TECHNICAL BRIEF

# FSCS SCV Reporting: Security & Architecture Considerations

macro global®
creating value through innovation

SA SF

# Table of Contents

# Introduction

FSCS Single Customer View (SCV) reporting is a depositor-protection capability. In a firm failure scenario, firms must be able to produce an accurate SCV file and Exclusions View so the FSCS can determine eligible deposits and support timely compensation. In practice, SCV readiness is an operational test: can the institution deliver complete, defensible outputs under time pressure with a clear audit trail?

Many institutions still rely on spreadsheet-led aggregation and manual intervention across fragmented source systems. Under stress, manual fixes create key-person dependency, weaken data lineage, and increase the likelihood of inconsistent outputs - all of which reduce audit defensibility.

When supervisory expectations tighten, organisations face increased scrutiny on data accuracy, eligibility marking, and the ability to run SCV on demand. Weak controls can trigger remediation programmes, heightened audit attention, and reputational damage.

A modern SCV approach combines controlled data ingestion, rule-driven validations, controlled matching, and secure handling of depositor identifiers — supported by evidence packs (logs, exceptions, remediation, and approvals) that stand up to audit and supervisory review.

This technical brief summarises the security, architecture, and automation controls required to modernise SCV delivery—from extraction and transformation to validation, reconciliation, output generation, and evidence capture—so SCV becomes a repeatable BAU capability.

# Objectives

Macro Global aims to improve the efficiency, accuracy, and security of the banking industry's Single Customer View reporting process. The initiative's objectives are as follows:

- **Automate the FSCS SCV Reporting Process:**
  Automate the end-to-end SCV and Exclusions View pipeline to reduce manual intervention, support on-demand runs, and improve cycle time—without ‘fixing data in flight’.

- **Improve Data Quality & Integrity:**
  Use AI-powered data validation technologies to assure the integrity and correctness of customer data. The system will use powerful algorithms to discover and fix inconsistencies, duplication, and errors in the data, offering a more dependable perspective of customer interactions and improving overall data quality.

- **Security Controls by Design:**
  Protect sensitive depositor data in transit and at rest using encryption, access controls, and secure authentication. Apply safe input handling and threat protections (e.g., rate limiting, CSP) to protect platform integrity and availability.

# Objectives

- **Improve Integration with Core Banking and Adjacent Systems:**
  Support controlled ingestion from core banking and related systems using standard interfaces and repeatable extraction patterns, enabling consistent aggregation and reconciliation across sources.

- **Support Governance and Audit Expectations:**
  Create a controlled pipeline with logs and evidence of validations, reconciliations, remediation actions, and approvals so outputs can be defended during internal audit, external audit, and supervisory review.

# Technological Challenges and Gaps in Existing Systems

The development of Macro Global's FSCS SCV (Single Customer View) Reporting Solution faced a variety of technological challenges. These challenges highlighted significant gaps in existing systems and emphasised the complexities involved in creating an integrated and secure reporting framework. Here's an analysis of those challenges and gaps:

## Complex Key Management

**Challenge:**

Implementing hybrid encryption using AES and RSA required complex key management processes. This brought about potential security risks due to the intricacies of generating, storing, and rotating encryption keys. Performance overhead was also a concern.

**Gap in Existing Systems:**

Many legacy systems lack robust key management capabilities, exposing organisations to risks related to key exposure, misuse, or loss.

## Compatibility Issues

**Challenge:**

Updating various frameworks and libraries, such as Bootstrap, resulted in compatibility problems with existing code and third-party dependencies.

**Gap in Existing Systems:**

Legacy applications often do not support modern libraries or frameworks, making upgrades challenging and sometimes leading to software stagnation.

## Data Sanitisation

**Challenge:**

Achieving comprehensive data sanitisation while preserving data integrity proved difficult, with the risk of over-sanitising, which could lead to loss of essential data distinctions.

**Gap in Existing Systems:**

Many existing data processing systems do not have tailored sanitisation methods, resulting in either excessive data loss or vulnerabilities.

## Rate Limiting for Email Flooding Attacks

**Challenge:**

Preventing email flooding attacks required sophisticated rate-limiting algorithms and infrastructure changes that complicated system architecture.

**Gap in Existing Systems:**

Existing systems often have basic or insufficient rate limiting, making them vulnerable to abuse and attacks.

## Content Security Policy

**Challenge:**

Configuring an adequate Content Security Policy was complicated by diverse browser compatibilities and complex setups.

**Gap in Existing Systems:**

Lack of uniformity in content security policies across different systems leads to vulnerabilities, making them susceptible to content injection attacks.

## HTML Injection and XSS Protection

**Challenge:**

Protecting against HTML injections and XSS attacks required stringent input validation and significant refactoring of legacy code.

**Gap in Existing Systems:**

Many older systems lack thorough input validation mechanisms, rendering them vulnerable to attacks that exploit unsuspecting user inputs.

## Integration of Microsoft Single Sign-On

**Challenge:**

Integrating Microsoft SSO necessitated significant changes to authentication flows and data handling mechanisms.

**Gap in Existing Systems:**

Existing systems often do not accommodate modern authentication methods like SSO, leading to a fragmented user experience and increased security risks.

# Systematic Approach of Macro Global to Address Technological Challenges

Macro Global’s R&D team employed a systematic and structured methodology to address various technological challenges encountered during the development of their advanced financial solutions. This approach involved a combination of thorough analysis, strategic planning, and innovative implementation, ensuring effective and timely resolutions to complex issues. Below is a detailed overview of this systematic approach.

## Identifying Technological Limitations

### Comprehensive Analysis:

The initial phase involved a thorough assessment of existing technologies to identify gaps and inefficiencies. The team critically reviewed traditional systems and their limitations, particularly in areas like security, performance, and interoperability.

### Stakeholder Feedback and Requirements:

We engaged stakeholders including reporting, data, technology, risk and audit teams — to validate requirements, prioritise controls, and define what evidence must be retained (exceptions, remediation steps, and approvals). This input shaped validation rules, operational workflows, and the evidence pack structure.

# Systematic Approach of Macro Global to Address Technological Challenges

### Requirements Discovery:

Continuous review of supervisory expectations and industry patterns informed prioritisation of controls for accuracy, timeliness, security, and auditability.

## Design Principles

### Goal Definition:

Goals focused on reducing manual handling, strengthening security controls, and improving repeatability and audit evidence for SCV delivery.

### Operational Usability:

The design prioritised operator workflows exception triage, remediation, approvals, and reruns — so SCV can be executed reliably by BAU teams, not just specialists.

## Control-driven Automation

Implementation focused on automated validations, controlled matching, secure authentication, and encryption—supported by logging and evidence capture.

### Hybrid Encryption (AES + RSA):

The delivery team intended to combine modern encryption algorithms to provide strong data security. AES would offer efficient symmetric encryption for data at rest, whilst RSA would enable secure key exchanges and asymmetric encryption for sensitive data transit. This hybrid architecture would balance security and performance requirements, addressing complaints about standard encryption methods. Thus, this maintains a high standard of compliance and data security across the whole regulatory life cycle and secures your SCV output files with a sophisticated and highly encrypted authentication mechanism.

# Systematic Approach of Macro Global to Address Technological Challenges

## Automated Data Validations and Reconciliation:

To address concerns about data accuracy and integrity, the team implemented AI-powered data validation frameworks.

Automated checks run throughout the reporting cycle to flag duplicates, missing mandatory fields, inconsistent classifications, and linkage errors early—reducing late-stage remediation and rework.

Controlled matching logic supports identity resolution by grouping and linking customer records based on defined rules and thresholds. Matching and merge decisions should be traceable and reviewable.

Reconciliation should be repeatable and logged, producing an audit record of exceptions, remediation actions, and approvals before final file generation.

Reliable methods for checking various data points across numerous sources are provided via integration with reputable third-party databases, such as FCA DB, Companies House, Royal Mail DB, Charities Register, BFPO Address, and OFAC Sanction checks. This procedure intends to improve data accuracy, decrease fraud risk, and enhance business operations.

Moreover, third-party platforms provide a variety of integration possibilities, such as APIs for automated validation, bulk upload tools for large datasets, user-friendly web services, and batch processing for offline verification.

## Integration with Core Banking and Adjacent Systems:

In recognition of the necessity for seamless interoperability, the team developed a system that can be integrated with any primary banking system or external data sources, such as legacy platforms or Excel-based data.

Controlled ingestion patterns enable consistent aggregation across sources and simplify reconciliation between upstream systems and SCV outputs.

### Adapting Frameworks and Platform Components:

A controlled upgrade strategy reduces fragility and supports secure modern libraries without breaking core reporting workflows.

A modular architecture supports scheduled and on-demand reporting runs, reduces point-to-point integration complexity, and simplifies controlled change when reporting rules or upstream systems evolve.

# Tackling Scientific and Technological Uncertainties

Security-by-design requires protecting sensitive depositor data at rest and in transit, with controlled access, key rotation, monitoring, and secure operational processes. The following pages provide deeper engineering detail on encryption and key governance patterns used.

## Robust Key Management Practices

The delivery team acknowledged the importance of secure key management in hybrid encryption using AES for symmetric encryption and RSA for asymmetric encryption. AES offers excellent security and speed for encrypting consumer data during transmission, whilst RSA enables safe key distribution and authentication.

This combination assures that sensitive customer information such as customer ID, account number, aggregate balance, and other personally identifiable information,  is fully protected, solving important security and performance concerns in the financial industry.

They implemented strict access controls, allowing only designated personnel to interact with the key management system.

To further mitigate risks, the team adopted periodic key rotation protocols, ensuring that even if a key was compromised, the potential damage would be limited.

## Rigorous Testing and Refactoring for Compatibility

As the development of the SCV reporting system progressed, integrating modern frameworks and libraries such as Bootstrap led to compatibility issues with existing code and third-party dependencies. The delivery team understood that a seamless user experience relied on maintaining functionality across all components.

A meticulous and structured testing and refactoring process was adopted. Each component of the system underwent rigorous compatibility testing, which allowed the team to identify issues before they could escalate.

They employed an incremental upgrade strategy, carefully replacing outdated libraries with modern alternatives while ensuring that existing functionalities remained intact. This approach emphasised consistency and robustness in the system architecture.

## Custom Data Sanitisation Routines

The challenge of ensuring comprehensive data sanitisation, while simultaneously preserving the integrity of critical information, required a nuanced understanding of the data flow within the system. The delivery team explored how to balance these competing needs without incurring significant risks.

The team has developed an AI-Powered Data Validation approach to address data sanitisation challenges within the Single Customer View reporting framework. This approach uses advanced artificial intelligence algorithms to enhance data accuracy and reliability by identifying and correcting errors, inconsistencies, and duplicates.

The system uses machine learning models to classify data entries according to established rules and patterns, ensuring high data quality across multiple entry fields.

Real-time error detection minimise the risk of flawed data being incorporated into the SCV.

Inconsistencies are identified and corrected, with the system alerting users to inconsistencies and suggesting corrections based on learned patterns from historical data.

**Identity Resolution Support:** Matching logic can be used to detect duplicates and link related depositor records based on defined rules and thresholds. Matching outcomes should be traceable and reviewable.

Grouping and clustering techniques can help surface related records and reduce duplication. Where automated linking is used, thresholds, exceptions, and overrides should be logged for review.

## Dynamic Rate Limiting Algorithms

The need to protect the system against email flooding attacks led the delivery team to investigate rate-limiting solutions that would not impede legitimate user interactions. They recognised that effective rate limiting required a balance between security and usability.

The team developed dynamic rate-limiting algorithms that adjusted thresholds based on real-time user behavior and traffic patterns. By employing machine learning principles, the algorithms could identify anomalies in traffic and adapt accordingly.

This methodology enabled the system to respond proactively to potential attacks while maintaining a fluid and responsive user experience, demonstrating the team’s commitment to security without sacrificing usability.

## Comprehensive Configuration of Content Security Policy

Recognising the critical role of CSP in mitigating content injection threats, the team delved into the complexities of configuring this security measure. They faced the challenge of ensuring CSP compatibility across diverse browsers and environments.

The R&D team embarked on extensive testing of CSP configurations across various browsers to refine settings meticulously. They utilised tools to simulate different browser behaviors and evaluated how CSP rules reacted under various circumstances.

This exploratory testing process enabled the team to create a solid and adaptable CSP, thereby significantly reducing vulnerabilities while ensuring consistent functionality across platforms.

## Meticulous Input Validation for HTML Injection and XSS Protection

Understanding the risks posed by HTML injection and XSS attacks required a comprehensive review of the existing codebase, particularly focusing on input fields that were susceptible to user tampering.

The team employed a dual approach that combined rigorous input validation techniques with substantial refactoring of legacy code. They meticulously analysed existing user input paths and enhanced these with validation checks designed specifically to thwart injection attempts.

This proactive enhancement not only fortified the system against vulnerabilities but also set a new standard for input validation that would be integrated into future development efforts.

## Seamless Integration of Microsoft Single Sign-On

The R&D team understood that the success of this integration hinged on effective token management and session handling.

The team redesigned the authentication flow to accommodate SSO requirements, focusing on secure handling of authentication tokens and streamlined session management.

**Operational Usability:** Map user journeys for report operators so exception handling, remediation, approvals, and reruns are efficient and consistent. Usability reduces workarounds that can weaken control evidence.

# Technological Breakthroughs and Solution Development

## Hybrid Encryption

A hybrid approach combines symmetric encryption (e.g., AES) for bulk data with asymmetric encryption (e.g., RSA) for secure key exchange, balancing confidentiality and performance.

**AES:** Effective at encrypting huge volumes of data quickly. It uses the same key for encryption and decryption, making it ideal for data storage and bulk encryption processes.

**RSA:** Employs a pair of keys, such as a public key for encryption and a private key to decrypt, to securely exchange encryption keys, rather than directly encrypting big datasets.

**Integration:** The AES algorithm encrypts sensitive data during transmission, and the RSA algorithm subsequently encrypts the associated encryption key. Therefore, even if a hacker intercepts the encrypted data, they are unable to access it without the decryption key.

## Content Security Policy

The team used CSP to protect web apps from XSS attacks and data injection.

CSP is a security feature that controls how and where resources can be loaded in a web application. By setting a whitelist of content sources (e.g., scripts, styles), the danger of loading harmful content is reduced.

**Configuration:** HTTP responses include a CSP header that specifies permitted sources.

**Effectiveness:** By enforcing such criteria, even if an attacker discovers a means to inject code into the web application, the browser will only execute scripts from trusted sources.

## Microservice Architecture

The usage of a microservices architecture allows the FSCS SCV reporting system to be scalable and maintainable.

A microservices architecture divides a large application into smaller, independently deployable services that execute specialised functions. Microservices can be designed, implemented, and scaled separately.

In the SCV reporting system, real-time processing can surface run-time exceptions quickly for example, missing mandatory identifiers, duplicate customer records, or reconciliation breaks between upstream sources and SCV outputs. Exceptions are routed for remediation with traceable approval before final file generation.

## Automatic Reporting Processes

The team developed automated reporting technologies to make report generation and delivery more efficient.

**Data Aggregation:** Data from multiple sources is gathered, converted to assure consistency, and then combined for reporting using ETL (Extract, Transform, Load) procedures.

**Scheduled Tasks:** Automation tasks can be scheduled to be executed at predetermined intervals, guaranteeing that reporting is current without the need for manual intervention.

**Notifications:** Integrating alerting systems enables stakeholders to receive automatic notifications when reports are ready or abnormalities are spotted, hence improving responsiveness.

## User-Centric Design Enhancements

Improved design principles were used to increase user experience and accessibility.

**Personalised Dashboards:** The system architecture offers user-specific setups, allowing users to customise their dashboards with metrics, graphs, and reports that are relevant to them.

The successful development of the SCV reporting system yielded substantial improvements in efficiency, accuracy, and security. Below is the key performance indicators used to measure the project’s success:

# Impact of Technological Advancements

## Efficiency Enhancements

- **Increased Data Processing Speed:**
  SCV report generation time decreased by ~30% (e.g., from ~30 minutes to ~21 minutes). Results depend on upstream data quality, run configuration, and operating model maturity.

- **Reduced Error Rate and Exceptions:**
  Validation and reconciliation controls significantly reduced common reporting errors (e.g., missing mandatory fields, duplicates, and classification issues). Residual exceptions are managed through logged remediation and approvals.

## Accuracy Gains

- Rule-driven validations and controlled matching improved consistency of customer aggregation and reduced duplication in measured runs. Accuracy outcomes vary by source-system quality and remediation processes.

## Security Improvements

- **Reduced Security Incident Rate:**
  Security controls (encryption, access controls, safe input handling, CSP/rate limiting) reduced exposure to common attack patterns within the platform scope. Security outcomes depend on deployment posture and monitoring.

- **Enhanced Compliance Adherence:**
  The solution was designed to align with relevant data protection and security expectations. It supports firms in implementing governance over data, configuration, and operating controls; compliance remains the firm’s responsibility.

## Potential Cost Savings

- **Reduced Operational Costs:**
  Automation can reduce manual effort in data preparation, validation, and report generation, freeing capacity for exception handling and control oversight. Actual savings vary by baseline process maturity and adoption.

- **Reduced Costs of Errors:**
  Earlier detection of validation and reconciliation breaks can reduce rework and late-stage remediation. Financial impact depends on error rates, remediation effort, and governance processes.

- **Reduced Infrastructure Costs:**
  Optimised performance can reduce resource overhead, but costs depend on architecture choices, hosting model, and usage patterns.

## Risk Reduction

- Strong security controls reduce exposure to common risks, but residual risk remains and must be managed through governance, monitoring, and incident response.

# Conclusion

This technical brief summarised the engineering and security controls that support a more resilient approach to FSCS SCV reporting—automation, validation, secure data handling, and repeatable execution with evidence capture.

A controlled pipeline improves audit defensibility by retaining logs of validations, reconciliations, exceptions, remediation actions, and approvals—helping firms demonstrate how SCV outputs were produced.

For maturity benchmarking and budget justification, use the FSCS SCV Readiness Business Case (maturity model). For implementation guidance focused on 24-hour delivery and audit defensibility, publish the new ‘FSCS SCV 24-Hour Delivery Playbook’ as the primary conversion asset.

## Next Step:

Book a short technical discovery session to review your current SCV process, key risks, and a pragmatic modernisation path (automation, audit evidence, or both).

Speak to Our SCV Expert

# We are here to help you

macro global®

creating value through innovation

Please click on the web link below to access our sales desk telephone numbers and email and we will be in touch straight back to you.

https://www.macroglobal.co.uk/contact-us/

Microsoft Gold Partner

amazon web services | Partner Network

TECHNOLOGY PARTNER

ISO 9001:2015 Quality Management System
Cert. #: 0922900102

ISO 27001:2013 Information Security Management
Cert. #: 09222700102

ISO 27701:2019 Privacy Information Management
Cert. #: 09222770102

ISO 27018:2019 PII Protection in Public Clouds
Cert. #: 09222701802

Macro Global (MG) is the trading name of Macro Infotech Limited, Inca Infotech Ltd & Macro Technology Solutions Pvt Ltd. Macro Infotech Limited & Inca Infotech Limited have Registered Office at 25, Cabot Square, Canary Wharf, London – E14 4QZ and these companies are registered in England & Wales under the registration number 06477763 & 04017901.