

WHITEPAPER

Why FSCS Compliance Starts with IT












A Strategy Guide for CIOs & CTOs



macro global®
creating value through innovation



Table of Contents

	Introduction	01
	Deep Diving into Compliance and Infrastructure Readiness	02
	Anatomy of an FSCS-Ready Architecture	06
	CIO takeaway: SCV isn't a file export - it's a living data pipeline	10
	Cloud Adoption vs. On-Premises vs. Hybrid: Making the Strategic Choice	12
	Security and Resilience as the Building Blocks	15
	Integration and Legacy Challenges	18
	CIO's Toolkit - Emerging Tech for SCV Readiness	20
	Vendor Scorecard: How to Choose the Right SCV Partner	24
	The First 90 Days Plan for CIOs/CTOs	28
	Conclusion	31

Introduction

FSCS compliance has become a critical mandate for financial institutions, demanding strong IT resilience at both the operational and Board level, where both CIOs and CTOs are directly accountable. With the regulator's 24-hour SCV readiness requirement and seven-day payout mandate, even minor system weaknesses can expose institutions to fines, reputational damage, and regulatory intervention. Recent FSCS actions increasingly cite IT gaps, which are not just reporting failures as the root cause of non-compliance.

To survive this scrutiny, financial institutions need more than reporting tools. Compliance must be engineered into IT frameworks, validated data flows, automated reconciliation at source, and secure controls designed to withstand independent audits, disaster recovery tests, and Board-level drills. Manual workarounds or fragmented systems will not stand up to stress.

This guide equips CIOs and CTOs to embed compliance directly into infrastructure planning, align SCV reporting with enterprise data architecture, and adopt cloud and AI-driven resilience.

The outcome: SCV systems that are not just compliant, but regulator-ready by design.

Deep Diving into Compliance and Infrastructure Readiness

FSCS compliance ultimately depends on the strength of IT systems rather than policy statements. A policy may look sound on paper, but without resilient infrastructure, institutions cannot deliver an accurate SCV within 24 hours or complete payouts in seven days. Systems are the backbone of compliance because they ensure that depositor data is unified, validated, and retrievable under pressure. In short, it is IT, not documents, that regulators rely on when testing an institution's true readiness.

When regulators run FSCS drills, they go far beyond checking procedures.

They examine whether an institution's systems and infrastructure can stand up to stress, focusing on evidence-based outputs such as:

01

System readiness:

Ability to generate SCV files within mandated timelines.

02

Secure file transfer:

Ensuring depositor data can be moved safely and without breaches.

03

Error logs and reconciliation:

Visibility into mismatches, duplicates, or anomalies.

04

Audit trails:

Traceability of every data change and action.

05

SCV and Exclusions files:

Accuracy, completeness, and eligibility checks.

06

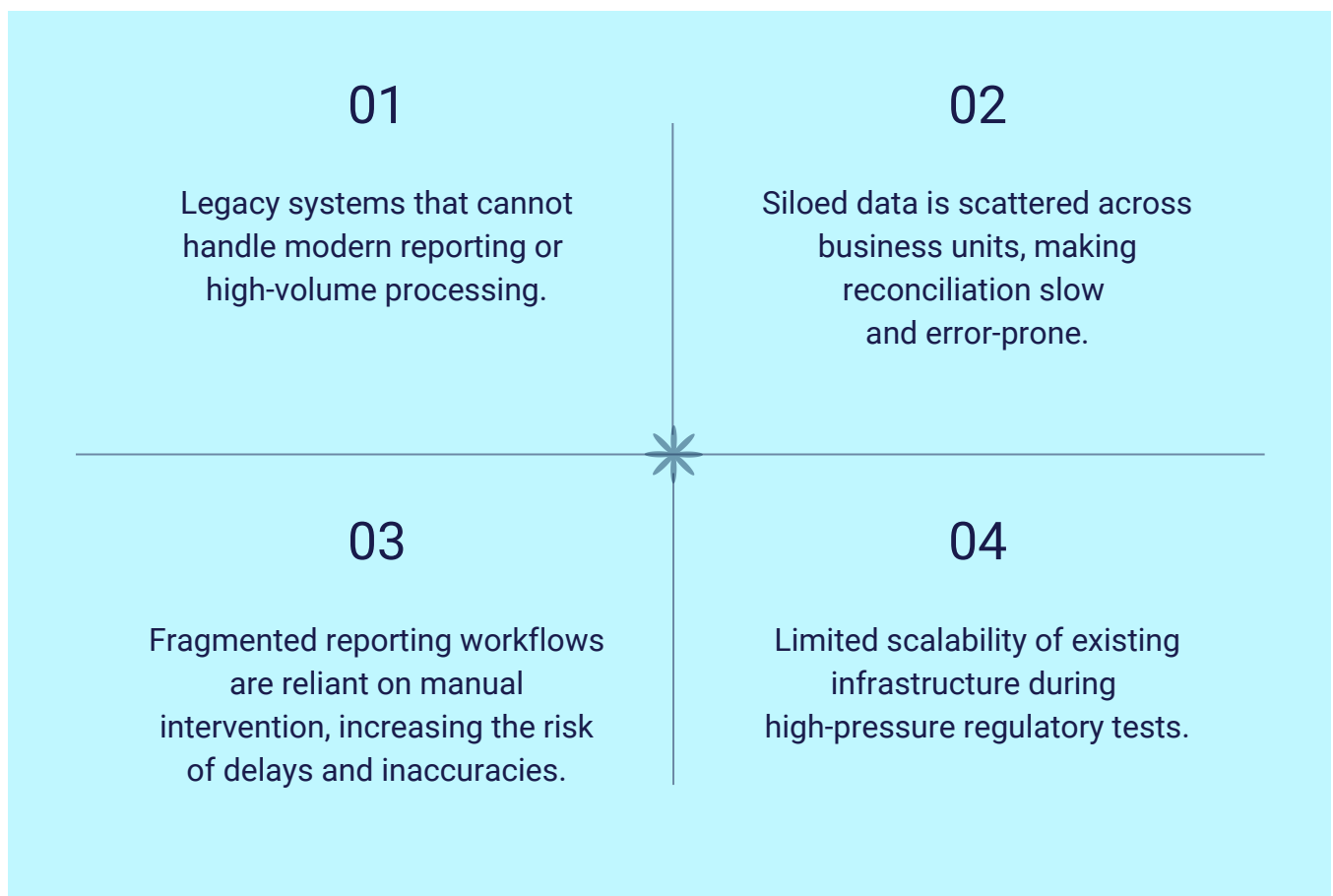
Annual Effectiveness Reports:

Backed by IT evidence, not just compliance narratives.

This is why firms need resilient, scalable, and audit-ready architectures that deliver compliance by design. Building such systems not only satisfies regulators but also supports broader digital transformation goals, ensuring that compliance readiness aligns with enterprise IT priorities such as agility, data integration, and cybersecurity.

Key Challenges Institutions Face

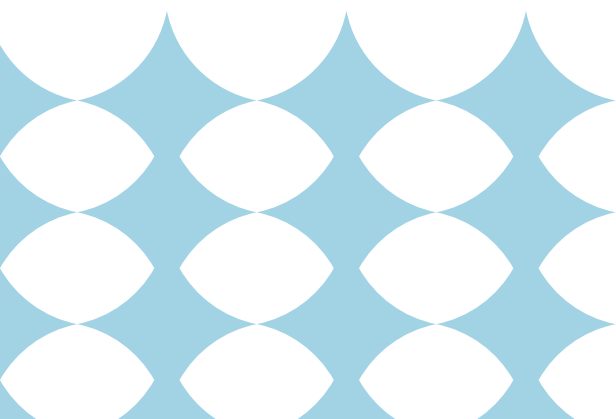
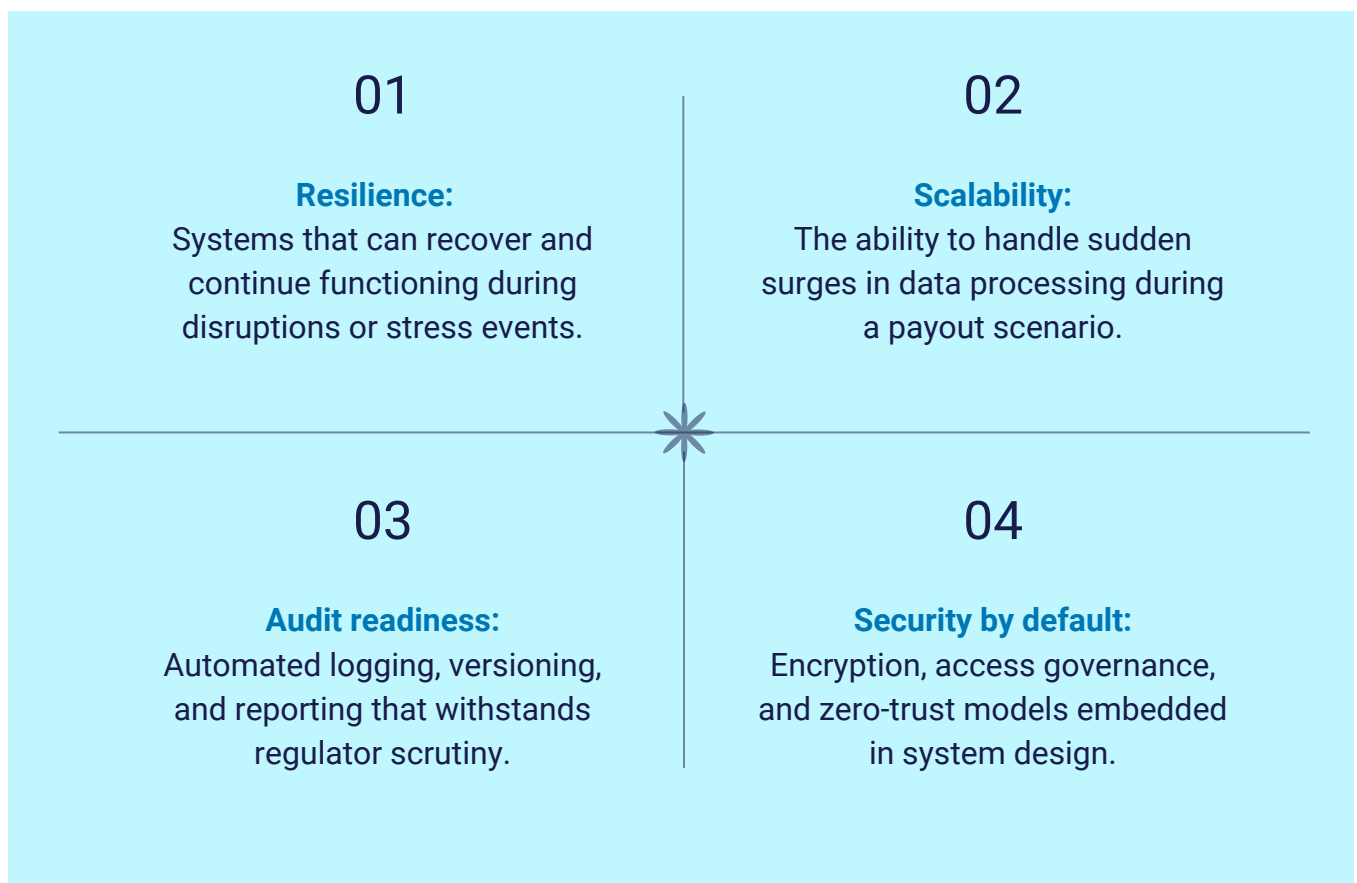
Many firms are constrained by systemic weaknesses that undermine FSCS readiness, such as:





The Case for Resilient, Scalable, and Audit-Ready Architectures

To overcome these challenges, CIOs and CTOs must prioritise infrastructures that are built for compliance from the ground up. The essential qualities include:

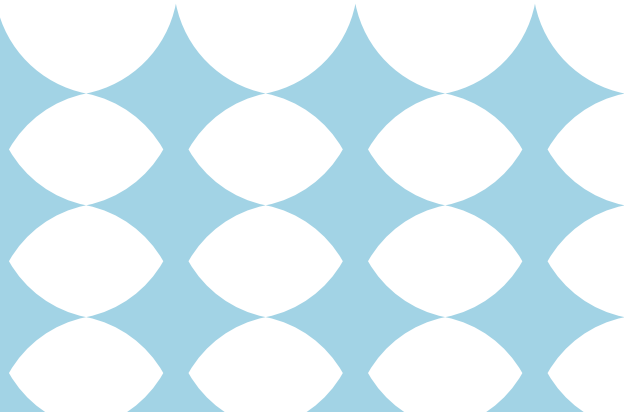
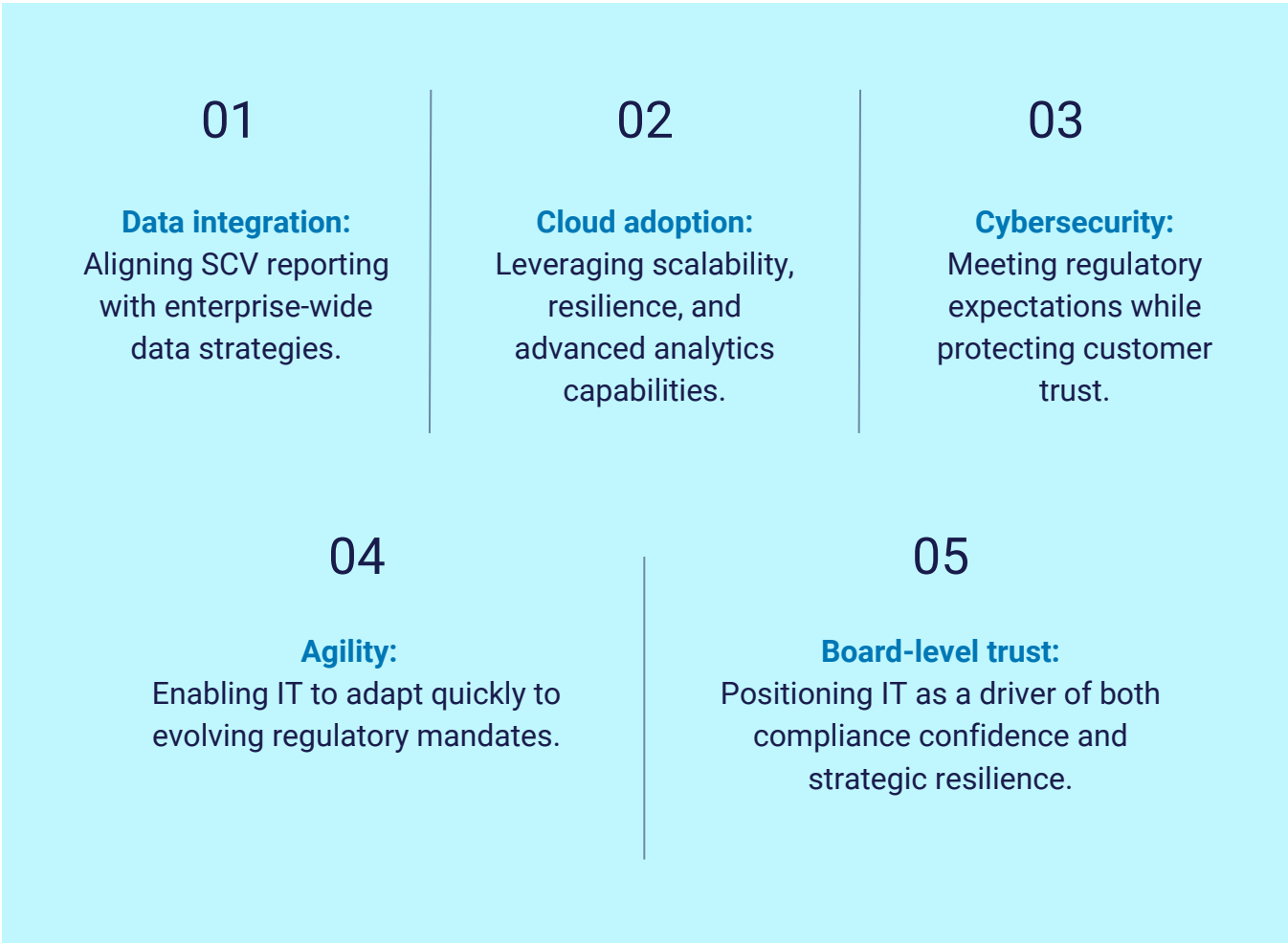




How FSCS Readiness Intersects with Digital Transformation

Designing for FSCS readiness does not sit apart from enterprise IT priorities—it directly complements them.

Forward-looking CIOs and CTOs recognise that compliance strengthens broader transformation goals, such as:



Anatomy of an FSCS-Ready Architecture

FSCS compliance has evolved over the years to now render resilience under a seven-day payout, which is considered the regulator's toughest test. To deliver with this precision and accuracy, the system demands an architecture built for accuracy, speed, and auditability, not after-the-fact patchwork.

A complete FSCS-ready system delivers more than just data pipelines and validation layers, but renders seamless data flow across silos, controls that hold under stress, and infrastructure that adapts as regulations shift.

It is also scaling as the blueprint for digital trust, where every layer is a governance layer, every checkpoint a risk control, and every design choice a message to regulators and boards that resilience is built-in, not bolted on.

Let us dissect each layer:

Data ingest layer

This layer unifies data from multiple enterprise sources to create a single foundation for SCV reporting.



Core Banking Systems (CBS):

Transaction and deposit records.



CRM Platforms:

Customer profiles and contact details.



KYC Repositories:

Identity verification and eligibility checks.



Payment Systems:

Deposit movements and balances.

By consolidating data at the source, the ingest layer ensures no customer record is overlooked and sets the stage for accurate downstream processing.

Validation and eligibility engine

Once data is ingested, it must be verified and processed against FSCS rules.



Deposit validation:

Ensuring balances are accurate and current.



Eligibility logic:

Marking deposits as covered or excluded.



Joint account handling:

Applying the correct rules for shared accounts.



Duplicate reconciliation:

Merging records to create a true single customer view.

Automating these checks reduces manual intervention and ensures compliance within regulator timelines.

Transformation layer

The transformation layer converts validated data into formats regulators require.



Schema mapping:

Aligning source data fields with FSCS reporting structures.



Exclusions handling:

Applying codes for legally dormant, sanctioned, or disputed accounts.



XML packaging:

Generating regulator-ready files in the mandated structure.

This layer makes the difference between raw data and regulator-compliant submissions, ensuring CIOs can deliver accurate SCV and Exclusions files on demand.

Secure transmission

Compliance is meaningless without data protection in transit.



SFTP/PGP encryption:

Secure transfer of sensitive depositor files.



Vaulting mechanisms:

Safeguarding files during staging.



Transfer logging:

Providing visibility and accountability for every movement.

This step demonstrates to regulators that security is embedded end-to-end, not an afterthought.

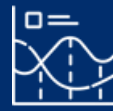
Audit & rollback

Every FSCS-ready system must prove that it can be trusted.



Version control:

Tracking changes to depositor records.



Drill logs:

Retaining regulator test results for future scrutiny.



Automated reconciliation:

Validating outputs against inputs.



Rollback mechanisms:

Recover quickly if errors are detected.

These capabilities provide confidence under audit and enable institutions to demonstrate continuous compliance.

CIO takeaway: SCV isn't a file export - it's a living data pipeline

To stay compliant and resilient, firms must treat SCV as an “always-on” capability that keeps evolving with regulatory and business needs.

Let's break down what that means in practice:

01

Continuous ingestion, not one-off extracts:

Depositor data must be refreshed in near real-time, capturing changes in accounts, beneficiaries, and KYC status without manual lag.

02

Built-in validation at source:

Errors, duplicates, and eligibility mismatches need to be flagged at entry, not discovered during drills.

03

Automated transformation logic:

Schema changes, eligibility rules, and product mappings should be adaptable without full rebuilds or vendor escalations.

04

Always-on security:

Encryption, RBAC, and zero-trust frameworks protect the pipeline at every handoff, not just the final output.

05

Audit by design:

Every data touchpoint leaves a traceable log, enabling drill evidence packs and regulator confidence without scrambling.

06

Resilience baked in:

Failover and disaster recovery tested against the seven-day payout clock, not theoretical RTO/RPO values.

07

Board-level reporting:

CIOs must be able to surface SCV health through dashboards, BI layers, and real-time readiness scores.

08

Scalable architecture:

Capable of absorbing new FSCS mandates, cross-border compliance, or new product lines without disruption.

09

Culture shift:

Frontline data stewards and senior leaders are both accountable for SCV accuracy, turning compliance into a shared, ongoing responsibility.

Cloud Adoption vs. On-Premises vs. Hybrid: Making the Strategic Choice

For FSCS readiness, the choice of infrastructure cloud, on-premises, or hybrid can determine how effectively an institution meets regulatory expectations.

While each approach has its merits, CIOs and CTOs increasingly recognise that cloud adoption provides unmatched resilience, scalability, and compliance agility.

Key Questions for CIOs/CTOs Before Choosing an Approach

When deciding on the right model, IT leaders should ask:

- **Data sovereignty:** Where will depositor data reside, and is this aligned with regulatory requirements?
- **Vendor lock-in:** Can the institution switch providers if needed, or is flexibility compromised?
- **Cost governance:** Are operational costs predictable and sustainable at scale?
- **Disaster recovery alignment:** Does the model support rapid failover and business continuity?

Why Cloud Adoption Leads the Way

Cloud adoption is increasingly the default choice for regulators, collaborators, and forward-looking institutions.

Its advantages include:

- **Resilience by design:** High availability, automated failover, and redundancy across geographies.
- **Scalability on demand:** Capacity to handle data surges during FSCS drills or payout events.
- **Advanced analytics:** Seamless integration with AI/ML tools for validation, anomaly detection, and risk monitoring.
- **Cybersecurity strength:** Enterprise-grade encryption, continuous monitoring, and shared responsibility frameworks.
- **Regulatory alignment:** Many regulators are themselves shifting operations to the cloud for transparency and efficiency.

By enabling faster, more secure, and regulator-aligned compliance, the cloud makes FSCS readiness not just achievable but sustainable.

Why On-Premises Still Has a Role

Despite the shift to cloud, on-prem remains relevant in certain scenarios:

- **Data sovereignty restrictions:** Jurisdictions that mandate depositor data remain physically on-site.
- **Legacy dependencies:** Institutions deeply tied to existing infrastructure may find cloud migration complex.
- **Direct control:** IT teams retain full authority over hardware, security settings, and system customisation.

For some firms, on-premises provides comfort and control, though it often comes at the expense of scalability and agility.

Why Hybrid Models Offer Balance

A hybrid approach blends the resilience of cloud with the control of on-prem. This model is attractive when:

- Certain workloads (e.g., depositor eligibility checks) must remain on-prem for compliance.
- High-volume reporting or AI-driven anomaly detection benefits from cloud scalability.
- Institutions want flexibility to scale without a full migration.

Hybrid architectures allow CIOs to **balance agility with sovereignty**, though they require careful integration and governance.

Considerations for All Models

Regardless of the chosen path, CIOs must plan around:

- **Migration strategy:** Ensuring minimal disruption while moving workloads.
- **Vendor risk management:** Assessing long-term reliability of providers.
- **Cost governance:** Preventing cloud sprawl or unchecked infrastructure expansion.
- **Security by default:** Encryption, access control, and monitoring across environments.

Security and Resilience as the Building Blocks

Regulators actively simulate outages, request instant SCV/Exclusion files, and drill institutions on the operational integrity of IT systems. Recent FSCS findings increasingly cite IT system weaknesses, unencrypted transmission channels, incomplete audit logs, and recovery lags over traditional reporting lapses.

This shift means CIOs and CTOs now hold the compliance lever, along with the infrastructure, which determines whether you can meet the 24-hour SCV readiness and seven-day payout mandate.

Let us deep dive into each factor that strengthens the Security and Resilience:

Cybersecurity

A robust SCV architecture must enforce defense-in-depth, protecting data from ingestion to reporting:

- ➔ **Data-in-Transit & Data-at-Rest Encryption:**
Depositor data must be encrypted at all times, AES-256 for storage, TLS 1.3/SFTP with PGP tunnels for transfers, and HSMs to safeguard key lifecycle management.
- ➔ **Zero-Trust & Access Governance:**
Access should never be assumed. Every user and device must be continuously verified, with RBAC tied to enterprise directories, and just-in-time provisioning with session recording to minimise insider risk.
- ➔ **Insider Threat Mitigation:**
Privileged sessions should run through PAM vaults with full capture, SCV directories must sit under strict DLP policies, and anomaly detection should automatically flag suspicious user activity.

Resilience

Resilience in FSCS is completely about proving that systems can withstand disruption and still deliver SCV outputs within payout deadlines.

- **Disaster Recovery Aligned to FSCS SLA:**
CIOs must design recovery against regulatory clocks, not just business norms. That means SCV and core banking engines were restored within four hours, with near-zero data loss through continuous replication, and active-active clustering across regions so failures don't interrupt depositor protection.
- **Failover and Continuity Design:**
Continuity must be automatic and invisible to operations. Hot standbys with orchestrated failover, mirrored SCV databases, and pre-tested load scenarios ensure SCV files are generated without degradation even under pressure.
- **Regulatory Stress Testing:**
Regulators won't just trust architecture diagrams — they simulate crises. Corrupted files needing rollback, throttled networks delaying transfers, or demands for file regeneration inside 12 hours are common drills. Firms that can withstand these tests without manual firefighting prove true FSCS resilience.

Auditability and Immutable Evidence

Regulators expect hard evidence. FSCS-ready systems must leave an immutable trail that proves every step of depositor data handling.

- **Comprehensive Audit Logging:**
Every SCV export should be cryptographically hashed and digitally signed, with logs preserved in tamper-proof WORM storage. Cross-system reconciliation, from source systems to SCV transformations, ensures regulators see integrity, not assumptions.
- **Rollback & Error Traceability:**
Pipelines must be version-controlled so errors can be reversed without corruption. Point-in-time restoration of depositor records and auto-exported drill logs gives regulators visibility into both prevention and recovery.

→ **Annual Effectiveness Evidence:**

Boards and auditors need proof at scale. Dashboards that auto-generate readiness status, archived system snapshots for drills, and end-to-end lineage tracing from CBS through KYC to final FSCS XML.

SCV Forza's immutable audit trail and rollback engine move compliance from defensive to proactive, giving CIOs a defensible, evidence-first position in front of both regulators and Boards.

The Fear Factor: Cost of IT Weakness

FSCS fines increasingly cite inadequate IT resilience:

- Insecure depositor data transmission.
- Delayed payouts due to disaster recovery gaps.
- Missing or corrupted audit logs during drills.

Each of these can cost millions in fines plus reputational damage, all because of IT failures, not compliance team lapses.

Integration and Legacy Challenges



For most institutions, the real bottleneck in SCV readiness lies deep in the integration. Legacy core banking systems were never designed to produce FSCS-ready files. Data is often scattered across CBS, CRM, KYC, and payments systems, each with its own format and logic. When these silos remain untouched, SCV files end up incomplete or inconsistent, no matter how strong the reporting tool is.

Common Pain Points

- Legacy CBS that can't natively generate efficient SCV outputs.
- Siloed data across systems that never truly “talk” to each other.
- Manual reconciliation steps slowing down readiness.

Options to De-risk Integration

- **Data Harmonisation:** Use integration frameworks to pull CBS, CRM, and KYC data into a single golden record.
- **ETL Mapping Templates:** Standardise transformations to save months of engineering effort.
- **Schema-Diff Tools:** Continuously check whether your data still aligns with FSCS schema updates.
- **Partner-Led Support:** At MG, we work hands-on with your IT team to map datasets, plug gaps, and align with a proven reporting structure.





The Risk of Ignoring This

Institutions often fail PRA/FSCS mock drills not because the SCV report is inaccurate, but because the data never flowed fast enough to generate it.

When integration is weak, the entire SCV pipeline the following challenges occur:

When integration gaps are overlooked, the consequences are serious and multi-dimensional:

- **Drill Failure Despite Good Reports:** Even accurate SCV logic won't help if core data flows are too slow or incomplete to deliver files within the PRA/FSCS deadlines.
- **Compliance Exposure:** Weak integration means exclusions, duplicates, or missing attributes slip through unnoticed, exposing the firm to regulator penalties.
- **Operational Fragility:** Manual workarounds create dependency on a few individuals. If they're unavailable, the SCV pipeline collapses under drill conditions.
- **Reputational Risk:** Failure to produce files on time damages market confidence and draws heightened supervisory scrutiny.
- **Wasted Investments:** Firms often spend on flashy reporting tools, only to discover integration gaps make those tools ineffective.



CIO's Toolkit - Emerging Tech for SCV Readiness

As FSCS expectations expand, CIOs and CTOs need an adaptive technology stack that can withstand scrutiny, scale with depositor growth, and evolve as regulations mature. Emerging technologies, if deployed carefully, provide both the resilience and explainability regulators demand, while also giving Boards visibility into the true state of SCV readiness.

AI/ML for SCV Data Integrity

AI/ML is reshaping supervisory oversight, and firms that use it responsibly gain a first-mover advantage in SCV readiness.

Core Use Cases

- **De-duplication:** AI models can spot duplicate depositor accounts across CBS, KYC, and third-party sources, ensuring clean and unified records.
- **Anomaly Detection:** Machine learning flags irregular balances, mismatched eligibility, or dormant-to-disputed shifts before they become regulatory flashpoints.
- **Eligibility Logic Automation:** Dynamic application of PRA/FSCS rules allows records to be validated at scale, reducing manual intervention and error rates.
- **Audit Trail Gaps:** Black-box ML can create non-reproducible results, making transparent audit trails critical for regulator confidence.
- **Explainability Challenges:** Supervisors demand “why” alongside “what” models must show clear decision paths to stand regulatory scrutiny.



CIO Guidance

- **AI/ML:** AI/ML is now central to SCV readiness, from de-duplication of depositor records to anomaly detection and dynamic eligibility logic. However, CIOs must balance adoption with control, as risks include audit trail gaps and explainability challenges.
- **Controlled Measures with Audit Versioning:** CIOs and CTOs should ensure that every SCV pipeline change is captured, versioned, and reversible.
 - ↘ Automated versioning with rollback capabilities.
 - ↘ Immutable, hash-signed audit logs.
 - ↘ Clear separation of test vs. production pipelines.
 - ↘ Drill reports automatically archived as regulator-ready evidence.
- **Dashboards & BI:** Real-time dashboards give visibility into validation status, drill simulations, and bottlenecks, enabling leadership to act on facts, not assumptions.
- **Simulation-as-a-Service:** Institutions can test SCV readiness on demand, simulating PRA/FSCS drills without waiting for formal audits.
- **Futuristic Compliance Architecture:** Next-gen compliance systems must go beyond today's patchwork. CIOs should prioritise:
 - ↘ Data integration and cleansing.
 - ↘ High-volume processing and reporting.
 - ↘ Immutable audit trails with explainability.
 - ↘ Infrastructure designed to evolve with FSCS mandates.
- **Market Gap:** Most vendors under-deliver in resilience and automation. This gap is a chance for CIOs to demand stronger capabilities and shape vendor roadmaps.



Dashboards & BI for Real-Time Assurance

Static reporting is no longer enough for FSCS readiness. CIOs require live, interactive visibility to pinpoint gaps and demonstrate compliance maturity.

- **Validation Status Dashboards:** Track depositor record readiness in real time, flagging exclusions, errors, and data quality issues before they escalate.
- **Drill Simulation Heatmaps:** Visual overlays highlight stress points and performance bottlenecks during mock runs, helping teams strengthen weak links ahead of regulator drills.
- **Board-Ready Reporting:** Automated MI packs consolidate key metrics, offering Boards and regulators a clear, evidence-backed view of SCV compliance progress.

Simulation-as-a-Service

Waiting for PRA/FSCS to initiate a drill is reactive. CIOs should take control by testing their own resilience under regulator-grade conditions.

- **Proactive Stress Testing:** Simulate 24-hour SCV readiness and seven-day payout scenarios.
- **What-if Modelling:** Test failures in CBS ingestion, file corruption, or delayed transfers.
- **Evidence for Regulators:** Demonstrate preparedness with logged simulation results.

Futuristic Compliance Architecture

FSCS rules keep changing, so IT systems must be built to adapt. CIOs should design infrastructure where compliance comes by default.

- **Data Integration & Cleansing:** Bring CBS, CRM, and KYC data together into one clean record.
- **High-Volume Processing:** Handle millions of depositor records quickly and reliably.

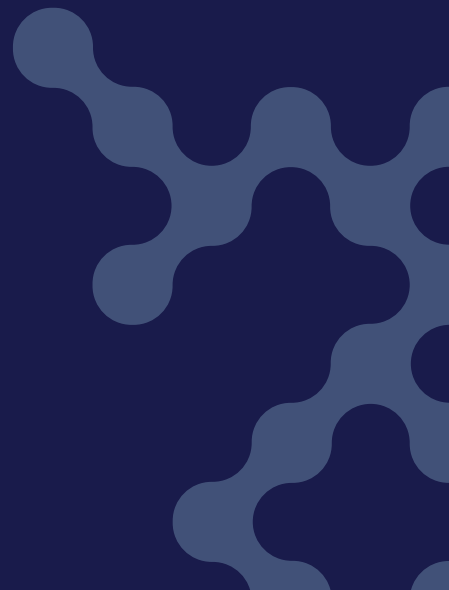


- **Automated Reporting:** Produce FSCS XML files with built-in checks and reconciliation.
- **Audit Trails:** Keep tamper-proof logs of every change and submission.
- **Explainability Layer:** Show clear reasons behind every SCV eligibility flag for regulators.

Market Gap: Time to Demand More

Most SCV vendors still fall short of what regulators and banks expect:

- **AI Explainability:** Models give outputs without showing how decisions are made.
- **Dashboards:** Often clunky, siloed, and lacking real-time integration.
- **Drill Readiness:** Focused on fixing issues after the fact instead of providing proactive resilience.
- **Audit Trails:** Fragile logs that don't stand up under regulator scrutiny.



Vendor Scorecard: How to Choose the Right SCV Partner

Selecting an SCV partner is a regulatory survival decision. The right vendor must balance reg-tech compliance, IT resilience, and cost discipline.

Must-Have Product Features

01

Schema Agility:

Adapt instantly to new FSCS/PRA schema updates without re-engineering.

02

Automation-First Workflows:

Automate exclusions, reconciliations, and SCV reporting to cut manual risk.

03

Drill Simulator:

Run PRA/FSCS-style drills on demand, proving resilience without regulator intervention.

04

RBAC & Access Governance:

Enforce least-privilege access, segregation of duties, and traceability.

05

Immutable Audit Trails:

Cryptographically logged, tamper-proof change history with rollback.

06

Core System Connectors:

Pre-built APIs for CBS, CRM, KYC, and Payments to avoid costly bespoke builds.

Red Flags (Walk Away If You See These)

01

Vendor Lock-In:

Bundled modules forced into contracts you don't need.

02

Oversized Tier-1 Platforms:

Expensive, over-engineered stacks mismatched to your scale.

03

Opaque Pricing:

Hidden costs for schema updates, connectors, or seat-based licensing.

04

Excel-Heavy Automation:

Manual workarounds disguised as technology.



CIO/CTO Due Diligence Questions

01

How fast was your last FSCS schema update rolled out?

02

What % of drill preparation is fully automated vs manual?

03

If the PRA triggers a drill tomorrow, can you simulate readiness instantly?

04

Show me how audit logs capture overrides or corrections.

05

Do you provide pre-built CBS/payments connectors, or must my IT team custom-build them?



CIO Angle - The Decision Principle

01

Demand Modularity:

Pay only for what you need; scale functionality as mandates grow.

02

Insist on Transparency:

Clear, predictable pricing aligned to compliance workloads.

03

Think Beyond the Product:

Assess the vendor's roadmap, drill track record, and customer support maturity.

The First 90 Days Plan for CIOs/CTOs

The first 90 days determine whether IT leaders are simply reacting to drills or leading a resilient FSCS-ready institution. Here's a step-by-step roadmap, balancing technical execution with cultural ownership.

Phase 1: Days 1 – 30 - Discovery & Ownership

Focus: Build clarity, accountability, and quick trust.



Map SCV Data Flows: Trace depositor data across CBS, CRM, KYC, and payments. Identify weak attributes, missing fields, and manual dependencies.



Gap Analysis & Risk Log: Compare against FSCS schema, exclusions, and payout readiness. Document gaps in a CIO-owned risk register.



Cultural Kick-off: Position compliance as a business-wide responsibility. Nominate “SCV Ambassadors” in ops, compliance, and IT.



Quick Wins: Run small validations (duplicate detection, joint account logic) to show immediate results and earn leadership confidence.

Phase 2: Days 31–60 — System Hardening & Security

Focus: Convert insights into resilient, regulator-proof systems.

- **Secure Data Transmission:** Implement SFTP along with PGP encryption with end-to-end logging for SCV files.
- **Validation Harness:** Automate eligibility checks, error handling, exclusions, and version-controlled audit trails.
- **Zero-Trust Controls:** Apply RBAC, least-privilege policies, and encryption by default to eliminate insider risks.
- **Upskill & Embed Culture:** Train staff to review compliance in “data proof” terms, not just policy claims.

Phase 3: Days 61–90 Simulation and Board Readiness

Focus: Demonstrate regulator readiness and board-level assurance.

- **Dry-Run Drill:** Simulate a full FSCS call today. Test SCV along with Exclusions against the 7-day payout target.
- **Evidence Pack:** Compile SCV files, exclusions, secure logs, and audit trails into regulator-ready documentation.



Board Briefing: Present dashboards, heatmaps, and drill outcomes, turning compliance into an enterprise success story.



Feedback Loop: Schedule quarterly dry-runs to keep SCV living and continuously improving.

Outcome at Day 90

Result: CIOs/CTOs shift from reactive to proactive compliance leaders.



Ownership Secured: Compliance accountability sits with leadership, not last-minute firefighting.



Pipeline Resilient: SCV is secure, automated, and regulator-auditable.



Culture Embedded: Business leaders and IT speak the same language of data-driven compliance.

Conclusion

SCV compliance is no longer a back-office exercise. It's about building systems that are secure, resilient, and regulator-ready with encryption, zero-trust controls, disaster recovery rehearsed against the seven-day payout target, and data pipelines that stand up to audit trails. When CIOs and CTOs take ownership, compliance shifts from last-minute panic to a predictable, controlled process.

But technology alone is not enough. Culture is the multiplier. Leaders who speak in data terms, frontline teams who care about data quality, and decisions traceable to evidence, this alignment transforms SCV from a file submission to a business capability. Quick wins like small-scale simulations, ambassador programs, and cross-team upskilling build momentum and trust.

This is where Macro Global's SCV Alliance and SCV Forza bring depth and agility. Built with schema flexibility, automation, drill simulators, and compliance-first resilience, they empower financial institutions to deliver SCV on time, with confidence. With the right partner, SCV becomes more than regulatory reporting; it becomes a strategic advantage in resilience, governance, and customer trust.

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/>



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.