AFC FINTECH LTD · REGULATORY POLICY PAPER

THE UNRESOLVED INTERSECTION

Automated Compliance, Regulatory Fragmentation, and the Sovereign Governance Problem in the UK Payment Services Sector

OLUSHOLA OKE-DANIEL
Barrister and Solicitor of the Supreme Court of Nigeria
Founder and Director, AFC Fintech Ltd · Inventor, Sovereign Auditor

CONTRIBUTOR AND REGULATORY REVIEWER
Dr Kolawole Oyekan
Chief Regulatory Director, AFC Fintech Ltd · PhD (Law), University of Warwick

Regulatory Anchor: FCA PS25/12 · CASS 15 · Effective 7 May 2026
Published: April 2026 · fintechafc.co.uk · Version 1.0

AUTHOR'S NOTE

This paper follows from an earlier submission — 'The Unfinished Law: Why CASS 15 Cannot Work Without a Mandatory Certified CASS Safeguarding Officer' — in which the author argued that FCA PS25/12 creates a technically demanding daily compliance obligation without simultaneously mandating the appointment of a specially trained professional to discharge it. That argument stands. The present paper does not revisit it.

What this paper addresses is a problem that lies beneath the question of who operates the compliance system — a problem that becomes visible only when one examines not the practitioner's obligations but the legal and regulatory architecture within which those obligations are simultaneously imposed by four distinct regulatory regimes that were designed independently and have never been formally reconciled.

The claim advanced here is structural rather than practical: that CASS 15 automated compliance systems exist at the convergence of FCA safeguarding law, the UK General Data Protection Regulation, the FCA's operational resilience framework, and the Senior Managers and Certification Regime — and that when these four frameworks impose obligations that conflict, overlap, or create ambiguity in the context of automated compliance, neither the FCA, the ICO, nor any other authority has provided a governing hierarchy. There is no map for the intersection. This paper draws one.

The Sovereign Auditor — the automated compliance engine developed by the author and operated by AFC Fintech Ltd for CASS 15 daily safeguarding reconciliation — is cited throughout this paper not as a commercial illustration but as a technical and architectural reference point. It is one of the few systems in the United Kingdom whose design has been required to navigate the intersection described in this paper in practice rather than in the abstract. The governance questions it raises are not hypothetical. They are live.

The previous paper asked who will operate the machine. This paper asks who governs the machine itself — and discovers that the answer, presently, is no one.

ABSTRACT

The Financial Conduct Authority's Policy Statement PS25/12 introduces, with effect from 7 May 2026, a CASS 15 safeguarding framework that requires automated daily reconciliation of client money across approximately 900 UK Electronic Money Institutions and Payment Institutions. In constructing this obligation, the FCA has drawn on well-established CASS architecture from the investment-firm sector. What it has not done is acknowledge that the automated compliance systems through which firms will discharge this obligation occupy a regulatory intersection of formidable complexity — one in which the concurrent demands of CASS 15 itself, the UK General Data Protection Regulation (in particular Article 22), the FCA's operational resilience framework (and its emerging alignment with DORA), and the Senior Managers and Certification Regime impose obligations that have never been formally reconciled.

This paper argues that this unresolved intersection constitutes the most significant structural vulnerability in the CASS 15 implementation architecture. When an automated compliance system processes personal financial data to produce a legally consequential compliance determination, reviewed by a named Senior Manager using an ICT system subject to operational resilience obligations, the resulting regulatory exposure is not the sum of four separate compliance exercises. It is something qualitatively different: a convergence zone in which obligations from different legislative regimes can simultaneously require, permit, and prohibit the same operational decision. No regulator has yet published guidance on how firms should navigate this zone.

The paper draws on four bodies of regulatory analysis: the technical architecture of automated CASS 15 compliance systems; the Article 22 UK GDPR framework for automated decision-making and its application to compliance determinations; the FCA's operational resilience requirements under PS21/3 and their intersection with the

Digital Operational Resilience Act; and the accountability structure of the Senior Managers and Certification Regime when applied to automated compliance governance. It concludes by arguing that the UK requires a new regulatory instrument — a Unified Automated Compliance Governance Standard — that resolves the intersection, establishes a clear obligation hierarchy, and provides firms with a defensible governance architecture for automated CASS compliance. In the absence of such a standard, enforcement against firms for CASS 15 failures may itself raise questions of regulatory fairness.

The paper advances a fifth argument that deserves particular emphasis. It is the author's reasoned inference — drawn from the established commercial architecture of the RegTech sector and the economics of software delivery at scale — that the majority of automated CASS 15 compliance solutions currently being marketed and deployed will be cloud-hosted Software-as-a-Service platforms. If that inference is correct, and the author believes it is defensible as a working hypothesis, then a systematic and daily violation of UK GDPR data protection principles is being quietly embedded into the implementation of CASS 15 at sector scale. The personal financial data of hundreds of thousands of UK payment service customers — their account balances, transaction histories, and identities — is being processed daily through internet-connected commercial servers under the banner of regulatory compliance, without those customers' informed awareness and, in many cases, without the architectural safeguards that data sovereignty requires. The FCA has created the obligation. It has not specified the minimum technology architecture through which that obligation may lawfully be discharged. This silence is not neutral. It is a regulatory failure of the first order — one that will be recognised, eventually, by the ICO.

"A law that creates a compliance obligation through an automated system, without simultaneously governing the system through which

that obligation must be discharged, has not completed its regulatory architecture. It has merely begun it."

CONTENTS

1. Introduction: The Governance Problem Below the Surface

1.1 What the Surface Shows

When the Financial Conduct Authority published Policy Statement PS25/12 in August 2025, the dominant professional reaction was one of recognition. The compliance community understood, broadly, what CASS 15 required: daily automated reconciliation of client safeguarding accounts; monthly reporting to the FCA under SUP 16.14A; annual independent audit under SUP 3A; a retrievable resolution pack under CASS 10A. These were demanding obligations — more demanding, by an order of magnitude, than anything the payment services sector had previously been required to perform on a daily basis — but they were comprehensible. They were, at least in outline, tractable.

The professional response was therefore primarily operational: how do we build the systems, hire the people, and implement the processes that these rules require? Law firms published implementation checklists. Accounting firms published cost estimates. Technology vendors published product specifications. The conversation was, in the main, one of execution.

This paper does not dispute the importance of that conversation. Execution is the proximate challenge. But execution, in the CASS 15 context, depends on a prior question that has not yet been asked — or rather, has been asked and answered only in fragments by four different regulatory bodies whose answers are not, as this paper will demonstrate, consistent with one another.

1.2 The Question Beneath the Surface

The question is this: when a firm builds or deploys an automated compliance system to discharge its CASS 15 obligations — a system

that processes personal financial data, produces legally consequential compliance determinations, operates as critical ICT infrastructure, and generates outputs for which a named Senior Manager is personally accountable — which regulatory framework governs the design, operation, audit, and accountability structure of that system?

The honest answer, as this paper will establish, is: four of them, simultaneously, with no agreed hierarchy and no published guidance on what happens when they conflict.

> *The problem is not that the law is silent. It is that four laws are speaking at once, and no one has been asked to chair the conversation.*

The four frameworks in question are: FCA CASS 15 (which governs the compliance output and the audit trail); UK GDPR Article 22 (which governs the automated decision-making process and imposes specific constraints on its operation); the FCA's operational resilience framework under PS21/3 and its emerging alignment with the EU's Digital Operational Resilience Act (which governs the ICT system through which the compliance process runs); and the Senior Managers and Certification Regime (which governs the accountability of named individuals for the system's outputs). Each of these frameworks was designed independently. None of them was designed with the other three in mind. And none of them — individually or collectively — has been interpreted or applied to the specific context of automated CASS 15 compliance in any published guidance, case law, or regulatory statement.

1.3 Why This Matters More Than It Might Appear

The legal significance of this intersection is not merely academic. It has three concrete regulatory consequences that firms currently

implementing CASS 15 automated compliance systems face without guidance.

The first is the obligation conflict problem. In specific circumstances — described in detail in Section 7 — the simultaneous application of CASS 15 reporting obligations, GDPR Article 22 safeguards, operational resilience requirements, and SM&CR accountability standards can require a firm to take actions that are simultaneously mandated by one framework and potentially inconsistent with another. No regulator has acknowledged this possibility, let alone resolved it.

The second is the accountability gap problem. The SM&CR requires a named Senior Manager to be personally accountable for CASS 15 compliance. But when the compliance function is performed by an automated system, the precise contours of that accountability — specifically, what constitutes adequate oversight of an automated system, and what evidences that oversight — have never been defined. A Senior Manager who relies on an automated system for CASS compliance, and who follows all existing FCA guidance on oversight and governance, may nevertheless find that guidance insufficient to discharge their obligation when something goes wrong.

The third is the audit validity problem. The annual safeguarding audit required under SUP 3A will be performed by auditors who must assess a firm's CASS 15 compliance. But if the firm uses automated compliance tools, the auditor must assess not just the output but the governance of the tool itself — including its Article 22 compliance, its operational resilience classification, and the SM&CR accountability structure around it. The FRC is not expected to publish a final auditing standard for CASS 15 until 2027. Until that standard exists, audit firms are being asked to opine on a governance structure they have no agreed methodology for evaluating.

These three problems — obligation conflict, accountability gap, and audit validity — are the practical stakes of the theoretical problem this

paper describes. They are not future risks. They are present realities for every firm that deploys automated CASS 15 compliance today.

2. The Architecture of the Intersection: Four Regimes, One System

2.1 A Mapping Exercise

Before the conflicts can be understood, the terrain must be mapped. The four regulatory frameworks that converge on automated CASS 15 compliance are not of equal specificity or equal authority in this context. They approach the automated compliance system from different directions, ask different questions of it, and impose different standards upon it. What they share is the automated compliance system itself: the same software, the same data flows, the same decision process, and the same human beings who design, operate, and are accountable for it.

Framework	Primary Question Asked of the System	Governing Authority	Current Guidance Status
FCA CASS 15	Does the system produce a compliant, documented, accurate daily reconciliation output?	FCA	Final rules published PS25/12 (August 2025)
UK GDPR Article 22	Is the system's automated determination of compliance status a decision with legal or similarly significant effect, and if so, is there adequate human oversight?	ICO / FCA	No CASS-specific GDPR guidance published
FCA PS21/3 / DORA	Is the system classified as a critical or important ICT function? What are the resilience, testing, and incident reporting obligations?	FCA / PRA / DORA	PS21/3 (March 2021); DORA alignment consultation ongoing
SM&CR	Which named Senior Manager is accountable for the system's outputs, and what evidence of oversight is required?	FCA	No automated compliance system-specific SMF guidance published

2.2 Why the System Triggers All Four Simultaneously

A natural first response to the mapping table above might be that these frameworks address different aspects of the same system — and therefore that careful attention to each, in sequence, would produce a compliant outcome. This intuition is mistaken, and understanding why it is mistaken is central to this paper's argument.

The four frameworks do not address different aspects of the system. They address the same aspects of the system through different lenses. Consider a single operational act: the automated compliance system processes a firm's client account data and produces a determination that the firm is GREEN — fully compliant, no shortfall, no commingling, for the reconciliation date. This single output triggers all four frameworks simultaneously.

> **A single GREEN compliance determination:**
>
> **Under CASS 15:** It is the legally required daily output. Its accuracy is a compliance obligation. Its timing is mandated. Its format is prescribed.
>
> **Under UK GDPR Art. 22:** It is potentially an automated determination with legal effect — it tells a regulated firm whether it is in compliance with a regime that carries personal liability consequences. The data processed to reach it is personal financial data.
>
> **Under PS21/3:** It is the output of an ICT system that is arguably critical to the firm's regulatory obligations. A failure of the system on any given reconciliation day is a potential operational resilience breach.
>
> **Under SM&CR:** The Senior Manager named as responsible for CASS 15 compliance is personally accountable for this determination. Their liability attaches the moment the determination is issued — or fails to be issued.

The same act, the same output, the same moment. Four frameworks. Four sets of requirements. No published guidance on what happens when they point in different directions.

3. The First Dimension: CASS 15 and the Automated Determination Problem

3.1 What CASS 15 Requires of Automated Systems

FCA PS25/12 and the CASS 15 rules do not prohibit automated compliance systems. Nor do they explicitly endorse them. They require the outcome — a daily reconciliation, timestamped, documented, and evidenced — without specifying the method. This is, in one sense, regulatory pragmatism: the FCA is indifferent to whether a firm meets the reconciliation requirement through manual processes, spreadsheet calculations, or multi-agent analytical pipelines. What it requires is the output, and the audit trail.

The consequence of this output-focused approach, however, is that the internal architecture of automated compliance systems — the processing logic, the data sources, the decision algorithms, the escalation pathways — exists in a regulatory vacuum so far as CASS 15 itself is concerned. The rules say nothing about how reconciliation software must be designed, validated, tested, or governed. They say nothing about what constitutes adequate oversight of an automated system. They say nothing about what a firm must do if the automated system produces an incorrect determination — except that the firm will be treated as non-compliant from the moment any shortfall or commingling occurred, regardless of when the system failed to detect it.

3.2 The Accuracy Obligation and Automated System Failure

The accuracy obligation in CASS 15 is absolute in a manner that creates a specific and underappreciated risk for automated compliance. The rules are clear: if a shortfall exists, the firm is in breach from the moment of its existence. The automated system's function is detection — it does not create the shortfall, but it is the

mechanism through which the shortfall is identified and reported. If the system fails to detect a shortfall that exists — whether through a software error, a data feed failure, an incorrect algorithmic mapping, or a model that has not been updated to reflect a regulatory change — the firm is in continuous breach for every day the shortfall goes undetected.

The critical observation here is that the CASS 15 framework's absolute accuracy requirement implicitly demands a level of automated system governance — validation, testing, model risk management, error detection, and update protocols — that is entirely absent from the rules themselves. The obligation is imposed. The infrastructure for meeting it is assumed. The governance of that infrastructure is unaddressed.

> *CASS 15 requires accuracy from a machine it has never described, validated, or governed. The obligation is real. The governance framework for the obligation is invisible.*

4. The Second Dimension: UK GDPR Article 22 and the Limits of Human-in-the-Loop

4.1 Article 22: The Statutory Architecture

Article 22 of the UK GDPR — as it stands following the Data (Use and Access) Act 2024 — provides that data subjects have the right not to be subject to a decision based solely on automated processing that produces legal or similarly significant effects. The traditional analysis of Article 22 in a regulatory compliance context treats this provision as not directly applicable: the compliance determination is a determination about the firm, not about a data subject. It is, on this reading, a B2B compliance output, not a decision 'about' any individual.

This analysis is superficially plausible but analytically incomplete. It conflates the nominal subject of the determination (the firm's compliance status) with the functional subjects of the data processing that underlies it (the individual clients whose account data is processed, mapped, and reconciled to reach that determination). The determination that a firm is GREEN or RED is, necessarily, a determination that derives from processing the personal financial data of every individual client whose money the firm holds. Those individuals have not consented to that processing in the Article 22 sense. They have not been offered the right to contest the determination. They have not been told that an automated system processes their account data daily to produce a compliance output that determines whether their money is adequately protected.

4.2 The Client Data Processing Problem

The daily CASS 15 reconciliation processes, at minimum: the identity of every client account holder; the balance of every client account; the history of every transaction in and out of those accounts for the reconciliation period; and the cross-reference between internal records

and external bank statements. This is, unambiguously, the processing of personal data — and it is processed through an automated system to produce a determination. The question Article 22 raises is not whether the determination is 'about' the individual clients. It is whether the processing of their data in an automated determination process creates obligations that the firm has not discharged.

The ICO's guidance on Article 22 focuses on automated decisions that directly affect data subjects. But Article 22's reach extends to any automated processing that produces 'similarly significant effects' — a phrase that has not been interpreted in the specific context of CASS 15 compliance. The argument that an automated CASS compliance system might engage Article 22 is not fanciful. A determination that a firm is non-compliant could, in a downstream scenario, trigger regulatory action that freezes client accounts, restricts fund withdrawals, or initiates insolvency proceedings. These would be effects that are highly significant to the individual clients whose data was processed to produce the underlying determination.

4.3 The Human-in-the-Loop Solution and Its Limitations

The standard response to Article 22 concerns in automated compliance is the human-in-the-loop model. If a qualified human reviews and authorises every automated determination before it is issued, the determination is not 'solely automated' and Article 22's restrictions do not apply. This is the architecture adopted by the Sovereign Auditor: every compliance determination produced by the three-agent analytical pipeline is reviewed and formally authorised by Dr Kolawole Oyekan, Director and Chief Regulatory Director of AFC Fintech Ltd, before delivery to any client.

This architecture is legally sound as a solution to the Article 22 problem as currently formulated. But it raises a deeper governance question that Article 22 does not fully resolve: what are the minimum

standards for the human review that makes the determination 'non-solely-automated'? Article 22 requires human involvement — but it does not define what that involvement must consist of, what qualifications the reviewing human must hold, what information they must have access to, or what evidence of their review must be retained. In other words, the human-in-the-loop requirement is itself unspecified.

A reviewing human who clicks an 'approve' button on an output they have not read is technically human-in-the-loop. A reviewing human who has no legal qualification to interpret the CASS 15 rules they are being asked to validate is technically human-in-the-loop. Neither scenario is what the law intends, but neither is excluded by the law as written. The specification of what constitutes a genuinely meaningful human review is a regulatory gap that sits squarely at the intersection of GDPR and CASS 15 — and neither regulator has filled it.

> *The human-in-the-loop is the answer to Article 22. But Article 22 has never described what the loop must contain, or what the human must know in order to stand meaningfully inside it.*

5. The Third Dimension: Operational Resilience and the ICT Dependency Chain

5.1 PS21/3 and the Operational Resilience Framework

The FCA's Policy Statement PS21/3, published in March 2021, established the UK's operational resilience framework for financial services firms. Under this framework, firms must identify their important business services — those whose disruption would cause significant harm to consumers or market integrity — and set impact tolerances for the maximum disruption they would accept. They must then conduct mapping and testing exercises to demonstrate that those impact tolerances can be met even in severe but plausible disruption scenarios.

The critical question for CASS 15 implementation is whether the automated compliance system that performs daily safeguarding reconciliation constitutes an 'important business service' or a critical underlying resource within such a service. The answer has significant implications. If it does, the firm must subject it to the full operational resilience regime: impact tolerance setting, mapping, scenario testing, third-party dependency assessment, and annual self-assessment.

5.2 The Case That Automated CASS Compliance Is a Critical ICT Function

The author's analysis is that an automated CASS 15 compliance system very likely constitutes a critical ICT function for any firm that depends on it for its regulatory compliance. The reasoning proceeds as follows. Under CASS 15, the failure to perform a daily reconciliation is not merely an operational inconvenience — it is a regulatory breach. A firm that is unable to perform its CASS 15 reconciliation on any given business day is, for that day, non-compliant with a mandatory legal obligation. If the inability to perform the reconciliation derives from a

failure of the automated compliance system, then the system is a critical operational dependency for the firm's regulatory compliance.

This analysis engages the Digital Operational Resilience Act (DORA), which came into force for EU firms in January 2025. DORA imposes specific requirements on ICT systems classified as critical or important — including mandatory resilience testing, contractual requirements with third-party ICT providers, incident reporting obligations, and digital operational resilience testing protocols. The UK has not enacted DORA directly, but the FCA has signalled alignment with DORA's principles, and many UK payment firms with EU operations are subject to both frameworks simultaneously.

For firms using third-party CASS 15 compliance platforms — which will be the majority of the 900+ regulated firms, given the practical constraints on building proprietary solutions — the third-party ICT dependency chain creates a specific obligation stack. Under PS21/3, the firm must understand its dependencies and be able to demonstrate resilience. Under DORA (where applicable), the firm must have specific contractual provisions with the ICT provider. Under CASS 15, the firm is responsible for compliance regardless of whether the failure was its own or its technology vendor's.

> **The Third-Party ICT Dependency Chain — Four Obligations, No Single Resolution:**
>
> **CASS 15:** The firm is responsible for its compliance. Third-party system failure is not a defence.
>
> **PS21/3:** The firm must have mapped its dependency on the system and set an impact tolerance for its failure.
>
> **DORA (where applicable):** The firm must have contractual provisions requiring the vendor to support DORA compliance.
>
> **SM&CR:** The named Senior Manager is accountable for the firm's CASS compliance — including when the third-party system fails.

6. The Fourth Dimension: SM&CR Accountability and the Governance of Automated Outputs

6.1 The Senior Manager as the Human Locus of Accountability

The Senior Managers and Certification Regime operates on a principle of named, personal accountability. For any significant business function at a regulated firm, there must be a Senior Manager Function holder whose responsibility for that function is clearly allocated, documented, and evidenced. In the CASS 15 context, the FCA expects that a named individual will be personally accountable for the firm's safeguarding compliance — for the daily reconciliation, for breach reporting, for audit trail maintenance, and for the adequacy of the systems through which these obligations are discharged.

This principle is sound in a context where human beings perform the compliance function directly. It becomes significantly more complex when the compliance function is performed by an automated system. The question that SM&CR raises — but does not answer — is: what does it mean, in practice, for a Senior Manager to be personally accountable for the outputs of an automated compliance engine they did not design, do not fully understand, and cannot directly verify on a line-by-line basis?

6.2 The Oversight Standard for Automated Systems — A Regulatory Lacuna

The FCA's SM&CR guidance addresses the oversight of business functions performed by human beings and teams. It requires Senior Managers to have adequate oversight, to receive adequate management information, and to take reasonable steps to ensure that their area of responsibility operates in compliance with applicable

rules. None of this guidance was written with automated compliance systems in mind.

The consequence is that there is no published FCA guidance on what constitutes adequate oversight of an automated compliance system for SM&CR purposes. There is no guidance on what management information a Senior Manager should receive about system performance, accuracy rates, exception handling, or model updates. There is no guidance on what training or qualification a Senior Manager needs to oversee an automated system effectively. And there is no guidance on what happens when a Senior Manager's oversight was diligent — they reviewed the system's outputs, received appropriate management information, and made reasonable decisions — but the system was nevertheless inaccurate, and a breach resulted.

This is not a theoretical gap. It will be tested when the first enforcement action for CASS 15 non-compliance arising from an automated system failure occurs. At that moment, the question of what the Senior Manager should have done — and whether what they did was sufficient — will have to be answered. Currently, neither the Senior Manager nor their legal advisers have any published FCA guidance to point to.

> *The Senior Manager is accountable for the machine's outputs. The law has never told them what it means to adequately oversee a machine. When things go wrong, they will discover that accountability without a standard is the architecture of injustice.*

7. The Intersection in Practice: Where the Four Regimes Collide

7.1 Collision Scenario One — The Reporting Dilemma

Consider the following scenario. An automated CASS 15 compliance system detects, during its nightly reconciliation cycle, what appears to be a shortfall in one client's safeguarding account. The system flags it as AMBER — a condition requiring investigation before a final determination can be made. Under CASS 15, the firm has an obligation to notify the FCA without undue delay if it cannot immediately remedy or explain a shortfall.

Under UK GDPR, the automated flag constitutes a data processing output derived from personal financial data. If the firm were to notify the FCA of the apparent shortfall by including client-level data in its notification, it would be processing and sharing personal data. The question is whether it can do so on the basis of a legal obligation (CASS 15 reporting) without separately satisfying Article 22 requirements for any automated determination component of the output, and without ensuring compliance with data minimisation principles that might require the FCA notification to exclude personal identifiers.

The CASS 15 obligation says: notify without undue delay. The GDPR framework says: ensure your processing — including the automated detection and the regulatory notification — is lawful, necessary, and minimised. Neither framework tells the firm which takes precedence if they create tension. No published guidance addresses this scenario.

7.2 Collision Scenario Two — The System Failure During the Business Day

A firm's automated CASS 15 compliance system suffers an ICT failure at 07:00 on a business day. The daily reconciliation cannot be completed. The firm has three regulatory obligations pulling in

different directions simultaneously. Under CASS 15, it must complete the reconciliation and if it cannot do so, must report the failure to the FCA. Under PS21/3, it must activate its incident management procedure and may have an obligation to report the operational incident if it breaches an impact tolerance. Under SM&CR, the named Senior Manager must be notified and must take personal responsibility for the firm's response. Under GDPR, the system failure may constitute a personal data incident if client account data was inaccessible or at risk, triggering potential ICO notification obligations.

These four obligations are not sequenced. They arise simultaneously. They each have their own timelines, their own reporting authorities, and their own standards for what constitutes adequate response. A firm that reports to the FCA under CASS 15 without also considering PS21/3 incident management and ICO breach notification has not managed its regulatory exposure. A firm that does consider all four simultaneously, without guidance on how to prioritise and coordinate them, is doing so without a map.

7.3 Collision Scenario Three — The Algorithm Update Problem

A firm's automated CASS 15 compliance engine is updated by its software vendor to reflect a change in the FCA's interpretation of what constitutes 'adequate evidence' for safeguarding accounts under revised Approach Document guidance. The update changes the system's logic for flagging AMBER conditions. Before the update, certain account configurations were classified as GREEN; after the update, they are classified as AMBER.

Under CASS 15, the firm must ensure its reconciliation reflects current regulatory requirements — the update is therefore not only permissible but required. Under Article 22 GDPR, the change in automated determination logic constitutes a significant modification to an automated system producing outputs with potential legal

consequences — potentially requiring a new Data Protection Impact Assessment and re-evaluation of Article 22 safeguards. Under PS21/3, the update constitutes a material change to a critical operational system — potentially requiring change management procedures, testing protocols, and impact tolerance re-assessment. Under SM&CR, the Senior Manager responsible for CASS compliance should arguably be approving the system change before it goes live.

The same software update triggers four different governance processes under four different frameworks. No framework tells the firm what order to perform them in, or what happens if performing them in the required sequence takes longer than the regulatory timeline for implementing the underlying rule change.

8. The Cloud Architecture Problem: Data Sovereignty and the Systematic GDPR Risk in Market-Standard CASS Compliance Solutions

8.1 A Speculative Inference That the Evidence Makes Compelling

This section advances an argument that the author acknowledges is, in its specific claims, inferential. The FCA has not published data on the technical architecture of the CASS 15 compliance solutions that regulated firms are deploying. No sector-wide audit of compliance system design has been conducted. It is therefore not possible — at the date of this paper's publication — to state as empirical fact that any particular category of technology is dominant in the market.

What is possible — and what this paper asserts with confidence — is to reason from first principles about what the market is likely to have produced, and why. The argument proceeds as follows. The commercial software industry has, over the past two decades, converged almost entirely on a cloud-hosted, Software-as-a-Service delivery model. This convergence is not accidental. It reflects genuine economic advantages: lower marginal cost per customer, centralised infrastructure maintenance, rapid deployment, and subscription-based revenue that is predictable and scalable. RegTech, as a sub-sector of the software industry, has followed this trajectory. The compliance platforms that serve financial services firms — for AML monitoring, transaction surveillance, regulatory reporting, and now CASS 15 reconciliation — are, with very few exceptions, delivered as cloud-hosted SaaS.

It is the author's reasoned inference that the automated CASS 15 compliance solutions currently being marketed to the UK's 900+ regulated EMIs and PIs will, in the overwhelming majority of cases, be cloud-hosted platforms. This inference is grounded in three observable facts: the commercial architecture of existing RegTech vendors who

have extended their products to cover CASS 15; the cost and complexity barriers to on-premises or locally-processed solutions at the scale required; and the procurement preferences of regulated firms that lack the technical infrastructure to manage locally-hosted compliance systems. The author invites any reader with evidence to the contrary to present it. In the absence of such evidence, the inference stands.

> *If most CASS 15 compliance systems are cloud-based — and the economics of the RegTech sector make it highly probable that they are — then the daily compliance exercise that PS25/12 has made mandatory is simultaneously, and daily, processing the personal financial data of hundreds of thousands of UK customers through internet-connected commercial servers. The FCA does not know this. The ICO has not addressed it. The customers whose data is being processed have not been told.*

8.2 What Cloud-Based CASS Processing Actually Involves

To understand why cloud-based CASS 15 processing raises acute GDPR concerns, it is necessary to be specific about what the daily reconciliation actually processes. The CASS 15 reconciliation requires, at minimum, the following categories of personal data for each client account: full name or business name of the account holder; unique account identifier; current balance and transaction history for the reconciliation period; the associated safeguarding account reference; and any flag or exception status triggered by the reconciliation analysis.

In a cloud-hosted SaaS architecture, this data does not remain within the regulated firm's own infrastructure. It is transmitted — typically over encrypted internet connections — to the vendor's servers, where it is processed, stored, and made available as output through a web-based interface. The processed data may reside on servers located in

the United Kingdom, in the European Economic Area, or in third countries with varying levels of data protection adequacy. It is subject to the vendor's own data security protocols, staff access controls, and sub-processor arrangements. And it is processed daily — not as a one-time event, but as a permanent, recurring transfer of personal financial data from the regulated firm to the third-party infrastructure.

The GDPR implications of this architecture are significant and, in the author's view, insufficiently appreciated by either the regulatory community or the firms deploying these systems.

8.3 The Five GDPR Principles That Cloud-Based CASS Processing Must Satisfy

Article 5 of the UK GDPR establishes six data protection principles that all processing must comply with. Five of them create specific and non-trivial obligations for cloud-hosted CASS 15 compliance processing that the author believes have not been systematically addressed.

The lawfulness, fairness, and transparency principle requires that processing have a lawful basis and that data subjects be informed of it. The lawful basis for CASS 15 data processing is most plausibly Article 6(1)(c) — processing necessary for compliance with a legal obligation. This basis is available, but it does not eliminate the transparency obligation. Data subjects — the customers whose financial data is being processed — must be informed, in the firm's privacy notice, that their data is transmitted to a third-party automated compliance platform for daily reconciliation. If firms are deploying SaaS CASS 15 solutions without updating their privacy notices to reflect this processing, they are in breach of the transparency requirement from the first day of operation.

The purpose limitation principle requires that data be collected for specified, explicit purposes and not processed in ways incompatible with those purposes. Client financial data is collected for the purpose

of providing payment services. Its daily transmission to a third-party SaaS platform for CASS 15 compliance processing is a secondary use that may or may not be compatible with the original purpose, depending on the terms of the firm's client agreements and privacy notices. Where the secondary use has not been disclosed, purpose limitation is breached.

The data minimisation principle requires that only data that is necessary for the processing purpose be used. A cloud-based CASS 15 platform that ingests complete transaction records, full account histories, and detailed client profiles — when the reconciliation function requires only balance confirmation and account status — may be processing more data than the legal obligation requires. Data minimisation in CASS 15 processing has never been addressed in any published guidance.

The storage limitation principle requires that personal data be kept in identifiable form no longer than necessary. In a cloud-based CASS 15 platform, the vendor's data retention policies — not the regulated firm's — determine how long client financial data is retained on the vendor's infrastructure. If those policies permit retention beyond the period necessary for the compliance function, storage limitation is breached. The regulated firm remains the data controller and is responsible for the vendor's retention practices under Article 28.

The integrity and confidentiality principle requires that data be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and accidental loss. A cloud-hosted CASS 15 compliance platform, by definition, introduces a third party into the data processing chain. The security of that processing depends on the vendor's technical and organisational measures — which the regulated firm must assess, contractually require, and periodically audit under its Article 28 processor obligations. Whether firms deploying SaaS CASS 15 solutions are

performing these assessments with the rigour that the volume and sensitivity of the data requires is, at present, unknown.

Five GDPR Article 5 Principles Applied to Cloud-Based CASS 15 Processing:

1. Transparency: Are data subjects informed that their financial data is transmitted to a third-party SaaS platform daily?

2. Purpose limitation: Has the secondary use of client data for CASS 15 compliance processing been disclosed and authorised?

3. Data minimisation: Is the platform processing only the data the legal obligation requires, or more?

4. Storage limitation: Does the vendor's retention policy align with the minimum necessary period for compliance purposes?

5. Integrity and confidentiality: Has the regulated firm conducted adequate Article 28 due diligence on the vendor's security measures?

8.4 Article 25: Data Protection by Design and by Default

Article 25 of the UK GDPR requires that data protection principles be implemented by design and by default. In the context of automated CASS 15 compliance systems, this requirement has a specific and demanding application. A system that is designed — at its architectural level — to transmit personal financial data to cloud infrastructure for processing is a system that has not implemented data protection by design in the most fundamental sense. The design choice itself — cloud-hosted rather than locally processed — determines the data protection profile of every subsequent processing operation.

A system that is designed to process all compliance analysis locally, without transmitting raw personal financial data to any external server, and to transmit only anonymised, aggregated, or mathematically transformed outputs as the compliance determination, is a system that implements Article 25 from its foundation. The choice of architecture is itself a data protection decision — and it is the most

consequential data protection decision that any CASS 15 compliance system designer makes.

The FCA has not addressed this distinction. PS25/12 is silent on the question of whether firms must implement data protection by design in their CASS 15 compliance systems, and silent on what that requirement would mean in architectural terms. The ICO's general Article 25 guidance does not address the specific context of automated regulatory compliance. The result is that two firms — one using a cloud-hosted SaaS platform that transmits raw client data to external servers, and one using a locally-processed system that never transmits raw personal data at all — are treated as equivalent by the CASS 15 framework. They are not equivalent. Their data protection profiles are fundamentally different, and those differences carry legal significance that the regulatory framework has not yet recognised.

8.5 The DPIA Obligation and Its Likely Non-Compliance

Article 35 of the UK GDPR requires a Data Protection Impact Assessment before commencing processing that is likely to result in a high risk to the rights and freedoms of data subjects. The ICO's guidance identifies several categories of processing that are likely to require a DPIA, including: systematic and extensive processing using automated means; large-scale processing of special categories of data; and processing involving new technologies.

Daily automated processing of personal financial data — encompassing account balances, transaction histories, and client identities — for hundreds or potentially thousands of clients, using automated reconciliation software, through cloud infrastructure, would appear to satisfy at least two and arguably all three of these criteria. A DPIA should, therefore, have been conducted by every regulated firm before deploying a cloud-based CASS 15 compliance platform.

The author has no empirical evidence that DPIAs have been widely conducted for CASS 15 automated compliance systems. What the author can observe is that neither the FCA nor the ICO has published any guidance requiring or recommending DPIAs in this context, and that the urgency of CASS 15 implementation — with firms under pressure to deploy compliant solutions before 7 May 2026 — creates conditions in which governance steps that are legally required but not specifically mandated are likely to be overlooked. If, as the author infers, the majority of regulated firms are deploying cloud-based CASS 15 solutions without first conducting DPIAs, then a regulatory compliance obligation designed to protect clients is being implemented through a process that itself violates the rights of those same clients.

8.6 The Architecture of Lawful Processing: What It Must Look Like

The author does not argue that automated CASS 15 compliance is inherently incompatible with GDPR. It is not. What the author argues is that GDPR-compliant automated CASS 15 processing requires a specific architectural profile — one that may not be present in cloud-hosted SaaS solutions but that is achievable and has been demonstrated in practice.

A GDPR-compliant architecture for automated CASS 15 processing would exhibit the following characteristics. Personal financial data would be processed locally — within the regulated firm's own infrastructure or on dedicated hardware under the firm's exclusive control — rather than transmitted to third-party cloud servers. The processing would occur within a secure, isolated environment from which raw personal data cannot be exfiltrated. The output transmitted externally — to the compliance officer, to the auditor, to the regulatory report — would be a compliance determination: a classification, a flag, a numerical summary. Not raw data. The identity of individual clients would never need to appear in the output layer. The system would process mathematical representations of the data rather than the data

itself wherever technically feasible. And the human reviewer who authorises the final determination would receive a human-readable compliance summary — sufficient to exercise genuine professional judgement — rather than access to the underlying raw data of each individual client.

This architecture is not a theoretical ideal. It is technically achievable. It has been implemented. The existence of systems that achieve it demonstrates that the GDPR and CASS 15 are reconcilable obligations — not in conflict, but requiring deliberate architectural choices that the FCA has never specified and the market has not been required to provide.

8.7 The Regulatory Failure and What Must Follow

The failure identified in this section is not the failure of individual firms or individual technology vendors. It is a regulatory failure — the failure of the regulatory framework to specify the technology architecture standards that CASS 15 compliance systems must meet in order to simultaneously satisfy the daily reconciliation obligation and the data protection rights of the clients whose data that obligation requires to be processed.

The FCA has created a legal obligation. It has not governed the technology through which that obligation will be discharged. The ICO governs data protection but has not engaged with the specific processing characteristics of CASS 15 automated compliance. The result is a regulatory gap in which firms can claim CASS 15 compliance while simultaneously — and daily — violating the data protection rights of their customers. The obligation to reconcile and the obligation to protect personal data are not separate concerns that can be addressed sequentially. They are simultaneous constraints on the same operation, and they require a technology architecture that satisfies both.

Until the FCA specifies minimum technology architecture standards for CASS 15 automated compliance systems — standards that include data processing location requirements, data minimisation obligations, and encryption standards at the architectural level — the daily reconciliation obligation will continue to be discharged, by many firms, through systems whose data sovereignty profile is irreconcilable with the rights of the customers those systems are nominally designed to protect.

> *The FCA has mandated the exercise. It has not governed the instrument through which the exercise is performed. In the absence of technology architecture standards, CASS 15 compliance and GDPR compliance are not two obligations a firm can satisfy simultaneously with a cloud-hosted SaaS platform. They are, for many firms, a daily contradiction — one that the regulatory framework has created and has yet to resolve.*

9. A Proof of Concept: The Architectural Qualities of a GDPR-Compliant Automated CASS 15 Compliance System

9.1 From Problem to Demonstrated Solution

The preceding section argued that the dominant market architecture for automated CASS 15 compliance — cloud-hosted Software-as-a-Service platforms — is likely to create systematic tensions with the data sovereignty obligations of UK GDPR. That argument is, of necessity, inferential in its characterisation of the market. What is not inferential is the following: the architectural approach that would resolve those tensions exists, has been built, and has been demonstrated to work in the CASS 15 compliance context.

The authors of this paper have, in the course of their work at the intersection of regulatory law and compliance technology, directly encountered and contributed to the development of one architectural model that addresses the intersection described in the preceding sections. That model is described in this section not as a commercial proposition but as a reference architecture — a proof of concept that demonstrates, concretely, that CASS 15 compliance and GDPR compliance are not in conflict when the system is designed from first principles to satisfy both simultaneously. Its qualities are presented here as a contribution to the regulatory and academic conversation about what a minimum technology architecture standard for CASS 15 compliance should require.

The authors do not claim that this is the only architecture capable of satisfying the intersection. They do claim that it demonstrates the intersection is navigable — that the regulatory fragmentation described in this paper need not produce an impossible compliance burden, but that it does require deliberate, principled architectural choices that the market, left ungoverned, is unlikely to make spontaneously.

9.2 The Foundational Principle: Data Sovereignty as an Architectural Starting Point

The architectural model described here begins with a commitment that is, in the authors' view, the necessary starting point for any GDPR-compliant automated CASS 15 compliance system: the raw personal financial data of the firm's clients never leaves the firm's own controlled environment. It is processed locally. It is analysed locally. It never traverses the internet. It never resides on a third-party server. The compliance determination — the output of the analysis — is what travels. The data is what stays.

This commitment is not a feature. It is a foundational architectural principle that shapes every subsequent design decision. Once this principle is established, the data minimisation, purpose limitation, and integrity and confidentiality obligations of Article 5 UK GDPR follow naturally. There is no data to minimise in transmission because no data is transmitted. There is no purpose limitation question about secondary use because the data never leaves the processing environment for which it was collected. There is no third-party security risk because there is no third party in the data processing chain.

The principle can be stated simply: the compliance provider brings the analytical capacity to the data, not the data to the analytical capacity. This reversal — which runs counter to the economic logic of cloud-hosted SaaS — is the architectural decision that reconciles CASS 15 compliance with GDPR data sovereignty in a single design choice.

> *We brought the machine. We brought the mathematics. We never saw your money. This is not a marketing claim. It is an architectural guarantee — and the distinction between the two is the difference between nominal compliance and genuine data protection.*

9.3 The Multi-Stage Analytical Pipeline: Separation of Functions

The processing architecture that implements the foundational principle described above operates through a multi-stage analytical pipeline in which different functions are performed sequentially and independently, with each stage receiving only the output of the previous stage rather than access to the underlying raw data. This separation of functions is significant for two reasons: it implements data minimisation at the architectural level, and it creates natural audit trail checkpoints at each stage boundary.

In the first stage, the system performs data aggregation and mapping — ingesting the firm's client account records and safeguarding account data and constructing a structured internal representation of the safeguarding position. This stage has access to personal financial data. It does not produce personal financial data as its output. It produces a structured analytical dataset — a mathematical representation of the safeguarding position — from which the next stage proceeds.

In the second stage, the system performs the compliance analysis — reconciling the analytical dataset against the CASS 15 rule set, identifying variances, classifying exceptions, and producing a preliminary compliance determination. This stage operates on the structured analytical dataset from stage one. It does not require, and does not have access to, the raw personal financial data of individual clients. Its output is a compliance classification and an exceptions package.

In the third stage, the system performs synthesis — combining the outputs of the first two stages into a structured compliance determination document designed for human review. This document contains sufficient information for a qualified professional to exercise genuine, informed judgement about the determination: the overall compliance classification, a plain-language summary of any exceptions,

the evidential basis for each classification decision, and the specific questions that require human professional resolution.

The human reviewer — whose role is described in the following subsection — receives the stage three output. They do not receive, and do not need to access, the raw personal financial data of individual clients in order to exercise meaningful professional oversight. The pipeline has, by design, separated the personal data from the compliance determination before the output reaches the human review layer.

9.4 The Human-in-the-Loop as an Architectural Requirement, Not a Governance Layer

The previous section of this paper argued that the human-in-the-loop requirement under Article 22 UK GDPR is underspecified — that 'human involvement' has never been defined in terms of what it must consist of, what qualifications the reviewing professional must hold, or what evidence of their review must be retained. The architectural model described here addresses this specification gap not through additional governance procedures but through architectural design.

The human review function in this architecture is not a downstream step that could, in principle, be bypassed or abbreviated. It is a structural requirement embedded in the pipeline itself. The compliance determination cannot be issued — cannot be delivered to the client firm, cannot be incorporated into any regulatory report, cannot be stored as a completed compliance record — until it has been reviewed and formally authorised by the designated qualified professional. The system does not permit the determination to proceed without this step. The authorisation is not recorded as a separate governance note attached to an automated output. It is the act that transforms the analytical output of the pipeline into a compliance determination.

This design choice has specific legal consequences. It means that no compliance determination produced by the system is, in the Article 22 UK GDPR sense, 'solely automated.' The human review is not nominal. It is constitutive — it is what makes the output a determination rather than an algorithm's classification. The qualified professional reviewing the stage three output brings their professional knowledge, their regulatory judgement, their personal accountability, and their authority to the determination. They can challenge the classification, override the exception analysis, escalate a finding that the system has flagged as routine, or defer a determination pending additional information. Their involvement changes the output, not merely the record of it.

The minimum qualification standard for this review function is, in the authors' view, a matter for the regulatory framework to specify — as argued in the companion paper 'The Unfinished Law.' What the present paper argues is that the architectural design of the pipeline should make it impossible to bypass the human review, not merely inappropriate to do so.

9.5 Zero-Knowledge Output: What Leaves the System

The output of the analytical pipeline — the compliance determination that is delivered to the client firm, incorporated into the FCA's SUP 16.14A monthly return, and retained as the day's compliance record — contains no personal data. It contains the overall compliance classification (compliant, amber, or non-compliant), the number of accounts reconciled, the aggregate variance figure (zero, or the amount of any shortfall), the specific exceptions identified and their regulatory classification, the timestamp of the determination, and the formal authorisation of the reviewing professional.

The identities of individual clients whose accounts were reconciled to produce this determination are not in the output. Their individual balances are not in the output. Their transaction histories are not in

the output. The output is a compliance determination — a professional judgement about the firm's regulatory position — not a report on individual clients' financial affairs. This distinction is not merely a matter of data minimisation, though it satisfies that principle. It is a fundamental design decision about what the CASS 15 compliance function actually requires as output, and what it does not.

The CASS 15 rules require the firm to maintain records demonstrating its compliance. They do not require those records to contain personal financial data in identifiable form. A compliance determination that states the firm has reconciled twelve accounts, found zero variance, and classified its position as fully compliant is a complete CASS 15 compliance record. It serves the regulatory purpose without creating a daily archive of personal financial data outside the firm's own controlled environment.

9.6 Cryptographic Verification and the Tamper-Evident Audit Trail

The integrity of the compliance determination is secured through cryptographic means. Each determination is assigned a unique reference and a cryptographic hash — a mathematical fingerprint that is computed from the content of the determination at the moment of its authorisation. If the determination is subsequently altered — whether by accident, administrative error, or deliberate manipulation — the hash will no longer match the content, and the tampering will be detectable.

This cryptographic verification serves three regulatory purposes simultaneously. For CASS 15, it provides an immutable audit trail that demonstrates the determination was issued at the stated time with the stated content — addressing the FCA's requirement for a contemporaneous, timestamped record. For UK GDPR, it demonstrates that the personal data processing underlying the determination was not subsequently misused to alter or expand the output — supporting

the accountability and integrity principles of Article 5. And for the annual safeguarding audit under SUP 3A, it provides the auditor with a technically verifiable record of every determination issued during the audit period — one that cannot be retrospectively amended without detection.

9.7 The Phase 2 Roadmap: Advanced Data Sovereignty at Scale

The architecture described in this section represents the current operational state of the reference model. The authors are aware that local processing — while ideal for data sovereignty — creates a practical constraint: the analytical capacity must be physically present at or near the client firm's premises, or the client firm must transmit its data to a dedicated, air-gapped processing environment under the compliance provider's exclusive physical control. This constraint is manageable for large institutions with the resources to accommodate dedicated on-site infrastructure. It requires a different solution for the broader market of smaller regulated firms.

The Phase 2 architecture in development addresses this constraint through advanced cryptographic techniques that are now approaching practical deployment readiness. The central insight of Phase 2 is that the local processing requirement can be satisfied without physical co-location if the data is transformed — before transmission — into a mathematical form that cannot be decrypted by the compliance provider. Processing is performed on this transformed representation. The compliance determination is derived from the transformed data. The compliance provider never holds a decryption key. They never have access to the readable personal financial data of the client firm's customers.

This approach — known in the cryptographic literature as Fully Homomorphic Encryption — allows computation on encrypted data to produce an encrypted result, which the data owner (the regulated firm)

can then decrypt to obtain the compliance determination. The compliance provider processes mathematical ciphertext throughout. They bring the analytical capacity to the encrypted data. They receive the encrypted result. They never see the underlying information.

Complementary techniques — post-quantum cryptographic transport using lattice-based key encapsulation mechanisms that are resistant to quantum computing attacks, and hardware-level trusted execution environments that provide attestable guarantees about the integrity of the processing environment — form the remainder of the Phase 2 architecture. Together, they represent the direction of travel for a compliance technology sector that takes data sovereignty seriously: not as a constraint on what automation can achieve, but as the design principle from which automation must begin.

9.8 The Two-Tier Model: Scalability Without Compromise

The reference architecture described in this section operates through two distinct deployment tiers that address the full spectrum of the regulated market without sacrificing data sovereignty at either end.

The first tier — appropriate for large institutions with significant safeguarding obligations — involves dedicated, physically isolated processing hardware operating on the client's premises or in a secure facility under the compliance provider's exclusive physical control, with no network connectivity during the processing cycle. This tier provides absolute data sovereignty guarantees: the data never leaves the client's physical environment, and the processing environment is isolated from external networks during operation. The compliance determination is the only output that travels.

The second tier — appropriate for the broader market of smaller regulated firms — provides the same data sovereignty guarantees through cryptographic means rather than physical isolation. Client

data is transformed cryptographically before transmission. Processing occurs on transformed representations. Only the compliance determination travels in readable form. The compliance provider never holds a decryption key for any client's data, at any point in the process.

Both tiers satisfy the foundational principle: the compliance provider brings the analytical capacity to the data, not the data to the analytical capacity. The difference is in the mechanism — physical isolation for Tier 1, cryptographic transformation for Tier 2 — not in the guarantee. Both tiers can demonstrate, to the client and to the regulator, that raw personal financial data has not been transmitted to or processed on third-party infrastructure. Both tiers satisfy the data sovereignty requirements that the FCA's technology architecture standard — when it is published — should, in the authors' view, require.

This two-tier model is not proposed as the only possible architecture for GDPR-compliant CASS 15 compliance. It is proposed as a demonstration that scalability and data sovereignty are not inherently in conflict — that the economics of compliance technology delivery do not require firms to choose between operational practicability and their customers' data rights. The choice has been made in favour of both. The architecture exists to prove it.

10. The Concentration Risk That No Single Regime Addresses

10.1 The Systemic Blind Spot

Beyond the governance intersection at the firm level, there is a systemic vulnerability in the CASS 15 framework that transcends any single regulatory regime and has not been adequately addressed by any of the four frameworks described above. It is the concentration risk created by the structure of the UK safeguarding bank market.

PS25/12 requires firms to hold relevant funds in designated safeguarding accounts with authorised credit institutions. In practice, the market for safeguarding accounts is highly concentrated. A small number of credit institutions — predominantly the large retail clearing banks — provide the vast majority of safeguarding accounts for the UK's 900+ regulated EMIs and PIs. This means that a significant proportion of the £32 billion in UK client money under safeguarding flows into the same institutions through accounts that are, for CASS 15 purposes, individually segregated but institutionally co-located.

The catastrophic implication of this concentration became vivid in March 2023, when the simultaneous failures of Silvergate Bank, Silicon Valley Bank, and Signature Bank in the United States created a crisis for hundreds of fintech firms that had concentrated their operational and client money deposits at those institutions. The UK has its own precedent: in 2022, the collapse of a mid-tier banking institution would have simultaneously affected dozens of EMIs whose safeguarding accounts were concentrated there. Daily reconciliation — however accurate and automated — cannot protect against this risk. A firm whose safeguarding bank is in resolution is compliant with its reconciliation obligations right up to the moment the bank's doors close.

10.2 The Macro-Prudential Gap

CASS 15 is, by design, a micro-prudential instrument. It regulates the behaviour of individual firms. It has no mechanism for addressing concentration risk at the sector level — for identifying that too many firms have their safeguarding deposits concentrated with the same institution, or for requiring diversification across multiple credit institutions as a systemic safeguard. The FCA's macro-prudential responsibilities sit with the Bank of England and the PRA, not with CASS 15.

The result is a structural vulnerability that daily automated reconciliation cannot address: the possibility of a simultaneous multi-firm safeguarding failure triggered not by any individual firm's non-compliance, but by the failure of a single safeguarding bank serving many of them. In such a scenario, a firm's CASS 15 compliance record — however immaculate — provides no protection to its clients. The Resolution Pack might be retrievable in 48 hours. The PESAR special administration regime might be activated. But the fundamental structural problem — that client money was effectively undiversified at the system level — will have persisted through every daily reconciliation without triggering any regulatory flag.

This is a problem that the PS25/12 framework, for all its ambition and rigour, has not addressed. It is also a problem that no individual firm can solve alone. It requires a sector-level regulatory response — either a mandatory diversification requirement for safeguarding deposits, or a systemic stress-testing framework that models multi-firm simultaneous safeguarding account failure. Neither exists.

11. The FRC Standard Gap: Auditing Compliance Without a Standard

11.1 The Auditing Architecture and Its Missing Foundation

The annual safeguarding audit required under SUP 3A is a mandatory reasonable assurance engagement. It requires a qualified, independent auditor to opine on whether the firm maintained adequate systems for safeguarding compliance throughout the audit period and was compliant at the period end. The first audit period commences on 7 May 2026. The first audit reports are due within six months of the period end — meaning the first reports must be submitted to the FCA by approximately November 2027 for firms with May 2026 start dates.

The Financial Reporting Council, which is responsible for auditing standards in the UK, has indicated that it intends to consult on a draft Relevant Funds Audit Standard in the second half of 2026 and to publish a final standard in 2027. The logical consequence is that the first wave of safeguarding audits will be conducted without a finalised, FRC-endorsed auditing standard. Auditors are being asked to reach professional conclusions — ones that they will be professionally accountable for — using criteria that have not been standardised, using methodologies that have not been agreed, and applying professional judgement to a new regime that has no established body of audit practice behind it.

11.2 The Automated System Audit Problem

The absence of an auditing standard is particularly acute when the firm being audited uses automated compliance systems. An auditor assessing a firm's CASS 15 compliance through manual processes can apply traditional audit techniques: test the reconciliation, verify the trail, confirm the account structures, review the breach records. The

audit methodology, while new in the CASS 15 context, is conceptually familiar.

An auditor assessing a firm's CASS 15 compliance through an automated compliance engine faces a qualitatively different challenge. They must assess not just the output — the reconciliation — but the governance of the system that produced it: Was the system's logic correctly specified? Was it validated against the CASS 15 rule set? Were changes to the system adequately controlled? Was the human review mechanism — the human-in-the-loop — meaningful or ceremonial? These are questions from the domain of technology audit, model risk management, and IT governance — not traditional financial audit.

The FRC standard, when it is published, will need to address these questions. Until it does, auditors assessing automated CASS compliance systems are working without either a methodology or a standard — and firms deploying such systems are unable to design their governance architecture with any certainty about what the auditor will be looking for.

12. The Post-Repeal Regime Pause and the Unresolved Property Law Problem

12.1 The Statutory Trust and Why It Was Paused

The most fundamental unresolved question in the CASS 15 framework is not operational but legal. It is the question of ownership. When a client's money is held in a safeguarding account by an authorised EMI or PI, who owns that money in the legal sense? The answer determines what happens to the client when the firm fails — whether the money is immediately and unambiguously theirs, retrievable from the safeguarding account without joining the queue of the firm's creditors, or whether it forms part of an asset pool whose distribution depends on insolvency proceedings.

The answer that PS25/12 does not provide — because it cannot, under the existing statutory framework — is the creation of a statutory trust over safeguarded funds. Such a trust would make the answer unambiguous: the money is the client's. The firm is merely its custodian. The firm's creditors have no claim over it. This was the outcome that CP24/20's proposed Post-Repeal Regime would have achieved — and it was the outcome that the Court of Appeal judgment in Baker v FCA (Re Ipagoo LLP) [2022] EWCA Civ 302 demonstrated to be legally necessary for genuine client money protection.

The FCA paused the Post-Repeal Regime following industry pressure. The stated rationale — that the Supplementary Regime should be bedded in first before further reform — is understandable as regulatory pragmatism. But it leaves a structural gap at the heart of CASS 15 that daily automated reconciliation cannot close. A firm may be impeccably compliant with every CASS 15 requirement: its reconciliations accurate, its audit trail complete, its resolution pack retrievable. If that firm enters insolvency, the absence of a statutory trust means that the legal status of its clients' money will once again

be determined not by a clear property right but by insolvency litigation — the very outcome that the Ipagoo judgment exposed as inadequate.

12.2 The Implication for Automated Compliance Systems

This legal uncertainty has a specific implication for automated CASS compliance that has not been noted in the existing literature. The Sovereign Auditor and systems like it are designed to produce compliance determinations under the existing CASS 15 framework. They verify, on a daily basis, that the firm's safeguarding is adequate under the rules as currently written. What they cannot verify — because it is beyond the scope of CASS 15 as a legal instrument — is whether the property law architecture within which the safeguarding obligation sits would protect clients in the event of insolvency.

A firm that receives a GREEN determination from its automated compliance system every day for three years, and then enters insolvency on day 1,096, has complied with CASS 15 throughout. Its clients may nevertheless lose a significant proportion of their money if the courts do not recognise a trust over the safeguarded funds. The automated compliance system has done everything it was designed to do. The law has done less than everything that client protection requires.

This is the deepest limitation of the CASS 15 Supplementary Regime as a consumer protection instrument. It is a regime built on compliance verification rather than legal protection. Until the statutory trust is enacted through the Post-Repeal Regime, the daily GREEN determination is a statement of regulatory compliance — not a guarantee of client money safety.

13. Towards a Unified Automated Compliance Governance Standard

13.1 The Regulatory Gap That Requires a New Instrument

The analysis in the preceding sections establishes that the convergence of CASS 15, UK GDPR, operational resilience requirements, and SM&CR accountability in the context of automated compliance systems creates regulatory exposure that no single existing framework adequately addresses. The gap is not one that can be resolved by more detailed guidance from any single regulator. It requires a cross-regulatory instrument — one that acknowledges the intersection, establishes an obligation hierarchy, and provides firms with a coherent governance architecture.

The author proposes that this instrument take the form of a Unified Automated Compliance Governance Standard (UACGS) — a joint publication by the FCA and the ICO, with input from the FRC and the National Cyber Security Centre, that establishes binding standards for the design, operation, oversight, audit, and accountability of automated compliance systems used to discharge FCA-mandated obligations. The UACGS would not be a new legislative instrument. It would be a coordinated regulatory statement — modelled on the existing Joint FCA-PRA Supervisory Statement on Algorithmic Trading — that draws together and reconciles the obligations that currently flow, uncoordinated, from four different regulatory sources.

13.2 The Core Architecture of the UACGS

The UACGS would need to address five structural elements.

The obligation hierarchy establishes, clearly and bindingly, the priority order when the four frameworks create conflicting obligations. The author's proposed hierarchy — subject to regulatory consultation — would give CASS 15 accuracy obligations primacy in the compliance

determination process, subject to GDPR Article 22 safeguards in the data processing infrastructure, with SM&CR accountability structuring the human oversight layer and PS21/3 operational resilience requirements governing the ICT architecture.

The human oversight standard defines what constitutes adequate human review for Article 22 purposes in the automated CASS 15 compliance context — specifying the minimum qualifications, access to information, and evidence of review required to make a compliance determination genuinely human-in-the-loop rather than merely nominally so.

The automated system governance framework establishes minimum standards for the design, validation, change management, and testing of automated CASS 15 compliance systems — addressing the regulatory lacuna that currently allows firms to deploy systems whose accuracy and reliability have never been externally validated.

The incident management protocol provides a sequenced, coordinated response framework for operational system failures — specifying in what order CASS 15, PS21/3, SM&CR, and ICO notification obligations should be discharged when an automated compliance system fails during a business day.

The audit methodology framework — developed in collaboration with the FRC — establishes the standards against which automated CASS 15 compliance systems should be audited under SUP 3A, resolving the audit validity problem identified in Section 11.

UACGS Element	Problem Resolved	Responsible Authorities
Obligation hierarchy	Provides a framework for resolving conflicts between CASS 15, GDPR, PS21/3, and SM&CR when they point in different directions	FCA + ICO

UACGS Element	Problem Resolved	Responsible Authorities
Human oversight standard	Defines what meaningful human-in-the-loop review requires, resolving the Article 22 ambiguity	FCA + ICO
Automated system governance	Establishes minimum design, validation, and change management standards for automated compliance engines	FCA + NCSC
Incident management protocol	Sequences and coordinates the reporting obligations triggered by automated system failures	FCA + ICO
Audit methodology framework	Provides auditors with the standards and methodology required to audit automated CASS 15 systems	FCA + FRC

14. Recommendations

14.1 To the Financial Conduct Authority

- Acknowledge, formally and publicly, that automated CASS 15 compliance systems exist at the intersection of CASS 15, UK GDPR, operational resilience, and SM&CR obligations — and commit to publishing coordinated guidance that addresses the intersection before the first annual safeguarding audit cycle commences in 2027.
- Initiate a joint working group with the Information Commissioner's Office to clarify the Article 22 GDPR obligations that apply to automated CASS 15 compliance systems, including: the minimum standard for human-in-the-loop review; the DPIA requirements for automated reconciliation processing; and the conditions under which a CASS 15 automated determination should be treated as engaging Article 22 safeguards.
- Issue a Supervisory Statement clarifying what constitutes adequate oversight of an automated CASS 15 compliance system for SM&CR purposes — specifying the management information Senior Managers should receive, the training or qualification appropriate for their oversight role, and the evidence of oversight required to establish reasonable steps.
- Work with the FRC to accelerate the publication of the Relevant Funds Audit Standard — targeting H1 2026 for a consultation draft rather than H2 2026 — so that the first wave of safeguarding audits commences with the benefit of an agreed professional standard.
- Commission a sector-level concentration risk assessment examining the distribution of safeguarding deposits across UK credit institutions — and consult on whether a mandatory diversification requirement is appropriate to address the systemic vulnerability identified in Section 9.
- Confirm a timeline for the Post-Repeal Regime consultation — and acknowledge explicitly that the Supplementary Regime does not resolve the underlying property law uncertainty identified in the Ipagoo judgment.

14.2 To the Information Commissioner's Office

- Publish specific guidance on the application of UK GDPR Article 22 to automated regulatory compliance systems — addressing the question of whether automated CASS 15 compliance determinations engage Article 22 obligations, and if so, what those obligations require.

- Clarify the lawful basis for the data processing undertaken in automated CASS 15 reconciliation — specifically, whether the processing of personal financial data for regulatory compliance purposes is adequately covered by the 'legal obligation' lawful basis under Article 6(1)(c), or whether additional analysis is required.

14.3 To the Financial Conduct Authority: Technology Architecture Standards

- Publish, jointly with the ICO, a Technology Architecture Standard for CASS 15 Automated Compliance Systems that specifies: minimum requirements for data processing location (including whether cloud-hosted processing is permissible and on what conditions); data minimisation requirements applicable to the reconciliation process; encryption standards for data at rest and in transit; and the minimum technical and organisational measures required under Article 32 UK GDPR for systems processing client financial data in the CASS 15 context.
- Require all firms deploying automated CASS 15 compliance systems to conduct and document a Data Protection Impact Assessment before going live — and specify, in guidance, the minimum contents of a CASS 15 DPIA including assessment of data processing location, data minimisation, sub-processor arrangements, and data sovereignty risk.
- Consider whether the CASS 15 technology architecture standard should require that raw personal financial data is processed locally — within the regulated firm's own infrastructure or on dedicated hardware under its exclusive control — rather than transmitted to third-party cloud servers, with only compliance determination outputs (anonymised, aggregated, or mathematically transformed) transmitted externally.
- Engage with the Information Commissioner's Office to clarify the data sovereignty requirements applicable to firms using third-party SaaS platforms for CASS 15 processing — including whether the daily transmission of personal financial data to cloud infrastructure constitutes a restricted transfer requiring additional safeguards, and whether existing data processing agreements between firms and SaaS vendors adequately reflect Article 28 obligations.

14.4 To FCA-Regulated EMIs and Payment Institutions

- Do not assume that deploying an automated compliance system resolves your governance obligations. Build the governance architecture — human oversight standards, change management procedures, SM&CR accountability documentation, operational resilience assessment — before the system goes live, not after.

- Commission a legal review that specifically maps the four-framework intersection as it applies to your automated compliance system — identifying where the obligations align, where they create potential tensions, and what your current governance architecture does and does not address.
- Ensure that the named Senior Manager accountable for CASS 15 compliance receives adequate training and management information to oversee the automated system, not just its outputs. The accountability attaches to the system as well as to the reconciliation it produces.

14.5 To the Financial Reporting Council

- Accelerate the timeline for the Relevant Funds Audit Standard — specifically developing interim guidance on the audit of automated CASS 15 compliance systems that can be applied before the final standard is published.
- Engage with automated compliance technology providers to understand the architectural features of modern CASS 15 systems before finalising the audit standard — ensuring that the standard reflects the realities of how compliance is actually performed rather than how it was performed under manual processes.

15. Conclusion: The Map for the Intersection

The Financial Conduct Authority's CASS 15 framework is a serious and necessary regulatory achievement. The protection of client money in the UK payment sector — against the shortfalls, the commingling, the catastrophic insolvencies documented in the FCA's own data — is a legitimate and urgent policy objective, and PS25/12 advances that objective significantly. The author does not diminish that achievement.

What this paper has argued is that the achievement is incomplete in a structural sense that will become visible — and costly — as the automated compliance industry that CASS 15 has called into existence begins to operate at scale. The incompleteness is not in the reconciliation rules, which are well-designed. It is not in the audit requirements, which are appropriate in principle if underspecified in methodology. It is not in the reporting obligations, which are proportionate. The incompleteness is in the governance architecture for the machines through which these rules will, in practice, be discharged.

When a firm deploys an automated compliance system to perform its CASS 15 daily reconciliation, it is simultaneously deploying a personal data processing system, a critical ICT function, and the operational substrate of a named Senior Manager's personal liability. The regulatory framework that governs each of these dimensions was designed independently. The intersection has never been acknowledged, let alone mapped. The firms that deploy these systems today are navigating that intersection without a map — and with the knowledge that if something goes wrong, the regulatory and legal consequences will be distributed across four frameworks, none of which has anticipated the others.

This paper is the argument for drawing the map. It does not claim to have drawn it definitively. A definitive map requires the engagement of

the FCA, the ICO, the FRC, and the NCSC — the four regulatory bodies whose frameworks converge at this intersection. What this paper has done is identify the intersection, name its dimensions, document the collision scenarios, and propose the instrument — the Unified Automated Compliance Governance Standard — that would resolve it.

The previous paper in this series asked who will operate the machine. This paper asks who governs the machine. The answer, at present, is that the machine is governed by fragments — four partial answers from four frameworks that were never asked to form a whole. Until they are asked, and until they answer together, the governance of automated compliance in the UK payment sector is structurally incomplete.

The compliance community, the academic community, and the regulators themselves deserve better than a framework that was built to govern the outcome but left the process ungoverned. This paper is the argument for completing what PS25/12 began — not just in the rules, but in the architecture of governance within which the rules will be discharged.

> *A regulatory framework that governs the output but not the machine that produces it is not complete regulation. It is compliance in principle and uncertainty in practice. The intersection must be mapped. The standard must be written. The governance must be whole.*

Olushola Oke-Daniel

Barrister and Solicitor of the Supreme Court of Nigeria

Founder and Director, AFC Fintech Ltd · Inventor, Sovereign Auditor

Contributor: Dr Kolawole Oyekan, Chief Regulatory Director, AFC Fintech Ltd

April 2026 · olushola@fintechafc.co.uk · fintechafc.co.uk

REFERENCES AND REGULATORY SOURCES

Primary Regulatory Sources — FCA

1. Financial Conduct Authority, Policy Statement PS25/12, 'Changes to the Safeguarding Regime for Payments and E-Money Firms' (FCA, August 2025).

2. FCA Handbook, CASS 15: Client Money Safeguarding for Payment Services and Electronic Money Firms (effective 7 May 2026).

3. FCA Handbook, CASS 10A: Resolution Pack for Payment Services and Electronic Money Firms.

4. FCA Handbook, SUP 3A: Safeguarding Audits for Payment Services and Electronic Money Firms.

5. FCA Handbook, SUP 16.14A: Monthly Safeguarding Regulatory Return.

6. Financial Conduct Authority, Consultation Paper CP24/20, 'Changes to the Safeguarding Regime for Payments and E-Money Firms' (FCA, September 2024).

7. Financial Conduct Authority, Policy Statement PS21/3, 'Building Operational Resilience: Impact Tolerances for Important Business Services' (FCA/PRA/Bank of England, March 2021).

8. Financial Conduct Authority, Dear CEO Letter, 'Priorities for Payments Firms' (Matthew Long, Director of Payments and Digital Assets, March 2023).

9. Financial Conduct Authority, 'Safeguarding Arrangements of Non-Bank Payment Service Providers: Multi-Firm Review' (FCA, 2019).

Case Law

10. Baker and Another v Financial Conduct Authority; Re Ipagoo LLP (in administration) [2022] EWCA Civ 302 (Court of Appeal, 9 March 2022).

11. Re Supercapital Ltd (in administration) [2021] EWHC 1685 (Ch) (High Court, Chancery Division, 2021).

Data Protection and Privacy Law

12. Regulation (EU) 2016/679 (General Data Protection Regulation), as retained in UK law ('UK GDPR') under the European Union (Withdrawal) Act 2018.

13. Data Protection Act 2018 (UK).

14. Data (Use and Access) Act 2024 (UK) — amendments to automated decision-making provisions.

15. Information Commissioner's Office, 'Guide to the UK GDPR: Automated Decision-Making and Profiling' (ICO, current edition).

16. Article 22, UK GDPR — Automated Individual Decision-Making, Including Profiling.

Operational Resilience and Digital Infrastructure

17. Regulation (EU) 2022/2554, Digital Operational Resilience Act (DORA) — applicable to EU-passported UK firms; UK alignment framework under FCA consultation.

18. National Cyber Security Centre, 'Guidance for the Financial Sector: Cyber Resilience Standards' (NCSC, current edition).

19. Financial Stability Board, 'Third-Party Dependency in Cloud Services: Considerations for Systemic Risk' (FSB, 2019).

Professional Qualification and Audit Standards

20. Financial Reporting Council, 'Client Asset Assurance Standard' (FRC, revised November 2019, effective January 2020).

21. Financial Reporting Council, 'Consultation on a Relevant Funds Audit Standard' (FRC, anticipated H2 2026).

22. Chartered Institute of Securities and Investment, 'Client Money and Assets (CASS): Unit Specification' (CISI, current edition).

Professional and Academic Commentary

23. Linklaters LLP (Eddis, H.; Hay, R.; Murphy, O.; Hodgkins, F.; Lakhani, A.; Treacy, S.), 'FCA Confirms Tougher Safeguarding Rules for Payments and E-Money but Delays Longer-Term Reform' (Linklaters, August 2025).

24. Deloitte UK, 'The Safeguarding Shift Part 2: CASS 15 Internal and External Reconciliations' (Deloitte, October 2024).

25. Mayer Brown LLP, 'New Safeguarding Rules for UK Payment Firms: What Banks and Insolvency Practitioners Need to Know' (Mayer Brown, September 2025).

26. DLA Piper LLP, 'FCA Payments and E-Money Safeguarding Consultation: Contexts and Potential Consequences' (DLA Piper, October 2024).

27. Norton Rose Fulbright LLP, 'Preparing for the FCA's New Safeguarding Rules: A Countdown to 7 May 2026' (Norton Rose Fulbright, 2026).

28. Grant Thornton UK, 'Safeguarding Audits for Payment and E-Money Firms' (Grant Thornton, 2025).

29. Menzies LLP, 'Safeguarding Rules Finalised: A Pragmatic Update in PS25/12' (Menzies, August 2025).

30. Kohort Recruitment, 'Why CASS 15 Recruitment Is Getting Tougher in 2025' (Kohort, 2025).

31. AutoRek, 'The Future of Payment Operations: CASS 15 Readiness Survey' (AutoRek, 2025).

This Author's Related Work

32. Oke-Daniel, O., 'The Unfinished Law: Why CASS 15 Cannot Work Without a Mandatory Certified CASS Safeguarding Officer' — Regulatory Policy Seminar Paper submitted to the Financial Conduct Authority and industry stakeholders (AFC Fintech Ltd, March 2026, Version 1.0).

33. Oke-Daniel, O., 'AFC Certified CASS Safeguarding Lead (CCSL) Programme Specification' (AFC Fintech Ltd, March 2026) — submitted for academic partnership consideration.

34. Oke-Daniel, O. and Oyekan, K., 'The Sovereign Auditor: Human-in-the-Loop Governance Architecture for Automated CASS 15 Compliance' — Technical Architecture Document (AFC Fintech Ltd, 2025).