues. Self-identification is expected and is viewed favourably; a control owner who never self-identifies is not assumed to be operating a perfect control.	Quarterly for Key Controls	Business risk and control committee; results feed the annual attestation
2LOD	Compliance Testing and Monitoring (CTM): independent testing of design and operating effectiveness, including re-performance.	All Key Controls at least annually; risk-based thematic testing throughout the year	BSA/AML Officer; Financial Crimes Risk Committee
3LOD	Internal Audit: independent assurance over the whole program, including the adequacy of 2LOD testing itself.	Risk-based; AML program in permanent audit scope; correspondent banking, monitoring and reporting audited at least annually	Audit Committee of the Board
External	Independent testing by a qualified external party where Internal Audit lacks the specialist expertise; and regulatory examination.	As required	Audit Committee; regulators

11.2 Testing both questions

- **Design effectiveness.** If this control operated perfectly, every single time, would the risk be mitigated? Walk the control through the risk. A design test does not require a sample; it requires a walkthrough, the

documentation, and a hard question.

- **Operating effectiveness.** Did the control actually operate, on the whole population, throughout the period, with evidence? This requires a sample and re-performance — not an enquiry of the control owner, and not an inspection of a summary the control owner prepared.
- **Re-performance is the standard.** The tester reaches the conclusion independently from the source data and then compares. Inspecting the operator's conclusion and agreeing with it is not testing.

11.3 Sample sizes

Sample sizes are set by control frequency and by whether the control is Key. See Appendix A. Where a deviation is found, the sample is extended; a deviation in an extended sample results in a conclusion of **not effective** and the control cannot be relied upon in the risk assessment until it is remediated and re-tested.

12. Issue management and remediation

Severity	Definition	Root cause due	Remediation due	Approval to extend
Critical	A regulatory breach has occurred or is highly likely; a statutory filing was missed or late; a population was unmonitored; a prohibited relationship was onboarded.	5 business days	90 days	BSA/AML Officer + Board Risk Committee
High	A Key Control is not operating effectively; the risk of a breach is elevated but no breach is evidenced.	10 business days	180 days	BSA/AML Officer
Medium	A non-key control is not operating effectively, or a Key Control has a documentation or evidence deficiency without an outcome failure.	20 business days	270 days	Head of FC Risk and Control
Low	An efficiency or documentation observation with no risk impact.	n/a	365 days	Control owner

- Every issue has a named individual owner — never a team, never a committee. The owner is the person who can actually fix it, not the person who reported it.
- Root cause must be a cause, not a restatement of the symptom. "The analyst did not follow the procedure" is a symptom. Why did they not? Capacity? Training? An unclear procedure? A system that made the wrong action easier than the right one? Remediation aimed at a symptom does not close the issue.
- Extensions are governed, logged and reported. A second extension request on the same issue escalates automatically to the Financial Crimes Risk Committee. A pattern of extensions across a business is itself reported to the Audit Committee.
- Closure requires independent validation by CTM (2LOD issues) or Internal Audit (3LOD issues). An issue is never closed on the assertion of the owner that it is fixed.
- Where an issue reveals that a control was ineffective for a period, a **lookback** must be scoped: what activity occurred while the control was not working, and does any of it require a filing? The lookback is the remediation. Fixing the control forward without a lookback leaves the original suspicion unreported.

The lookback is not optional

If a monitoring scenario was broken for eight months, the Firm did not simply have a control gap — it may have failed to file reports it was legally required to file. The remediation plan must state the lookback population, the period, the methodology and the resourcing, and must be agreed with the BSA/AML Officer and, where material, disclosed to the regulator. Retrospective filings are made as soon as the suspicion is formed, not at the end of the exercise.

13. Control attestation and change governance

13.1 Annual attestation

Each control owner attests annually, in writing, that: the control as described in the RCM is the control actually operated; it operated throughout the period on the complete population; the evidence exists and is retained; every exception was identified, escalated and recorded; and any deficiency is declared in the attestation. Attestations are supported by the 1LOD self-testing results and are subject to CTM validation and Internal Audit testing. A false or unsupported attestation is a serious disciplinary matter (Policy § 22.4).

13.2 Change governance

- No control may be added, amended, withdrawn or downgraded from Key without the approval of the Head of Financial Crimes Risk and Control; withdrawal or downgrade of a Key Control additionally requires BSA/AML Officer approval and notification to the Financial Crimes Risk Committee.
- Where a control is withdrawn, the risk it mitigated must be re-mapped to another control or explicitly accepted. A withdrawn control that leaves a risk unmapped is a Critical issue on the day it is withdrawn.
- System changes affecting a Key Control follow AML-GOV-010: FCC approval, test evidence, a back-out plan, and post-implementation monitoring.
- The RCM in NG-GRC is the single system of record. Local spreadsheets, shadow control inventories and business-maintained matrices are prohibited; where they are found, they are reported as a control-inventory failure.

Appendix A — Control test sample-size table

Minimum sample sizes for testing operating effectiveness over a 12-month period, assuming no deviations. Key Controls take the higher figure. On the first deviation, extend the sample; on a deviation in the extended sample, conclude **not effective**.

Control frequency	Population (approx.)	Non-key sample	Key sample	Extended sample on first deviation
Annual	1	1	1	Not applicable — a deviation is a failure
Quarterly	4	2	3	All 4
Monthly	12	3	5	10
Weekly	52	8	12	25
Daily	250	25	40	60
Recurring / per item (e.g. per alert, per case, per filing)	Variable	25 (or 10% if lower)	45 (or 15% if lower)	Double the original sample, minimum 60
Automated (configuration-based)	n/a	1 test of configuration plus evidence that change control operated over the period	As non-key, plus independent re-performance of the logic against a data sample	Full re-performance

Appendix B — Control failure severity definitions

Severity	The control failure...	Example
Critical	...has resulted, or would in the ordinary course result, in a breach of a statutory obligation, an unreported suspicion, an undetected population, or a prohibited relationship.	A SAR filed on day 42. A monitoring feed absent for a quarter. An account onboarded without beneficial ownership. A true sanctions match cleared.
High	...means a Key Control cannot be relied upon, materially elevating the likelihood of a Critical outcome, though none is yet evidenced.	Four-eyes review evidenced in only 80% of a sample. Screening list loaded 3 days late on several occasions with no true matches in the window.
Medium	...affects a non-key control, or affects the evidence of a Key Control without evidence that the outcome was wrong.	The control operated but the rationale was not recorded to standard. QA sampling below the mandated rate for two months.
Low	...has no risk impact and is a matter of documentation, efficiency or presentation.	The RCM description is out of date relative to a system rename.

Approval

Approved by the Global Head of Financial Crimes Compliance (designated BSA/AML Officer) on 9 April 2026 and noted by the Financial Crimes Risk Committee on 16 April 2026. Effective 1 May 2026.

— End of Standard —