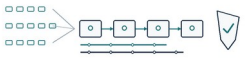
DQIntegrity | Resolvo Advisory

Decision-Critical Data Integrity and Controls



Independent assurance for data used in financial crime, payments, reporting and AI

Data fails quietly. Until it does not.

DQIntegrity helps regulated organisations establish whether decision-critical data remains complete, correct, timely, understood and controlled throughout its end-to-end journey.

It identifies where data integrity breaks, defines practical controls at the points where failure can occur, and provides evidence that monitoring, screening, payments, reporting and automated decisions can be trusted.

THE FOUR QUESTIONS THAT MATTER

01	02	03	04
COMPLETE	**CORRECT**	**TIMELY**	**EVIDENCED**
Did the full expected population arrive?	Did meaning remain right through transformation?	Did data arrive within the required decision window?	Can the organisation prove all three?

WHERE DQINTEGRITY OPERATES

Financial crime Transaction monitoring, screening, KYC/CDD and remediation	**Payments** End-to-end journeys, reconciliation, exceptions and operational evidence	**Reporting** Regulatory, risk and management decisions supported by controlled data
Platform change Migration, integration, transformation and pre-go-live assurance	**AI and analytics** Data readiness, provenance, traceability and decision controls	**Control remediation** Root causes, sustainable controls, ownership and evidence

Principal-led, independent and focused on control evidence - not a predetermined technology or generic data-quality programme.

DISCUSS A CONFIDENTIAL DATA INTEGRITY MANDATE

Where data integrity breaks

Stable outputs do not prove that the data journey underneath is complete or correct

Monitoring engines can generate alerts, screening can complete, payment processing can continue and dashboards can remain green while part of the required data population has already been lost, delayed or distorted.

THE END-TO-END JOURNEY AND COMMON BREAKPOINTS

SOURCE	INGEST	TRANSFORM	CURATE	DECIDE	OUTCOME
Customers, accounts, transactions and events originate upstream.	Files, messages or records may fail, filter or arrive late.	Mappings, formats and business meaning can change.	Partial or distorted data may still appear usable.	Monitoring, screening, reporting or AI acts on what arrived.	Controls appear operational even when coverage is weakened.

FOUR FAILURE MODES

COMPLETENESS
Missing records, partial populations, ungoverned filtering, dropped interfaces and late arrivals.

CORRECTNESS
Wrong mappings, truncation, invalid values, duplication, formatting changes and semantic drift.

TIMELINESS
Data arrives after monitoring, sequencing, reporting or operational decision windows have passed.

CONTROL EVIDENCE
No governed expected population, weak thresholds, unclear ownership or proof limited to final outputs.

WHY GENERIC DATA QUALITY IS NOT ENOUGH

DATA QUALITY

Often focuses on the condition of data already visible within a dataset: validity, format, accuracy, consistency or conformance.

- Can miss records that never arrived.
- May validate syntax without preserving business meaning.
- Can look healthy at the final layer while upstream coverage is broken.

DATA INTEGRITY

Tests whether data can still be trusted end-to-end after movement, filtering, transformation, aggregation and control execution.

- Defines the expected population before testing what arrived.
- Proves completeness, correctness and timeliness at critical hand-offs.
- Connects detected breaks to ownership, escalation and evidence.

WHAT FAILURE CREATES

FALSE ASSURANCE	CONTROL FAILURE	LATE DISCOVERY	REMEDIATION COST
Stable MI and control output can mask reduced coverage.	Monitoring or screening cannot act on records it never received.	Issues emerge through incidents, audit or regulatory challenge.	Weak root-cause control creates repeated fixes and prolonged exposure.

Working principle: if data integrity is not proven, control effectiveness is only assumed.

COMPLETE | CORRECT
TIMELY | EVIDENCED

The DQIntegrity control architecture

A repeatable framework for proving data integrity across the decision-data journey

The framework starts with the business decision and expected population, places controls where integrity can fail, and connects exceptions to accountable response and durable evidence.

FIVE-STAGE DIAGNOSTIC AND DESIGN METHOD

1	2	3	4	5
DEFINE	**TRACE**	**TEST**	**ASSESS**	**PRIORITISE**
Expected populations, material decisions and critical data requirements.	Sources, interfaces, filters, transformations and decision use.	Completeness, correctness, timeliness and reconciliation evidence.	Control design, ownership, thresholds, exceptions and governance.	Stabilisation, target controls, remediation and assurance roadmap.

CONTROL ARCHITECTURE

1 REQUIREMENTS AND EXPECTED POPULATIONS	Define the governed population, material decision, critical data elements, timing expectations and success criteria.	**What should exist and why does it matter?**
2 CONTROLS AT CRITICAL HAND-OFFS	Apply count and value reconciliation, mapping and field checks, uniqueness, timeliness and source-to-target evidence where failure can occur.	**Did the right data arrive, intact and on time?**
3 EXCEPTIONS, OWNERSHIP AND ESCALATION	Set thresholds, route exceptions, assign accountable owners, distinguish incidents from tolerated variance and drive root-cause response.	**Who knows, who decides and who acts?**
4 EVIDENCE, REPORTING AND SUSTAINABILITY	Retain control evidence, expose residual risk, track remediation, support audit and regulatory review, and monitor whether controls remain effective.	**Can senior stakeholders rely on the assurance?**

CORE CONTROL DIMENSIONS

POPULATION	RECONCILIATION	CORRECTNESS	TIMELINESS	OWNERSHIP	EVIDENCE
Expected records and scope	Counts, values and stages	Mappings, fields and meaning	Windows, sequencing and delay	Accountability and escalation	Repeatable proof and reporting

WHAT GOOD LOOKS LIKE

- The expected population is explicitly defined and agreed between data owner and data user.
- Controls sit at the hand-offs where data can be lost or meaning can change.
- Completeness and correctness are tested as distinct control disciplines.
- Exceptions route to accountable teams with clear escalation and remediation.
- Senior reporting distinguishes proven coverage from assumed system stability.
- Control evidence is repeatable, sustainable and usable for audit or regulatory challenge.

The objective is not more dashboards. It is defensible evidence that the data supporting material decisions remains controlled.

DEFINE | TRACE | TEST
ASSESS | PRIORITISE

Applications and commercial services

Specialist data-integrity support for high-consequence environments

DQIntegrity is applied where incomplete, incorrect or weakly governed data can undermine control effectiveness, regulatory confidence, operational decisions or automated outcomes.

WHERE THE FRAMEWORK APPLIES

TRANSACTION MONITORING Prove that required transactions, accounts and customer attributes reach monitoring in full, correctly transformed and within required windows.	**SANCTIONS AND SCREENING** Assess customer, account and payment populations, hand-offs, exclusions, mapping and evidence supporting screening coverage.	**KYC / CDD** Strengthen customer-data requirements, event-driven or periodic review inputs, workflow hand-offs and evidence supporting due-diligence decisions.
PAYMENTS AND RECONCILIATION Design count and value controls across interfaces, identify dropped or rejected transactions and improve exception ownership.	**REPORTING AND REMEDIATION** Test whether regulatory, risk and management reporting rests on controlled populations and whether remediation addresses root causes.	**AI AND ANALYTICS** Assess data readiness, representativeness, provenance, traceability, human oversight and fallback before automated decision use.

WHAT CLIENTS CAN ENGAGE DQINTEGRITY TO DELIVER

01 DATA INTEGRITY DIAGNOSTIC A focused assessment of critical data flows, integrity risks, control gaps, ownership and priority remediation.	**02 DATA CONTROLS FRAMEWORK** Design of practical completeness, correctness, timeliness, reconciliation, exception and evidence controls.
03 TM AND SCREENING DATA ASSURANCE Independent challenge of whether monitoring and screening receive the complete and correct data they are expected to process.	**04 PAYMENTS DATA AND RECONCILIATION CONTROLS** Controls across payment hand-offs, count and value reconciliation, rejected transactions and operational evidence.
05 AI AND ANALYTICS DATA READINESS Assessment of whether data is sufficiently understood, controlled, traceable and appropriate for automated or analytical use.	**06 REMEDIATION AND DELIVERY ASSURANCE** Independent oversight of remediation, migration or transformation where data integrity is a critical dependency.

COMMON TRIGGERS

- The organisation cannot prove that all required records reach a material control or decision tool.
- Existing reconciliations are aggregated, manual, late or unable to locate the point of failure.
- A migration, platform change or remediation depends on data that is not sufficiently evidenced.
- Monitoring or screening appears stable but coverage, mapping or timeliness remains uncertain.
- Ownership is fragmented across source systems, data platforms, technology and operational teams.
- AI or automation is advancing without a defensible data-readiness and control position.

Each service can stand alone or connect to NFRisk financial-crime, payments, programme-assurance or bank-readiness mandates where the findings justify it.

SPECIALIST DEPTH
WITHOUT AUTOMATIC DEPENDENCY

From uncertainty to defensible assurance

Principal-led diagnosis, practical control design and evidence for senior stakeholders

HOW AN ENGAGEMENT BEGINS

1	2	3	4
SCOPE	**DIAGNOSE**	**DECIDE**	**DELIVER**
Clarify the decision, expected population, material concern and evidence available.	Trace the journey, test controls and distinguish symptoms from structural causes.	Present findings, risk, immediate stabilisation and proportionate intervention options.	Design controls or provide independent remediation and implementation assurance where required.

TYPICAL ENGAGEMENT OUTPUTS

- Critical end-to-end data-flow and control-point map
- Expected-population and material data-requirement definition
- Completeness, correctness and timeliness risk assessment
- Record, value, mapping and transformation control findings
- Ownership, thresholds, exception and escalation assessment
- Immediate stabilisation actions and prioritised remediation roadmap
- Target control architecture and evidence model
- Executive assurance conclusion and presentation

EXPERIENCE INFORMING THE PROPOSITION

- Global transaction-monitoring data strategy and data-control leadership across complex, multi-country environments.
- Completeness, correctness, reconciliation, ownership and regulatory-evidence controls across multi-layer source-to-monitoring journeys.
- Financial-crime remediation, operating-model transformation and control closure involving business, data, technology and operations.
- End-to-end payments delivery spanning requirements, architecture, testing, reconciliation, operational readiness, go-live and warranty.
- Synthetic-data and data-readiness experience supporting perpetual KYC, testing and controlled AI or automation use cases.

WHY DQINTEGRITY

- Principal-led and independent
- Financial-crime, payments and control context
- End-to-end rather than tool-only view
- Practical controls and accountable evidence
- No predetermined technology or large-team dependency

BRAND AND DELIVERY ARCHITECTURE

RESOLVO ADVISORY	NFRISK	DQINTEGRITY
Legal and commercial umbrella	Principal senior advisory proposition	Specialist data and control integrity proposition

Available for selected advisory, diagnostic and transformation engagements. Prior-employer references describe experience and do not imply endorsement.

DISCUSS A CONFIDENTIAL MANDATE
DQINTEGRITY.COM | NFRISK.COM