A GOVERNANCE-GRADE MARKET INTELLIGENCE CONTROL

WHAT IS CQ?

CQ is an acronym for **C**ustomer ac**Q**uisition and began as a marketing project designed to expand digital banking. The goal was to help banks attract and retain SMEs and entrepreneurs by delivering accurate, high-frequency, high-granularity market-share insights for business account holders. For this to be possible, merging transactional data from multiple banks in each region was necessary, which resulted in clearing all regulatory hurdles and obstacles, notably in the EU/EEA where they are the strictest.

From this initial focus, CQ has evolved into a data-governance and decision-governance control layer that ensures banks operate on clean, auditable, regulator-safe market signals. It functions like a control because it:

- Enforces aggregation thresholds.
- Prevents personal-data exposure.
- Standardizes market-share measurement.
- Reduces model-risk and commercial miscalibration.
- Creates a single, audit-ready source of truth.

CQ is a *governance-strengthening control* which creates a **verifiable, auditable, non-personal, cross-bank market-share baseline** that reduces model risk, commercial miscalibration, and internal decision bias while staying fully outside PCI, GDPR, and banking-secrecy exposure.

1. CQ STRENGTHENS DATA GOVERNANCE BY ENFORCING STRICT AGGREGATION BOUNDARIES

CQ's architecture forces the bank to operate on **non-personal, non-PCI, non-customer-identifiable data**. This acts as a *structural control* because:

- Only **aggregated ATH/CTH-derived metrics** enter the CQ pipeline.
- No PAN, no SAD, no cardholder data, no behavioral patterns.
- CQ cannot technically access raw data – **the bank controls the file, the thresholds, and the sharing logic**.

This reduces governance exposure by eliminating entire classes of data-handling risk.

2. CQ IMPROVES MODEL GOVERNANCE AND REDUCES COMMERCIAL DECISION RISK

Banks routinely make pricing, acquisition, and RM decisions using **partial, biased, or incomplete market data**. CQ introduces a governance control by:

- Providing **externally benchmarked, cross-bank market-share baselines**.

- Eliminating internal over-reliance on a single bank's limited coverage.
- Reducing the risk of **mispriced SME portfolios**, **incorrect acquisition targeting**, or **false performance attribution**.

CQ acts as a **data quality uplift control** that reduces model error and improves decision defensibility.

3. CQ STRENGTHENS OVERSIGHT THROUGH AUDITABILITY AND TRACEABILITY

CQ's ingestion and aggregation logic is:

- deterministic
- threshold-based
- auditable
- fully bank-controlled

This gives the bank a **repeatable, reviewable, regulator-friendly** process for generating competitive intelligence. It becomes a governance control because it:

- Creates a **single source of truth** for market-share metrics.
- Ensures **consistent methodology** across business units.
- Supports **internal audit**, **model validation**, and **regulatory review**.

4. CQ REDUCES REGULATORY EXPOSURE BY DESIGN

CQ's architecture inherently avoids:

- PCI DSS scope
- GDPR personal-data processing
- Banking secrecy violations
- Cross-border data-transfer risk

Because CQ only receives **aggregated, threshold-validated business-type metrics**, the bank can demonstrate:

- **No personal data leaves the bank**
- **No merchant-specific insights are shared externally**
- **Only aggregated, competition-safe metrics** are exchanged

This positions CQ as a **regulatory-aligned control**, not a risk.

5. CQ ENHANCES GOVERNANCE OF SME AND MERCHANT-PORTFOLIO STRATEGY

Banks often lack a governance mechanism to ensure that:

- RM decisions are based on objective market data
- SME segmentation is consistent

- Pricing and acquisition strategies are evidence-based

CQ becomes the **governance layer** that ensures:

- RM teams operate on **validated, unbiased market baselines**
- Portfolio steering is **data-driven, not anecdotal**
- Strategic decisions can be **justified to ExCo, Audit, and regulators**

UNDER THE HOOD

Sub-Processor Registry: Best-in-Class Transparency

Two structured tables – core infrastructure and development/support – cover all 6 providers with legal entity, jurisdiction, purpose, data categories, residency, certifications, sub-processor chain, safeguards, DORA criticality rating, and exit/substitutability analysis. The Statement of Completeness explicitly confirms no analytics processing sub-processors, no external data enrichment, no ML model hosting, no observability vendors, and no deferred disclosures. This level of proactive transparency is rare in vendor submissions.

DORA Article 19 Incident Data Pack: Fully Specified

The seven-component incident data pack (classification, impact assessment, root-cause analysis, mitigation actions, recovery timeline, communication log, evidence bundle) matches a bank's own DORA Article 19 regulatory filing. This 'reduces DORA compliance effort by 2-3 weeks' and resonates with a bank's compliance team, which typically assembles this pack manually under time pressure during a live incident.

PCI DSS: QSA Statement Embedded

The QSA-validated scoping statement is quoted verbatim and referenced as a Phase 2 deliverable in the implementation plan. The verbatim quote – confirming no cardholder data storage, processing, transmission, or access – gives the bank's InfoSec team exactly what they need to close the PCI scope question without further correspondence.

SLA Schedule: Contractually Complete

99.9% uptime over a rolling 30-day window, maintenance exclusion (4 hours/month, 72-hour notice), p95 and p99 latency commitments, a five-band service credit table, per-incident DORA-aligned credit triggers, real time monitoring, and monthly/quarterly reporting. A per-incident clause (60-minute threshold) triggers 5% credit and DORA notification.

IN SUMMARY

CQ IS A GOVERNANCE CONTROL THAT TRANSFORMS FRAGMENTED INTERNAL DATA INTO A REGULATOR-SAFE, AUDITABLE, CROSS-BANK MARKET-SHARE BASELINE, REDUCING MODEL RISK, COMMERCIAL MISCALIBRATION, AND REGULATORY EXPOSURE.