

Compliance Latency Framework

The First Formal Definition of Compliance as a Verifiable State

Compliance has always been something you prove.

The CLF is the architecture that makes it something you hold.

CLF

v1.2

THE PROBLEM: COMPLIANCE LATENCY

Every time an individual encounters a new institution, they must prove their compliance from zero. The employer who verified their right to work last year. The bank that confirmed their identity six months ago. The professional register that published their licence this morning. None of it carries forward. Each institution starts again as if nothing has ever been proven. The individual pays the full cost of that starting-from-zero — in time, in friction, and in the uncertainty that persists even after documentation has been presented. This is Compliance Latency.

Temporal Latency

The time required to gather, submit, and have documentation processed — repeated in full at every new encounter.

Verification Friction

The cumulative effort imposed on a compliant individual by a system that does not recognise prior verification as valid.

Trust Deficit

The residual institutional uncertainty that persists even after documentation has been presented.

WHAT THE CLF DEFINES

The Compliance Latency Framework is not a product and not a technology platform. It is the first formal definition of compliance as a continuous, portable, verifiable state that travels with the individual rather than being rebuilt from zero at each new institutional encounter. The CLF names the structural failure, defines the architecture that addresses it, and establishes the open standard through which that architecture is adopted, governed, and trusted across every sector and jurisdiction. It is published as a versioned open standard. Any organisation, institution, or platform may reference, implement, and build upon it. The standard belongs to the profession.

THE FOUNDING INSIGHT

Compliance has always been an event — something done to satisfy a requirement at a specific moment, for a specific institution, in a specific format. The CLF proposes something fundamentally different: compliance as a continuous, verifiable state. Something a person holds rather than something a person repeatedly proves.

THE THREE-LAYER ARCHITECTURE

Layer 1 · The Open Standard

Exists now

The CLF and CIS are formally defined, versioned, and published. The standard belongs to the profession. No organisation owns it.

Layer 2 · The Technology

Being built

CLF-compliant platforms implement the standard commercially. ACOS-RAAS is the first. Multiple platforms may implement simultaneously.

Layer 3 · The Governing Body

Future layer

An independent professional institution stewards the CLF, accredits platforms, certifies professionals, and seeks chartered status.

Published under the Compliance Latency Framework · Patent applications GB2520418.1 and GB2521073.3 filed · Open standard · Attribution required

THE FIVE COMPONENTS OF THE CLF

The CLF defines five structurally distinct components. Each has its own function. Each creates the conditions for the next. Understanding the sequence is understanding the system.

- CLF** **Compliance Latency Framework**
 The named open standard. The first formal definition of compliance as a verifiable state. All other components derive their definition from the CLF. Published as a versioned open standard. Freely available. No organisation owns it.

- CIS** **Compliance Identity Standard**
 The first structure that makes compliance portable. Defines six domains, a three-tier verification hierarchy, four portability conditions, and the accreditation framework. A CIS-compliant profile is prepared once and recognised everywhere the standard

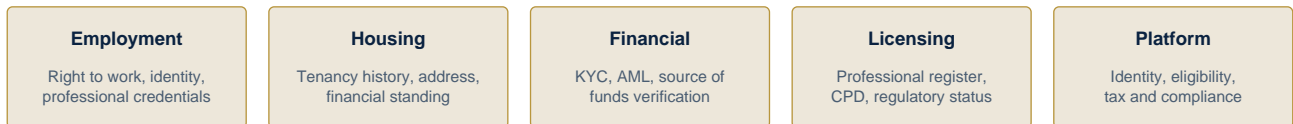
- CRE** **Compliance Readiness Engine**
 The first instrument that converts a static compliance record into a forward-looking readiness signal. Context-specific and predictive: the same CIS profile produces different CRE outputs depending on the institutional context being assessed.

- ACOS-RAAS** **Adaptive Compliance Operating System**
 The first technology platform built to implement the CLF. Developed by Rainfame Technologies Ltd. Protected by patent applications GB2520418.1 and GB2521073.3 covering the federated privacy-preserving architecture. A commercial

- CICP** **Chartered Institute of Compliance Professionals**
 The proposed future independent governing body. The first institution to constitute compliance as a single unified profession across every sector. Will steward the CLF, accredit platforms, certify professionals, and seek royal charter. Not yet incorporated.

THE COMPLIANCE LATENCY INDEX (CLI)

The CLI is the CLF's primary quantitative measurement instrument. It measures the mean time, in working days, required by an individual in a defined population to assemble and present a compliant, institution-ready proof of their compliance status in a specific context, starting from a baseline of zero prior institutional relationship with the receiving body. A CLI of zero represents instantaneous, fully portable compliance proof. The CLI is measured across five standard contexts: employment onboarding, housing tenancy application, financial services account opening, professional licensing verification, and regulated platform onboarding. It is published annually as the CLF's primary quantitative research output.



THE COMPLIANCE VERIFICATION GAP (CVG)

The Compliance Verification Gap is the CLF's plain-language expression of Compliance Latency: the space between what an individual has already proven to one institution and what a new institution will accept without requiring the entire proof to be rebuilt from zero. The CVG is not a measure of non-compliance. An individual experiencing the CVG is fully compliant. Their obligations are met. Their documentation exists. What does not exist is the structural layer that allows that compliance to travel with them. The CIS is the standard that closes the CVG.

WHO PAYS THE COST OF THE CVG

Compliance Latency falls hardest on the self-employed worker who moves between platforms, the migrant professional whose qualifications are unfamiliar to new institutions, the construction worker who resubmits their CSCS card to each new principal contractor, the healthcare locum whose NMC registration is current but must be resubmitted to each new NHS trust, and the gig economy worker whose working patterns do not fit the assumptions of a compliance infrastructure built for permanent employment. These are not edge cases. They represent tens of millions of people in the UK economy and hundreds of millions globally.

THE SIX CIS COMPLIANCE DOMAINS

The Compliance Identity Standard organises compliance across six primary domains. Each is self-contained and independently verifiable. A CIS-compliant profile may cover one domain or all six.

ID	Identity and Verification	KYC, right to work, biometric and document identity. The anchor of every CIS-compliant profile.
FIN	Financial and Tax Compliance	National Insurance, UTR, Self Assessment, VAT, and Making Tax Digital status.
LIC	Licensing and Professional Status	CQC, CSCS, FCA, SRA, NMC, CIBSE and any regulated professional licence.
REG	Sector-Specific Regulatory Compliance	UK GDPR, AML, NIS2, DORA, HSE, CQC, AI governance, ESG disclosure. Extensible.
HOU	Housing and Residency Compliance	Tenancy history, proof of address, and financial standing for housing access.
WE	Work Eligibility and Immigration	Right to Work verification through Home Office or certified DVS providers.

THE THREE-TIER VERIFICATION HIERARCHY

Tier One	Regulatory Verification	Statutory regulatory body Trust: Maximum · Validity: Up to 24 months
Tier Two	Certified Third-Party Verification	Certified provider under recognised scheme Trust: Medium · Validity: Up to 12 months
Tier Three	Holder-Asserted Information	Provided by holder — must be labelled HOLDER-ASSERTED Trust: Low · Validity: Holder's assertion

THE FOUR PORTABILITY CONDITIONS

1 Currency Every element within its defined CIS validity window at presentation.	2 Integrity Valid cryptographic integrity signal confirming profile has not been altered.	3 Accreditation Issuing platform holds current CLF Accredited Status at Tier C.	4 Relevance Profile covers the domains and tiers required for the specific context.
--	---	---	---

WHY NOW: THE REGULATORY CONTEXT

The regulatory environment has converged on conditions that make the CLF necessary and timely.

UK DVS Trust Framework Data (Use and Access) Act 2025 creates the statutory basis for certified portable digital identity in the UK f...
Employment Rights Bill 2025 Extends compliance obligations to platform and gig economy workers at a scale that makes repeated manual verif...
eIDAS 2.0 EU framework mandating portable digital identity wallets across member states, creating cross-border demand fo...
NIS2 and DORA Extend cyber security compliance obligations to a vastly expanded regulated population, increasing the populat...

THE GOVERNANCE MODEL

The CLF operates across three governance layers whose separation is the structural condition that makes the system credible.

<p>The Open Standard Exists now</p> <p>The CLF and CIS are published, versioned, and attributed. No organisation owns them. Free to reference and implement.</p>	<p>The Technology Being built</p> <p>CLF-compliant platforms are commercial products. ACOS-RAAS is the first. Multiple platforms may implement simultaneously.</p>	<p>The Governing Body Future layer</p> <p>The proposed independent CICP will steward the CLF, accredit platforms, certify professionals, and seek royal charter.</p>
---	---	---

ADOPTION TIERS — CLF ADOPTION AND ACCREDITATION PROTOCOL (CAP)

<p>Tier A CLF-Aligned</p> <p>Reference the CLF in policies, onboarding, or compliance frameworks. Free. No assessment required. Listed in the CLF Registry as CLF-Aligned.</p>	<p>Tier B CLF-Compliant Provisional</p> <p>Map internal processes to CIS domains. Structured self-assessment review. Listed in the CLF Registry as CLF-Compliant Provisional.</p>	<p>Tier C CLF Accredited Status</p> <p>Full CIS implementation independently assessed. Right to display the CIS Standard Mark. Listed as a recognised ecosystem participant.</p>
---	--	---

THE PATH FORWARD

<p>2025</p> <p>Standard Published</p> <p>CLF v1.2 and CIS v1.2 published as open standards. Patent applications filed. Founding council forming.</p>	<p>2026</p> <p>CICP Formation</p> <p>Proposed CICP incorporated as independent body. Founding council transitions to Board of Trustees. First accreditations.</p>	<p>2027</p> <p>Recognition</p> <p>BSI PAS application from 2027 once three or more institutional adopters and regulatory engagement are established.</p>	<p>2029</p> <p>Chartered Status</p> <p>Application to Privy Council for royal charter. CICP becomes the chartered body for the global compliance profession.</p>
--	---	--	--

HOW TO ENGAGE

<p>Read the Full CLF</p> <p>CLF v1.2 is available at rainfame.tech/frameworks. Free to download, reference, and implement with attribution.</p>	<p>Read the CIS Spec</p> <p>CIS v1.2 is the standalone specification for portable compliance identity. Available at rainfame.tech.</p>
<p>Apply for Tier C</p> <p>Submit a Tier C accreditation application to founder@rainfame.tech. Achieve CLF Accredited Status and display the CIS Standard Mark.</p>	<p>Join the Founding Council</p> <p>Senior compliance professionals are invited to serve on the CICP founding council. Contact founder@rainfame.tech.</p>

The standard belongs to the profession. The technology belongs to the market.

The governance belongs to the public interest.