CITY OF LONDON

THE GLOBAL CITY

In collaboration with

EY Shape the future with confidence

Hogan Lovells

Collectively Better

A Digital Verification Orchestrator (DVO) blueprint: scalable infrastructure for UK economic security

CITY OF LONDON

THE GLOBAL CITY

Contents

1. Forewords

“DV can form part of the backbone of data that supports economic and national security.”

Trusted digital verification (DV) is now critical infrastructure for UK financial services and for the wider digital economy. It supports the City of London Corporation’s Vision for Economic Growth[1] by helping to drive investment, innovation and a digital-first economy, while responding to the need for a stronger, trusted digital identity framework[2].

The Digital Verification Orchestrator (DVO) Initiative, managed by the City of London Corporation, sets out a practical route from blueprint to implementation of a trusted, interoperable digital verification model for the UK.

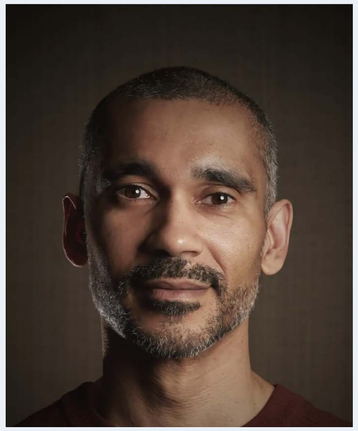
It shows how identity data providers (IDPs), relying parties (RPs) and firms can connect securely to exchange verified identity and attribute information, aligned with the Department for Science, Innovation and Technology’s (DSIT’s) Digital Verification Services (DVS) Trust Framework.

That alignment is a real value add. It can help establish common standards, strengthen interoperability, clarify responsibilities and instil trust in the system. This blueprint therefore goes beyond principle: it sets out capabilities and responsibilities, priority use cases, and high-potential existing market infrastructure, including candidates already accredited under the DSIT DVS Trust Framework and firms across the wider market that may have a role to play.

This matters at a moment of risk convergence. Artificial intelligence (AI)-enabled fraud, cyber threats, cryptography risks and geopolitical uncertainty all increase the need for trusted data, strong verification and UK data sovereignty. DV can form part of the backbone of data that supports economic and national security, helping to secure our economy while preserving user choice through voluntary private and public digital identity (ID).

The next phase must now focus on practical delivery, underpinned by coordination between government, regulators, industry and technology providers, as well as active engagement from chief executive officers (CEOs) and senior decision-makers. I thank all contributors for helping to shape this important initiative over the last five months. Together, we can build a safer, faster and more trusted digital future for the UK.

Christopher Hayward
Policy Chairman, City of London Corporation



Fraud thrives on fragmentation. The DVO Initiative is about addressing that fragmentation by giving the financial sector a modern, interoperable way to verify identity once and reuse verified information securely across the system, with appropriate consent and safeguards.

This blueprint should not be understood only as a fraud response. It is a practical document for implementation, setting out the capabilities, responsibilities, priority use cases and market conditions needed to build trusted DV at scale. It also recognises the importance of existing market infrastructure, including candidates accredited under the DSIT DVS Trust Framework and the wider range of firms that could support delivery.

The proposed DVO model offers a pragmatic trust layer built around standards, governance and liability. By aligning with the DSIT DVS Trust Framework, it can help create a shared basis for trust, interoperability, privacy, data security and auditability. That trust is essential if firms, consumers and public bodies are to rely on verified information with confidence.

The strategic context is changing quickly, not least as an enabler of agentic commerce and tokenisation. At the same time, AI, cyber threats, synthetic identity, cryptography risks, geopolitical uncertainty and data sovereignty are converging. The UK therefore needs these structures, clear communication and sustained strategic planning so that digital verification can support economic resilience and national security.

The economic opportunity is significant. As set out in *Securing growth: the digital verification opportunity*[3], the DVO model could generate at least £5 billion over five years through fraud loss mitigation and digital investment. The next task is to move from blueprint to implementation through pilots, firm-level commitment and coordinated action across government, regulators and industry.

Ezechi Britton MBE
DVO Initiative Steering Committee Chair, and

Alderman Sushil Saluja
DVO Initiative Steering Committee Vice Chair

1 City of London Corporation, Vision for Economic Growth: a roadmap to prosperity (2023).
2 HM Treasury, The Kalifa Review of UK FinTech (26 February 2021).
3 https://www.theglobalcity.uk/insights/securing-growth.

Forewords

“Trust is the foundation of digital growth. Done well, this is not just a fraud prevention agenda. It is growth infrastructure.”

Trust is the foundation of digital growth. Without safe, reliable ways to verify who people and businesses are, innovation slows, fraud rises and confidence weakens.

The City of London Corporation’s DVO blueprint is an important step towards changing that. It offers a practical way to make verification safer, faster and more reusable across the financial services ecosystem, helping firms protect customers while creating better, lower-friction digital journeys.

Done well, this is not just a fraud prevention agenda. It is growth infrastructure. A trusted verification layer can unlock new services, support responsible innovation and strengthen the UK’s position as a safe place to build, invest and transact digitally. As a firm dedicated to promoting growth and innovation, we are proud to contribute to this blueprint.

Ivan Heard
Partner, Financial Crime and Forensics, Ernst & Young LLP (EY)

2. Executive overview

The UK's digital verification market remains fragmented at the point when trusted, reusable identity signals are becoming critical to fraud prevention, customer experience, financial services innovation and national resilience. The DVO blueprint proposes a neutral orchestration model to address this gap by enabling verified identity and attribute information to be reused securely and consistently across financial services, with appropriate consent and safeguards. The immediate decision is whether industry, supported by government and regulators, will move from concept to practical market action through focused pilots that test the model, validate adoption conditions and build the evidence needed for scale.

Building on *Securing growth: the digital verification opportunity*, this DVO blueprint sets out the proposed DVO Model: defining its role, responsibilities, core capabilities, governance principles, liability considerations, priority use cases and recommended next steps for moving from concept to implementation.

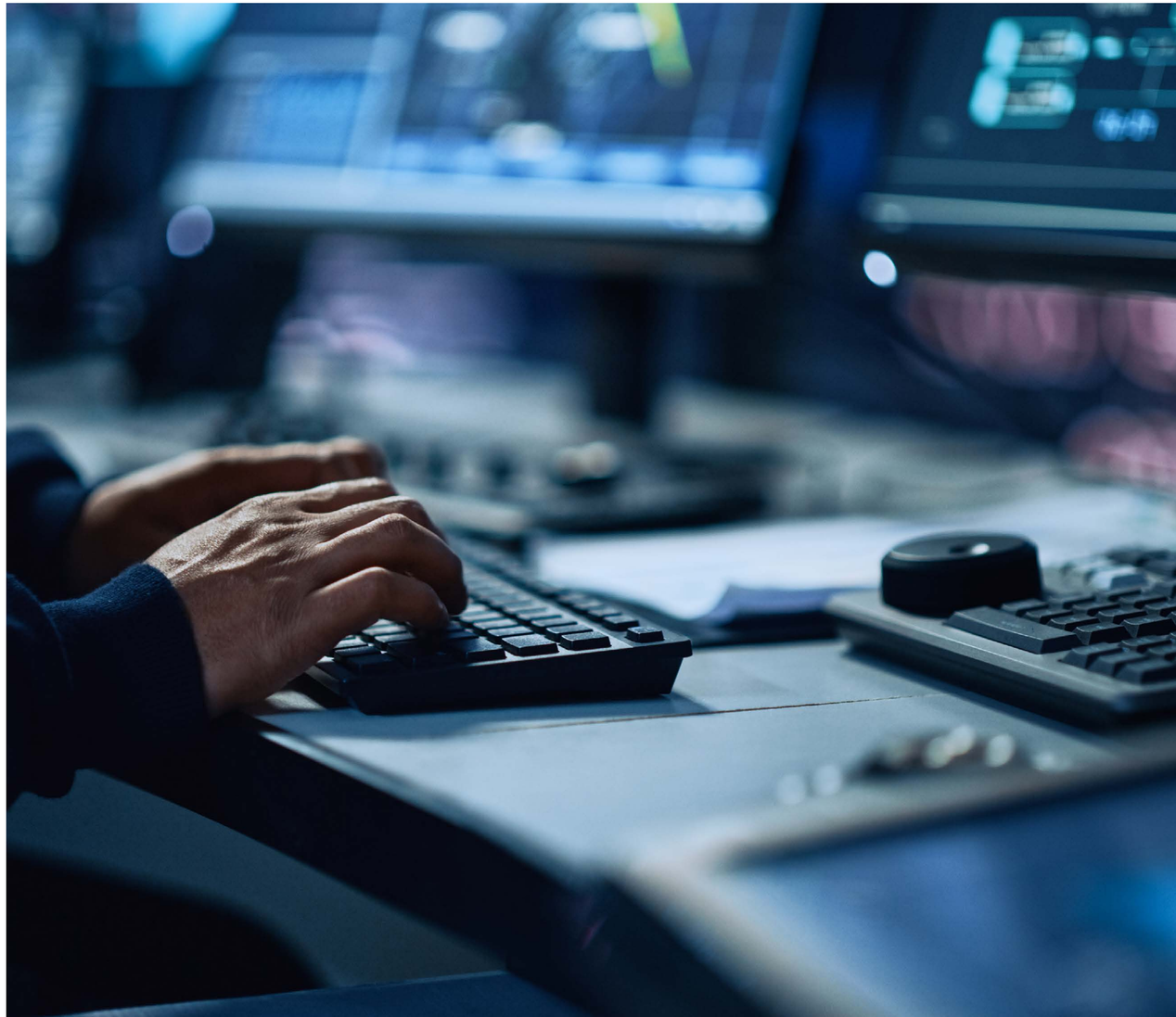
The intended audience for this blueprint is deliberately broad, reflecting the range of decisions needed to support adoption of the DVO model in financial services. It is intended to support three outcomes: encouraging financial services firms to begin testing DVO capability through practical pilots; giving DVO providers a clearer signal of the baseline capabilities, responsibilities and assurance that financial services firms are likely to need; and giving government and regulators an evidence base for supporting adoption through the UK's existing digital identity and regulatory architecture.

For financial services firms, this can reduce duplicated checks, lower onboarding costs, strengthen fraud prevention and support more confident reliance on trusted identity signals. For consumers, it can mean faster access to services, fewer repeated requests for the same information and greater confidence that their personal data is being handled securely.

To address these challenges, the DVO Initiative, managed by the City of London Corporation, sets out a blueprint for an independent orchestrator. This blueprint is a practical implementation document for a UK DVO. The blueprint helps define the role of the DVO so that participants in the ecosystem are clear on the responsibilities the DVO would hold and the capabilities any entity would need to demonstrate in order to perform that role.

In this blueprint, the DVO is defined as a neutral orchestration layer that supports secure consent led exchange of verified identity and attribute information between IDPs and RPs. It would not act as a central store of personal data or replace the underlying responsibilities of either party. Instead, the DVO would securely route verified data, validate data syntax quality, preserve data integrity in transit and support consent-led information exchange and auditability, enabling RPs to receive trusted verification signals in a consistent and interoperable way.

This document summarises the outputs of the DVO Initiative and the current position of the UK DV market. It defines the intended purpose and capabilities of a DVO, identifies priority use cases and sets out recommended next steps to move from blueprint to implementation. It is designed to support alignment across industry, government and regulators on a practical path to a trusted, interoperable DV ecosystem, whilst recognising that further work will be needed in the next phase on certain commercial and technical design choices required to support implementation at scale.



"Trusted DV should be understood as strategic infrastructure for the UK's financial services sector, not simply as a fraud-reduction tool."

- **The purpose:** The purpose of the DVO Initiative is to establish a trusted, interoperable framework for digital identity verification in the UK, with an initial focus on financial services. Whilst financial services are the starting point, a DVO designed to meet financial services requirements could also deliver value across non-financial sectors. The purpose of the DVO blueprint is to define the role, responsibilities and necessary capabilities of a DVO entity, and to provide a practical basis for implementation.
- **The proposed DVO model:** The proposed DVO model is based on three pillars: standards, governance and liability. The Responsibilities Matrix clarifies what the DVO is accountable for and what it is not. To fulfil the role, potential DVOs would need to evidence alignment with must-have capabilities and, where relevant, additional desirable capabilities. Non-discriminatory market participation and commercial sustainability are key principles underpinning the proposed DVO model.
- **Prioritised use cases:** Initial high-value financial services use cases include Know Your Customer (KYC)/onboarding, verification to enable access to credit, ongoing verification for fraud reduction, and portability/reuse of verified information across institutions. These use cases could improve user experience, reduce duplication and operational cost, strengthen fraud prevention and enable more secure reuse of verified information.
- **Market outlook:** Investment trends indicate that the digital verification market is maturing rapidly, with global venture capital (VC) and private equity (PE) investment increasing from £90.7 million in 2014 to £2.5 billion in 2023, whilst UK investment rose from £7.72 million to £114.7 million over the same period. However, the UK remains materially underdeveloped relative to more established markets, with DV accounting for just 0.047% of total UK PE and VC investment in 2024, compared with 0.36% in Sweden, suggesting significant headroom for further growth. A stronger national DV framework could therefore serve as a catalyst for additional investment, innovation and wider trust-enabled services across the economy. Market outreach indicates existing high-potential capability in the market, although some claims on accreditation, maturity and delivery capability remain subject to independent due diligence.
- **Next steps and recommendations:** The DVO Initiative's evidence highlights four key priorities to transition from blueprint to practical delivery, focusing on implementation pathways, market conditions and adoption enablers:

1. Launch a time-bound DVO pilot programme with committed IDPs, RPs and candidate DVOs. Within 12 months from the release of this blueprint the following should have occurred; (i) participating financial services institutions (FSIs) should agree the scope of two to three pilots; (ii) participating IDPs, RPs and candidate DVOs should run live or near-live tests across priority use cases; and (iii) the pilots should produce an implementation pack covering secure routing of verified identity and attribute signals, technical interoperability, consent, auditability, data integrity, customer experience, operational resilience, liability, commercial model and scale-up requirements.
2. Confirm the use of verifiable credentials within existing KYC, Anti-Money Laundering (AML) and consumer protection requirements. Government and regulators should review and confirm how verifiable credentials can operate within existing KYC, AML and consumer protection frameworks, including any updates to legislation or guidance needed to support reusable DV.
3. Embed DVO blueprint capabilities and responsibilities into the DSIT DVS Trust Framework[4] to support a neutral, open and interoperable market for orchestration. Government working with regulators and informed by industry should commit to incorporating the core aspects of this blueprint into the DSIT DVS Trust Framework and ensure that market-led orchestration is recognised as part of the wider DV framework, with open interfaces, consistent participation requirements and safeguards against structural advantage or lock-in.
4. Develop a liability, participation and dispute-resolution playbook for scale-up. Industry should develop a playbook, informed by pilot evidence and targeted engagement with government and regulators, covering liability allocation, operational failure, data integrity, data loss, dispute resolution, non-discriminatory participation, governance, funding and commercial conditions for adoption at scale.

- **Conclusion:** Trusted DV should be understood as strategic infrastructure for the UK's financial services sector, not simply as a fraud-reduction tool. The DVO blueprint offers a practical, interoperable model for scaling trusted verification, supported by existing high-potential market capability, although further independent due diligence and implementation testing are needed. The next phase should move from blueprint to delivery through focused pilots, firm-level commitment and coordinated action across government, regulators, industry and potential DVOs. If successful, the DVO model can help create a scalable, market-ready approach to secure, interoperable and privacy-preserving digital verification.

4 The DSIT DVS Trust Framework is a regulatory framework designed to establish standards and guidelines for digital identity verification services in the UK. It aims to help ensure that digital verification processes are secure, interoperable, and trustworthy, fostering confidence among users and organisations. The framework supports the safe sharing and use of verified identity data across sectors whilst maintaining privacy and with legal requirements.

3. The DVO Initiative

"The DVO blueprint should be understood as a route to strategic digital infrastructure that can make interactions with other firms and consumers more efficient, more secure and more trusted."

i. What this means for senior decision-makers

For senior decision-makers, the DVO blueprint should be understood as a route to strategic digital infrastructure that can make interactions with other firms and consumers more efficient, more secure and more trusted.

It can support better customer journeys, reduce duplicated verification activity and provide a stronger basis for relying on verified identity and attribute information across the financial services ecosystem. It can also support wider innovation across the organisation by creating reusable verification capabilities that help firms respond more quickly to emerging technologies and new digital services.

The next step is to advance two to three focused, time-bound pilots with committed IDPs, RPs and candidate DVOs, generating evidence on interoperability, customer experience, operational resilience, liability and commercial viability.

Any scaled model should remain open and market-led, supporting a competitive ecosystem of accredited providers while avoiding centralised data storage, proprietary lock-in or structural advantage for any single route to market. It will also require clear governance and funding choices from the outset, including defined accountability, a sustainable commercial model and safeguards to ensure that implementation costs, decision rights and delivery responsibilities are clearly allocated.

ii. Where are we today?

DV is a foundational enabler of the UK's digital economy, underpinning secure access to financial services, public services, and data-driven innovation. Despite progress, the market remains fragmented, with limited coverage from IDPs, persistent consumer trust concerns, and unclear liability frameworks.

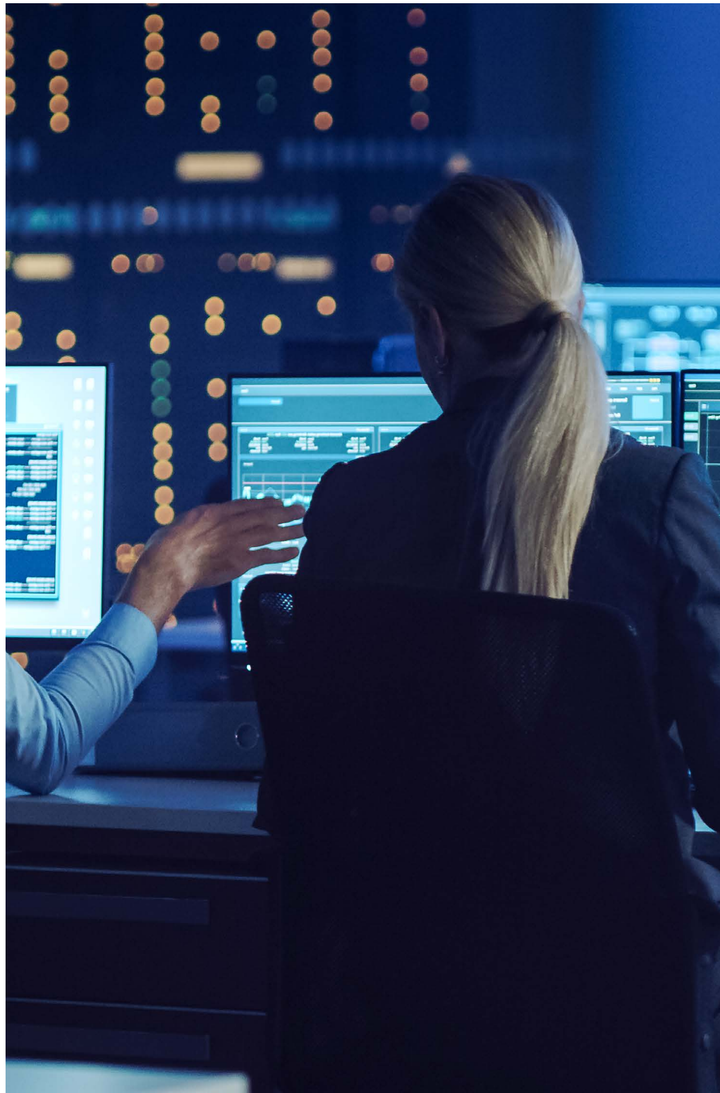
A more coordinated DV ecosystem would create clear value for both financial institutions and consumers. For banks and other RPs, it could strengthen security, reduce fraud losses, accelerate onboarding and lower operating costs through more automated, reliable and reusable identity checks. For consumers, it could enable a more seamless, secure and trusted verification experience, reducing friction, saving time and increasing confidence in how personal information is handled.

In March 2025, the City of London Corporation published its report *Securing growth: the digital verification opportunity*[5], which highlighted why the time is now to advance this conversation on DV in the UK. Developments since that report have only increased the urgency to act to bolster economic security in the UK.

The report proposed a conceptual model for DV in the UK centred around an independent entity, the DVO, and focused on user privacy and data security to build trust and encourage adoption and growth. Organisations including financial institutions can have a role in the DVO, as well as acting as both IDPs and RPs.

In simple terms, a DVO is an independent coordination layer that helps organisations share verified identity information securely and consistently. It does not replace IDPs or financial institutions, and it does not act as a central store of personal data. Instead, it helps connect the parties involved through agreed standards, governance and secure information exchange, so that RPs can receive trusted verification signals in a more interoperable and reusable way. In practice, this means a customer could verify themselves once with a trusted provider and, with appropriate consent, reuse that verification more easily across services.

The report also showed how the conceptual model could work in practice by applying it to a customer onboarding and KYC use case in financial institutions. This helped illustrate how the model's principles could operate in a real-world setting[6].



5 https://www.theglobalcity.uk/insights/securing-growth.
6 The customer onboarding and KYC use case is illustrated on pages 19 to 21 of the report Securing growth: the digital verification opportunity.

A conceptual model for DV in the UK

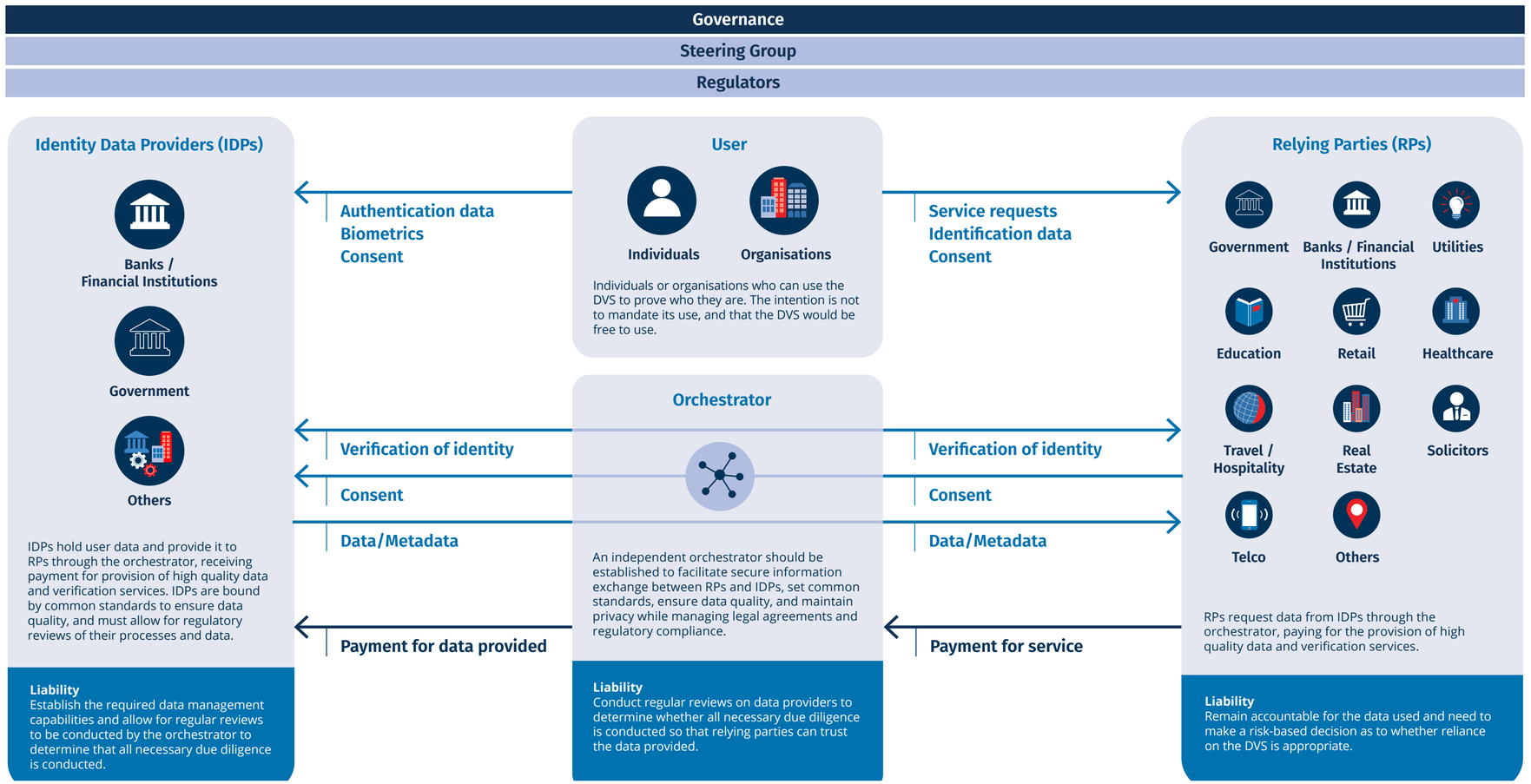


Figure 1: A conceptual model for DV in the UK, centred around a DVO.

"The model could improve efficiency, interoperability and trust for both firms and consumers."

Illustrative example

A customer seeks to open a new bank account online. Rather than repeating the full identity verification process, the customer consents to their previously verified identity information being shared through a trusted DVO-enabled route. The DVO does not store the underlying identity data itself but coordinates the secure exchange between the IDP and the bank using agreed standards, governance and controls. The bank receives the information it requires in a more consistent and auditable format, whilst the customer experiences a faster process with less duplication. This illustrates how the model could improve efficiency, interoperability and trust for both firms and consumers.

4. Purpose

i. Of the DVO

The purpose of the independent DVO is to facilitate secure information exchange between RPs and IDPs, apply and, as required, determine common standards, support data syntax quality and data integrity, and maintain privacy whilst managing legal agreements and supporting compliance with regulatory requirements.

The DVO should operate as a neutral, vendor agnostic orchestration layer, avoiding proprietary control or data monopolies.

ii. Of the DVO Initiative (30 January 2026 – 02 July 2026)

The DVO Initiative is managed by the City of London Corporation. It is chaired by Ezechi Britton MBE (Chair) and Alderman Sushil Saluja (Vice Chair). Hogan Lovells provides the secretariat and legal advice, and EY and Collectively Better provide strategic advice. The purpose of the DVO Initiative is to establish a trusted, interoperable framework for digital identity verification in the UK, particularly focusing on financial services. It aims to address current market fragmentation, consumer trust issues, and unclear liability by creating a governance-backed coordination layer that facilitates secure, standards-based information exchange between RPs (such as financial institutions) and IDPs.

The DVO Initiative complements the Centre for Finance, Innovation and Technology's (CFIT's) work on corporate identity verification as both initiatives aim to enhance identity verification processes within the financial services industry, ultimately aiming to reduce fraud, enhance user confidence and trust, and expand adoption of digital verification. Whilst CFIT's work focuses on the introduction of a Digital Company ID, the DVO Initiative focuses on the exchange of verified digital attributes (for example the exchange of verified Digital Company IDs).

The progression of the recommendations made by the DVO Initiative has the potential to deliver nearly £5 billion in uplift to the UK economy by 2031 through fraud loss mitigation and the modernisation of digital services. The strategic adoption of the DVO model is crucial for consumers, businesses and the overall economic landscape and its impact is anticipated to be comparable to the transformative impact of Open Banking.

iii. Of the DVO Initiative Working Group and Steering Committee (SteerCo)

The DVO Initiative is supported by the DVO Initiative Working Group and SteerCo. Details on the participants in the Working Group and SteerCo can be found in Appendix v.

The Working Group is constituted of FSIs, advisers, and academics. Participants draw upon the expertise within their organisations to provide technical, commercial, and legal input to shape deliverables, share market perspectives, and champion adoption of outcomes.

The SteerCo is constituted by senior representatives from FSIs, City of London, regulators and government and participants provide strategic oversight, validate outputs, and sign off deliverables.

iv. Of this document

This document contains the proposed DVO blueprint and is the primary deliverable of the DVO Initiative. It is a practical document that defines the role, responsibilities, and necessary capabilities of a DVO entity. It is intended to support three related audiences: financial services firms considering practical pilots and adoption pathways; DVO providers seeking to understand the baseline capabilities, responsibilities and assurance that the market is likely to require; and government and regulators considering how adoption can be supported through the UK's existing digital identity and regulatory architecture.

The DVO blueprint serves as a guide for industry, regulators, and potential DVO candidates to align on a neutral, scalable, and legally robust DV ecosystem. It is intended to foster collaboration, trust, and broad market adoption whilst helping ensure compliance with relevant frameworks such as the DSIT DVS Trust Framework.

The DVO blueprint highlights existing market capabilities and sets out proposed next steps for scaling the DVO model to support UK financial services.

The DVO blueprint has been informed by inputs from industry[7] and outlines governance structures, commercial and liability principles, technical and security standards, and participation rules.

7 In May 2026, the City of London Corporation published its news release ***Tech firms invited to lead fightback against fraud***, which called on tech firms to input into the blueprint for a DVO.

5. The proposed DVO model (based on standards, governance and liability)

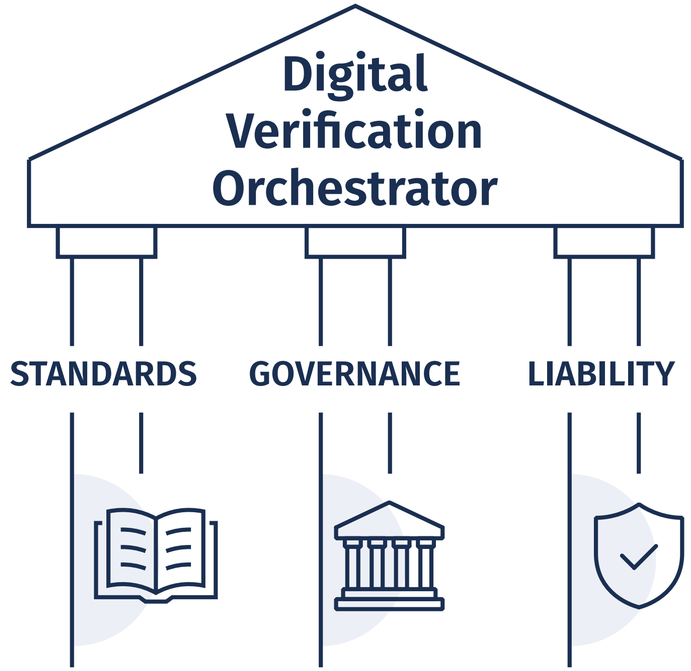


Figure 2: The DVO model based on standards, governance and liability.

"The proposed DVO model is intended to provide a trusted coordination layer between organisations that hold verified identity data and those that need to rely on it."

In practical terms, the proposed DVO model is intended to provide a trusted coordination layer between organisations that hold verified identity data and those that need to rely on it, supported by common standards, governance and clear liability arrangements.

The framework for the DVO model is based on three pillars:

- **Standards:** Setting and promoting the adoption of adequate standards and regulatory framework to support DV development.
- **Governance:** Putting in place minimum guardrails and a robust governance structure around fraud intelligence sharing and auditability to provide transparency and help build trust.
- **Liability:** Providing clear, flexible and market-led liability models for different use cases which inform how liability is shared between the parties with an effective dispute resolution mechanism/redress model to support this process.

A DVO would likely be operated by one or more accredited third-party orchestration providers, or by a governance-backed market utility, connecting banks, IDPs and other RPs through common technical, legal and operational rules. It would not hold a central database of personal identity information; rather, it would route verified signals securely between trusted participants.

Given the strategic importance of trusted digital verification infrastructure, any scaled DVO model should also support UK sovereignty. This includes ensuring that the governance, legal framework, operational control and critical service resilience of the DVO are aligned to UK requirements, so that a core layer of national digital verification capability is not dependent on arrangements that could undermine UK oversight, security or long-term strategic autonomy.

i. Responsibilities matrix

A DVO is expected to be able to:

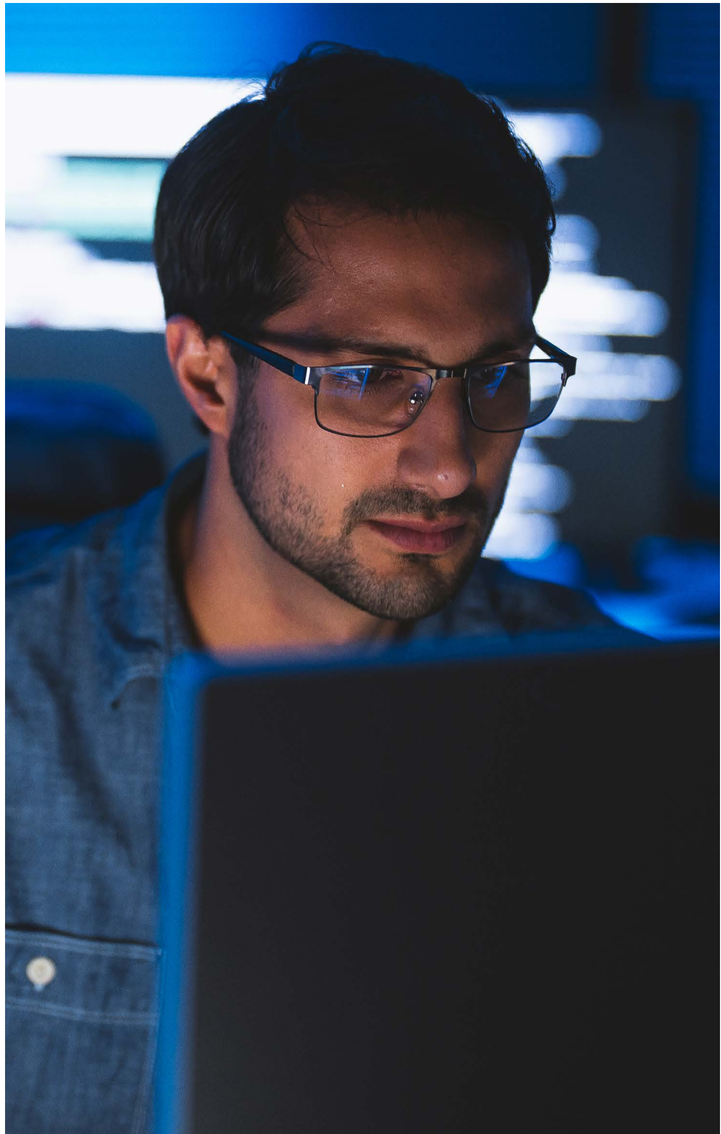
- **Apply and, as required, determine minimum standards as part of an orchestration layer:** Define and maintain technical and performance standards and security controls for participants (including accreditation under the DSIT DVS Trust Framework where applicable), helping ensure interoperability with UK and international identity frameworks. The DVO is expected to support multiple identity and authentication protocols to help ensure interoperability and resilience across diverse use cases. Details on the minimum standards required can be found in the Assessment Criteria in Appendix iii.
- **Enable secure, resilient data transfer:** Be accountable for the integrity, availability and performance of orchestration flows (e.g. connectivity, Application Programming Interfaces (APIs), metadata exchange) and for evaluating emerging technologies and standards to enhance orchestration capabilities (e.g. the DVO is expected to remain interoperable during transitions to post-quantum cryptographic standards without requiring major architectural changes).
- **Facilitate stakeholder coordination to support trusted verification data flow:** Collaborate with those operating across the model and regulators to support effective identify verification including providing a process for resolving operational issues outside of bilateral commercial contracts.
- **Support non-discriminatory market participation:** Enable fair and non-discriminatory access for users, IDPs and RPs, avoiding exclusivity or structural market advantage.
- **Support real-time auditability:** By maintaining immutable, real-time audit trails of all verification transactions. The DVO is expected to be able to enable trusted, consent-led, auditable data flows that preserve user agency and privacy, helping ensure compliance with data protection regulations.
- **Enable low-friction integration:** Integrate seamlessly with existing legacy financial and identity infrastructure, minimising disruption and preserving existing investments.
- **Aggregate verification signals across multiple IDPs:** Where appropriate and subject to consent, a DVO should be capable of coordinating and aggregating relevant attributes or verification signals from multiple IDPs in order to support a coherent, standards-based verification outcome.

By contrast, the DVO is not expected to act as:

- **A data store:** The IDPs hold user data and provide it to RPs through the orchestrator. IDPs are bound by common standards to support the quality of data attributes and must allow for regulatory reviews of their processes and data. The DVO facilitates secure information exchange between RPs and IDPs and conducts regular reviews on IDPs to determine whether all necessary due diligence is conducted so that RPs can trust the data provided.
- **A quality assurer for data attributes:** The RPs remain accountable for the data used and must make a risk-based judgment regarding reliance on the DVO. This process is bolstered by verifiable or audited evidence of IDP operations and processes in relation to data attributes, which are prerequisites for IDP accreditation under the DSIT DVS Trust Framework. The DVO (and appropriate regulatory bodies) conduct regular assessments of IDPs to support due diligence processes, thereby enhancing the RPs' confidence in the quality of data attributes provided. The accredited IDPs remain responsible for the accuracy and quality of the data attributes since they are the original sources that collect, validate, and maintain the identity data. The DVO helps ensure that the data syntax is consistently structured and correctly formatted to enable seamless interoperability, accurate processing, and reliable integration across diverse systems within the DV ecosystem. The DVO helps maintain the integrity of data as it passes through the orchestration layer to ensure that information remains accurate, complete, and unaltered during transfer. This helps to preserve trust, prevent fraud, and helps enable reliable decision-making based on authentic and trustworthy data.
- **A regulator:** Clear regulatory ownership and oversight of the DV model in the UK still needs to be designated. Given the initial focus on the Financial and Professional Services (FPS) sector as a primary use case and the role of banks as IDPs, the Financial Conduct Authority (FCA) may be a suitable candidate to help ensure oversight and compliance with financial regulations. The Information Commissioner's Office (ICO) may be a suitable candidate to help ensure oversight and compliance with UK General Data Protection Regulation (GDPR).

For the purposes of the responsibilities matrix, the following terms are used consistently. "Accountable" means the DVO owns the outcome for that activity within the orchestration layer. "Responsible" means the DVO performs or coordinates the activity but may not own all underlying outcomes. "Facilitates" means the DVO supports the process, for example by routing information, providing evidence, maintaining records or escalating issues, but does not own the underlying outcome. "Context-dependent" means the DVO's role may vary according to the use case, contractual arrangements and applicable regulatory requirements. "Not responsible" means the DVO does not own or perform the activity, although it may provide supporting evidence, routing or auditability where relevant.

The table below applies these terms to the activities a DVO would be expected to perform, coordinate, facilitate or avoid owning.



i. Responsibilities matrix

Category	Activity	DVO role	Detailed explanation
Standards	Setting Technical Standards	Accountable	The DVO is accountable for setting standards for entities operating within the model and helping ensure interoperability with national and international identity frameworks and standards.
	Performance Standards Management	Accountable	The DVO is accountable for setting standards for coverage, API availability and connectivity to help ensure consistent and reliable service delivery.
	Data Security and Authentication	Accountable	The DVO is accountable for: implementing and maintaining security controls to protect identity data and verification processes; monitoring and mitigating risks related to data breaches; and helping ensure security via encryption standards and API security.
	Compliance with New Regulations and Standards	Not responsible	Whilst the DVO is not responsible for enforcing compliance, the DVO must maintain systems to enforce compliance with evolving regulations and standards to support adherence within the ecosystem.
	Improvement and Innovation	Accountable	The DVO is accountable for evaluating new identity verification technologies and standards to enhance orchestration capabilities; and driving innovation to improve user experience, security, and efficiency of identity verification (e.g., during transitions to post-quantum cryptographic standards).
Governance	DSIT Framework Accreditation Verification	Accountable	The DVO is accountable for confirming that IDPs are accredited under the DSIT DVS Trust Framework, but not for managing or enforcing the certification process itself, which is managed by DSIT or relevant authorities.
	Data Transfer Management	Accountable	The DVO is accountable for the speed and integrity of data transfers between parties, helping ensure secure and efficient metadata exchange.
	Consent Management for Data Transfer	Responsible	The DVO needs to help ensure that appropriate consent mechanisms are in place for data transfers, potentially adopting models similar to those used in open banking.
	Audit and Due Diligence of Participants	Facilitates	The DVO would help facilitate audit and due diligence processes on behalf of DSIT or equivalent authorities through activities such as escalating concerns about participant compliance or operations.
	Performance Monitoring	Accountable	The DVO is accountable for monitoring the performance, availability, and reliability of the identity verification orchestration platform; and managing service level agreements (SLAs) with identity verification providers.
	Reporting and Documentation	Accountable	The DVO is accountable for maintaining detailed documentation of identity verification workflows, compliance status, and security measures; and providing regular reports to management and regulatory bodies, as required.
	Stakeholder Coordination	Responsible	The DVO is responsible for collaborating with internal teams, external IDPs, regulators, and consumers to help ensure effective identity verification; and providing guidance and support to stakeholders on identity verification processes and compliance requirements.
	Dispute Resolution Process	Responsible	The DVO is responsible for providing a mechanism for resolving operational issues outside of contractual agreements but does not act as the sole arbitrator or assume liability for underlying data issues.
	Aggregation of Verification Signals Across Multiple IDPs	Responsible	The DVO coordinates consent-led aggregation of signals from multiple IDPs, whilst the underlying data remains with the IDPs.

Category	Activity	DVO role	Detailed explanation
Liability	Contractual Agreements Between IDPs and RPs (and Orchestrators)	Context-Dependent	In most cases, the DVO would not assume liability, as liability should be primarily allocated between IDPs and RPs. However, liability could arise depending on the contractual arrangements entered into, use cases and contexts, and applicable regulatory developments. Each case should be assessed individually.
	Quality of Data Attributes	Not responsible	The DVO is not responsible for the quality of data attributes i.e. the accuracy and correctness of the underlying identity data. The quality of the data attributes is expected to be managed by RPs and IDPs via bilateral contracts. The accredited IDPs remain responsible for the accuracy and quality of the data attributes since they are the original sources that collect, validate, and maintain the identity data.
	Quality of Data Syntax	Responsible	The DVO is responsible for the quality of the data syntax and helps ensure that all identity verification data exchanged between different IDPs and RPs is consistently structured and correctly formatted.
	Integrity of Data during Transfer	Responsible	The DVO is responsible for maintaining the integrity of data as it passes through the orchestration layer to ensure that information remains accurate, complete, and unaltered during transfer.
	Data Processing	Context-dependent	The DVO only passes metadata. To the extent the DVO is subject to the GDPR for a specific use case, it would act as a processor rather than a controller. The DVO should avoid becoming a centralised data repository of personal data.

ii. Capabilities

This Responsibilities Matrix helps to clarify which responsibilities across the model fall on the DVO and which do not.

To fulfil this role, a DVO **must** be able to demonstrate evidence of:

- Alignment with the DSIT DVS Trust Framework.
- Examples of integrating at least three identity providers and verification services.
- Adherence to audit and compliance processes including Systems and Organisation Controls (SOC) reports[8] and security audits.
- Experience of helping ensure interoperability between different identity verification systems and standards, including compliance with Electronic Identification, Authentication and Trust Services (eIDAS)[9].
- Demonstrated capability to design scalable and flexible orchestration solutions.
- Success in managing complex identity verification projects or platforms.
- Evidence of coordinating and, where appropriate, aggregating attributes or verification signals from multiple IDPs.

It is also **desirable** for a DVO to demonstrate the following:

- Experience in service orchestration and helping ensure high availability and reliability, including system redundancy and management of third-party suppliers.
- Compliance with Tier IV Data Centre Infrastructure Standard[10] for availability and redundancy.
- Examples of working with multiple stakeholders including technology providers, financial services and regulators.
- Strong communication skills to explain technical and compliance requirements clearly.
- An innovative mindset to adopt emerging technologies and standards in digital identity verification.
- A clear funding plan and viable business model.
- Strength to act independently among all the parties including direct experience of building and managing governance models.
- Awareness of the Model Context Protocol (MCP)[11], Agentic Context Protocol (ACP)[12] and Post-Quantum Cryptography (PQC)[13].
- Experience of providing a dispute resolution process.
- Examples of intentional strategies and investments towards accessibility, performance, user experience, and infrastructure to bridge the digital divide.

8 SOC reports are independent third-party audits that evaluate and verify the effectiveness of an organisation's internal controls related to security, availability, processing integrity, confidentiality, and privacy. These reports provide assurance to stakeholders that the organisation manages risks and complies with relevant standards and regulations.
9 eIDAS is a European Union (EU) regulation that provides a legal framework for electronic identification and trust services to enable secure and seamless electronic transactions across EU member states.
10 The Tier IV Data Centre Infrastructure Standard is the highest level of data centre certification defined by the Uptime Institute. It represents a data centre designed to provide the highest levels of fault tolerance and redundancy, helping ensure continuous availability and uptime.
11 The MCP is a standardised framework designed to enable secure and interoperable sharing of identity and attribute data across different systems and organisations. It facilitates the exchange of contextual information related to digital identity verification, helping to ensure that data is used appropriately and consistently within trusted digital ecosystems.
12 The ACP is a framework or protocol designed to manage and communicate the context of actions or decisions made by autonomous agents or systems in digital identity and verification environments. It helps capture and convey the circumstances, intentions, and authority under which an agent operates, helping ensure transparency, accountability, and trust in automated or delegated processes.
13 PQC refers to cryptographic algorithms designed to secure data against the potential threats posed by quantum computers, which could break many current encryption methods. PQC aims to develop new encryption techniques that remain secure even in a future where quantum computing is powerful and widely available.

Figure 3: Must have and desirable capabilities of a DVO.

iii. Funding, commercial sustainability and non-discriminatory market participation

Funding

The blueprint does not, at this stage, prescribe a single institutional form for the DVO. However, any scaled implementation would need to determine the appropriate legal form, governance model and funding approach for the entity or entities performing the DVO role. This includes questions such as whether the market model is best delivered through an independent private-sector provider, a consortium-based structure, a market utility model, or another form of governance-backed delivery arrangement. These choices will be important to help ensure the DVO is operationally credible, commercially sustainable, appropriately governed and capable of maintaining trust across the ecosystem.

Commercial sustainability

Commercial sustainability should be treated as a distinct requirement when assessing candidate DVOs. A DVO candidate will need a credible funding plan, a resilient operating model and a clear route to long-term financial sustainability, including the ability to support ongoing investment in technology, security, governance and service delivery as the model scales.

The DVO model should support a self-sustaining commercial structure that provides adequate incentives for participation whilst remaining financially viable over time. This includes careful evaluation of initial set-up and onboarding costs, ongoing operating costs, expected revenue streams, pricing approach and the likely pace of adoption across priority use cases. The commercial model should be sufficiently flexible to reflect different transaction volumes, use cases and participant types without undermining interoperability or trust.

At this stage, the blueprint does not prescribe a single commercial model for the DVO. This reflects the fact that the most appropriate commercial structure may vary according to the use case, the underlying transaction economics, the composition of market participants and the allocation of risk across the value chain. Nonetheless, moving from blueprint to implementation will require further consideration of the commercial design choices that would best support adoption at scale. These include, for example, the extent to which pricing arrangements should be transparent across participants, whether the DVO should manage commercial terms through bilateral contracting with participants or whether such arrangements should be negotiated directly between parties, and the degree to which buy-side and sell-side pricing should be standardised for comparable use cases. These issues are central to determining how the model can be made straightforward for RPs whilst preserving appropriate commercial incentives across the wider ecosystem.

Commercials will remain use-case specific, and contracting parties will need to negotiate pricing, liability allocation, insurance and appropriate mitigations in a way that reflects the value and risk profile of the service being provided.

Given recent experience in industry payments infrastructure, any DVO model will need a governance and funding approach that avoids unclear accountability, open-ended industry cost exposure and slow collective decision-making.

At maturity, the DVO should be capable of operating on a sustainable basis without relying indefinitely on subsidy, whilst retaining the ability to adapt its commercial approach as technology, regulation and user demand evolve.

High potential DVOs should be considered as potential recipients of strategic investments from both private and public sources, including through organisations such as the British Business Bank and the National Wealth Fund.

Non-discriminatory market participation

The DVO model should be open to both IDPs and RPs on fair, transparent and proportionate terms, and should avoid creating structural advantages for particular firms, technologies or routes to market. This means a candidate DVO should be able to demonstrate how access would be offered to IDPs and RPs, what objective conditions would apply to participation, how onboarding and technical integration would be managed, and how any restrictions would be justified. The model should be clear on the treatment of exclusivity: exclusive arrangements that foreclose participation, restrict interoperability or distort competition would be difficult to justify, whereas limited and proportionate exclusivity in narrowly defined circumstances may need to be considered case by case.

Non-discriminatory participation also depends on a fair value exchange across the ecosystem. Open access alone will not be sufficient if the commercial model does not provide credible incentives for key participants to join, invest and remain active. In particular, IDPs that contribute high-quality verification signals, including banks and other holders of trusted customer data, should be able to participate on terms that recognise the value of that contribution, whilst preserving openness, interoperability and user consent. Commercial arrangements should therefore enable broad participation and investment without creating structural advantage, lock-in or undue barriers to entry. This also underlines the importance of a clear liability regime, so that incentives to provide high-quality data and services are aligned with responsibility and risk.

To support a pro-competitive landscape, the DVO should operate with transparent participation criteria, fair commercial terms and appropriate governance safeguards. It should be possible to monitor whether access is being granted and maintained on a non-discriminatory basis, for example through transparency reporting, auditability and clear challenge or escalation routes where access is unfairly denied or degraded.

6. Prioritised use cases

It is anticipated that the DVO model will be able to support high value financial services use cases, including the below. In practice, these use cases may require the DVO not only to route verification requests between parties, but also, where appropriate and subject to consent, to coordinate and aggregate attributes or verification signals from multiple IDPs.

i. KYC and customer onboarding

KYC is a regulatory process used by banks and institutions to verify a customer's identity, assess their suitability, and evaluate risks in maintaining a business relationship. It involves collecting personal information such as identity documents, proof of address, and other relevant details to prevent fraud, money laundering, terrorist financing, and other financial crimes.

Customer onboarding is the comprehensive process of welcoming and establishing a new customer with a bank or financial service. It involves collecting and verifying customer information (including KYC), setting up accounts and services, educating customers about products and terms, and enabling access to digital banking platforms.

Recent research cited by UK Finance[14] has identified customer onboarding as a key growth priority for financial services firms, noting that the onboarding experience is critical to conversion in an increasingly competitive market, while UserTesting has reported that 68% of financial services onboarding attempts across Europe fail[15], underlining the commercial importance of reducing friction in digital account opening and verification journeys.. It is anticipated that a DVO could play a crucial role in both KYC and customer onboarding by streamlining and securing identity verification. It could standardise verification protocols and facilitate the efficient, secure exchange of verified identity data between multiple IDPs and financial institutions, reducing the need for customers to repeatedly submit documents. The DVO could help ensure regulatory compliance, manage customer consent, and enhance interoperability across verification services. By coordinating these activities, the DVO could significantly accelerate onboarding, improve accuracy, reduce fraud risk, and deliver a smoother, more trustworthy experience for new customers.

ii. Verification to enable access to credit

The verification process to enable access to financial credit involves confirming a customer's identity, assessing their creditworthiness, and validating relevant financial information such as income, employment, and credit history. This process helps ensure that the lender can accurately evaluate the risk of extending credit whilst complying with regulatory requirements. It helps prevent fraud and supports responsible lending decisions.

This is increasingly important because synthetic identity fraud is rising sharply in the UK: LexisNexis Risk Solutions estimates there are already 2.8 million high-risk synthetic identities in circulation, creating a potential £4.2 billion threat to UK businesses by 2027[16].

It is anticipated that a DVO could support the verification process for financial credit by securely coordinating the exchange of verified identity and financial data between IDPs, credit bureaus, and lenders. It could help ensure that data is accurate, compliant with regulations, and shared with proper consent, enabling lenders to efficiently assess creditworthiness. By standardising verification protocols and enhancing interoperability, the DVO could help reduce fraud, significantly speed up credit decisions, and improve the overall reliability of the credit access process.

iii. Ongoing verification to combat fraud

The ongoing verification process to combat fraud involves continuously monitoring and validating a customer's identity and transaction activities to detect and prevent suspicious or unauthorised behaviour. This includes real-time checks against updated identity data, transaction patterns, and risk indicators to quickly identify potential fraud. The process helps maintain security and trust throughout the customer relationship.

It is anticipated that a DVO could enhance ongoing verification by continuously coordinating secure data exchanges between IDPs and RPs to monitor customer identities and transactions in real time. It could help ensure that updated verification information is shared promptly and consistently, enabling early detection of suspicious activities. By maintaining standardised protocols and managing consent, the DVO could help reduce fraud risk whilst preserving privacy and trust across the ecosystem. The need is clear: UK Finance reported more than £1.1 billion of fraud losses in 2024[17], whilst Credit Industry Fraud Avoidance System (CIFAS) recorded nearly 250,000 identity fraud cases in the same year, representing 59% of all cases filed to the National Fraud Database[18].

iv. Reuse and portability of verified information across institutions

Reusing verified information across financial institutions involves securely sharing a customer's previously verified identity and compliance data to streamline processes like onboarding or credit applications.

A DVO could facilitate the secure and efficient reuse and portability of verified information across financial institutions by acting as a trusted intermediary that manages data sharing with proper consent. The DVO could support user agency by allowing users to decide which financial institutions access their information and under what terms. Furthermore, it could help ensure standardised verification protocols and interoperability among diverse IDPs and financial institutions, enabling seamless access to up-to-date, accurate identity data. This could reduce duplication, significantly accelerate processes, and enhance customer experience whilst maintaining compliance with privacy and regulatory requirements. Open banking adoption in the UK has reached 13.3 million active users, showing that consumers and small businesses are increasingly willing to use consent-based data sharing when it is seamless and trusted[19].

14 UK Finance, Onboarding in 2025: Strategies to deliver a standout customer experience, 22 January 2025.
15 Top 5 customer frustrations with digital bank account opening, January 3, 2025
16 LexisNexis Risk Solutions press release, 12 June 2024.
17 UK Finance, Annual Fraud Report 2025.
18 CIFAS, Fraudscape 2025, published 3 April 2025.
19 Open Banking Limited, "OBL Impact Report 7: open banking delivers real-world impact as adoption accelerates year-on-year", 16 May 2025.

1. KYC and customer onboarding
Verification of identity for customer onboarding

2. Verification to enable access to credit
Verification for lending and credit access

3. Ongoing verification to combat fraud reduction
Continuous verification for fraud prevention

4. Reuse and portability of verified information across institutions
Sharing verified information between organisations

Figure 4: The DVO model will be able to support high value financial services use cases.

The main benefits of a DVO are consistent across each high value use case:

- **Multi-modal identity verification:** The DVO could allow the integration of multiple identity verification methods (e.g., biometrics, document verification and facial recognition) and help choose the most appropriate or strongest combination for each transaction, helping ensure robust authentication.
- **Seamless integration:** By orchestrating various verification services and data sources, the DVO provides a unified and streamlined authentication process, reducing friction for customers whilst maintaining high security standards.
- **Regulatory compliance:** The DVO helps banks in complying with the Strong Customer Authentication (SCA)[20] requirements under the UK Payment Services Regulations 2017 (PSR) / the EU Revised Payment Services Directive (PSD2)[21] across different channels and transaction types.
- **Improved user experience:** By automating and optimising the verification flow, customers experience faster and smoother authentication without losing control over their own verified credentials or data.
- **Centralised management and reporting:** Banks gain better visibility and control over authentication processes.
- **Reduced operational costs:** Increased automation of identity verification reducing manual intervention, lowering operational costs and minimising human errors.

Multi Modal Identity Verification
Integration of biometrics, document verification, facial recognition, etc.

Improved User Experience
Faster smoother authentication

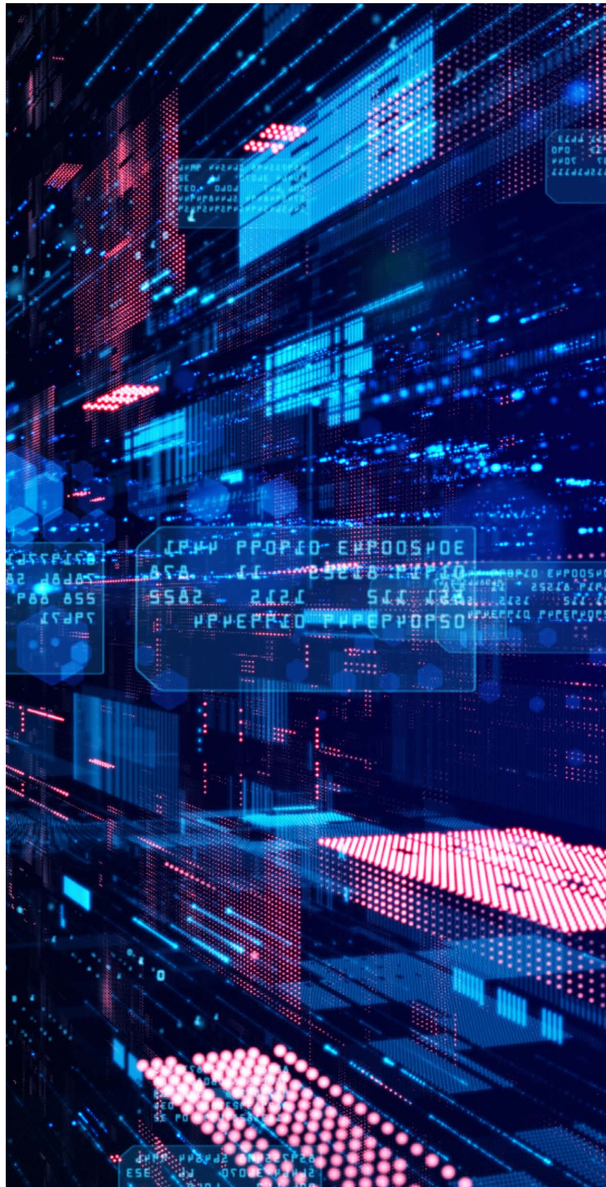
Seamless Integration
Unified authentication process reducing customer friction

Centralised Management and Reporting
Better visibility and control for banks

Regulatory Compliance
Ensuring PSD2 and SCA requirements are met

Reduced Operational Costs
Automation reducing manual work and errors

Figure 5: Benefits of a DVO across use cases.



20 SCA is a requirement under PSD2 designed to enhance the security of electronic payments and reduce fraud. SCA requires that electronic payments be authenticated using at least two of the following three elements: i) something the customer knows, ii) something the customer has, iii) something the customer is. These requirements apply to online payments and certain other electronic transactions to help ensure that the person initiating the payment is the legitimate account holder.

21 PSD2 is an EU directive aimed at regulating payment services and payment service providers throughout the EU and European Economic Area. PSD2 enhances consumer protection, promotes innovation and competition in the payments industry, and introduces requirements such as strong customer authentication and open banking.

7. Market outlook

i. Investment in the global and UK DV market

The global DV market is experiencing a surge in investor interest, with VC and PE funding soaring to £2.5 billion in 2023 - a dramatic rise from just £90.7 million in 2014, representing a 265% increase over the decade. This growth is further underscored by a significant increase in average deal sizes, which have exceeded £2 million per deal in three of the last five years, up from £270k per deal in 2015, reflecting the maturation of the industry.

Investment in the UK's DV market is also accelerating, climbing from £7.72 million in 2014 to £114.7 million in 2023, a 1386% increase. Although annual investment levels fluctuate, the UK has averaged almost £69 million per year between 2020 and 2024. Despite this growth, the UK's share of PE and VC investment in DV remains modest at 0.047% in 2024, compared to countries with established national DV frameworks such as Sweden, where DV investment accounted for 0.36% of total PE and VC funding[22].

These investment trends highlight the potential for a robust national DVS to catalyse innovation and attract greater capital into the DV ecosystem. A well-developed national framework not only supports foundational trust enabled services such as verified payments and smart contracts but also unlocks further investment opportunities in DV infrastructure and related services. Whilst UK-based companies are already attracting significant funding, there remains substantial scope to boost investment through the advancement of a comprehensive and mature DV system.

ii. DVO candidates in the market: insights from industry inputs

In May 2026, the City of London Corporation published its news release *Tech firms invited to lead fightback against fraud*, which called on technology firms to input into the DVO blueprint. A total of 22 responses were received from prospective DVO candidates. The inputs from the DVO candidate responses[23] have informed the blueprint by providing an indicative picture of existing market capability, areas of alignment with the proposed DVO role, and the issues that would require further work before any delivery model is progressed.

What the inputs suggest

The industry inputs suggest that there is already capability in the market to support a DVO model. Most respondents either operate in the UK already or identified the UK as a priority market, and a number of respondents pointed to existing accreditation under the DSIT DVS Trust Framework, including some with orchestration service provider accreditation[24]. Across the responses, common capability signals included experience integrating multiple identity providers and verification services, operating interoperable solutions across UK and international frameworks, managing audit and security processes, and delivering orchestration capabilities in live or near-live environments.

A number of respondents were also able to point to adjacent strengths that are relevant to the proposed DVO role, including scalable platform design, governance and stakeholder coordination, commercial models with more than one revenue stream, and support for high-value use cases such as onboarding, fraud reduction and portability of verified information. We would expect that a number of firms not captured in the call for input would also be likely to fulfil these adjacent strengths. Taken together, these inputs indicate that the market is not starting from zero: there is a base of potentially relevant capability on which a DVO delivery model could build.

What still requires validation

At the same time, the responses should be treated as indicative rather than conclusive. The submissions were self-attested and anonymised, and the strength of evidence varied materially across respondents. Independent due diligence is required to verify candidate claims. This includes technical capabilities, accreditations, and legal position. The industry inputs are useful for identifying where potentially relevant capabilities may already exist, but they do not remove the need for structured follow-up validation.

iii. DVO candidate assessment: Boston Box

The DVO Initiative Working Group reviewed the anonymised industry input submissions against the proposed DVO role and assessment criteria, scoring each response based on both fit with criteria and strength of evidence/ maturity. Reviewer inputs were calibrated to support consistency of approach, and aggregated scores were then used to inform the suggested position of each candidate within the Boston Box[25]. Details on the assessment criteria can be found in Appendix iii.

22 Pitchbook data (2025). Accessed 19 February 2025.
23 These were self-attested and then anonymised, and whilst they were scrutinised by advisers and the DVO Initiative Working Group, this should not substitute for independent due diligence of candidates to strengthen validation.
24 https://www.digital-identity-services-register.service.gov.uk/register/all-providers. Accessed 9 June 2026.
25 The "below minimum threshold" positions are indicative based on information supplied in the anonymised industry input submissions.

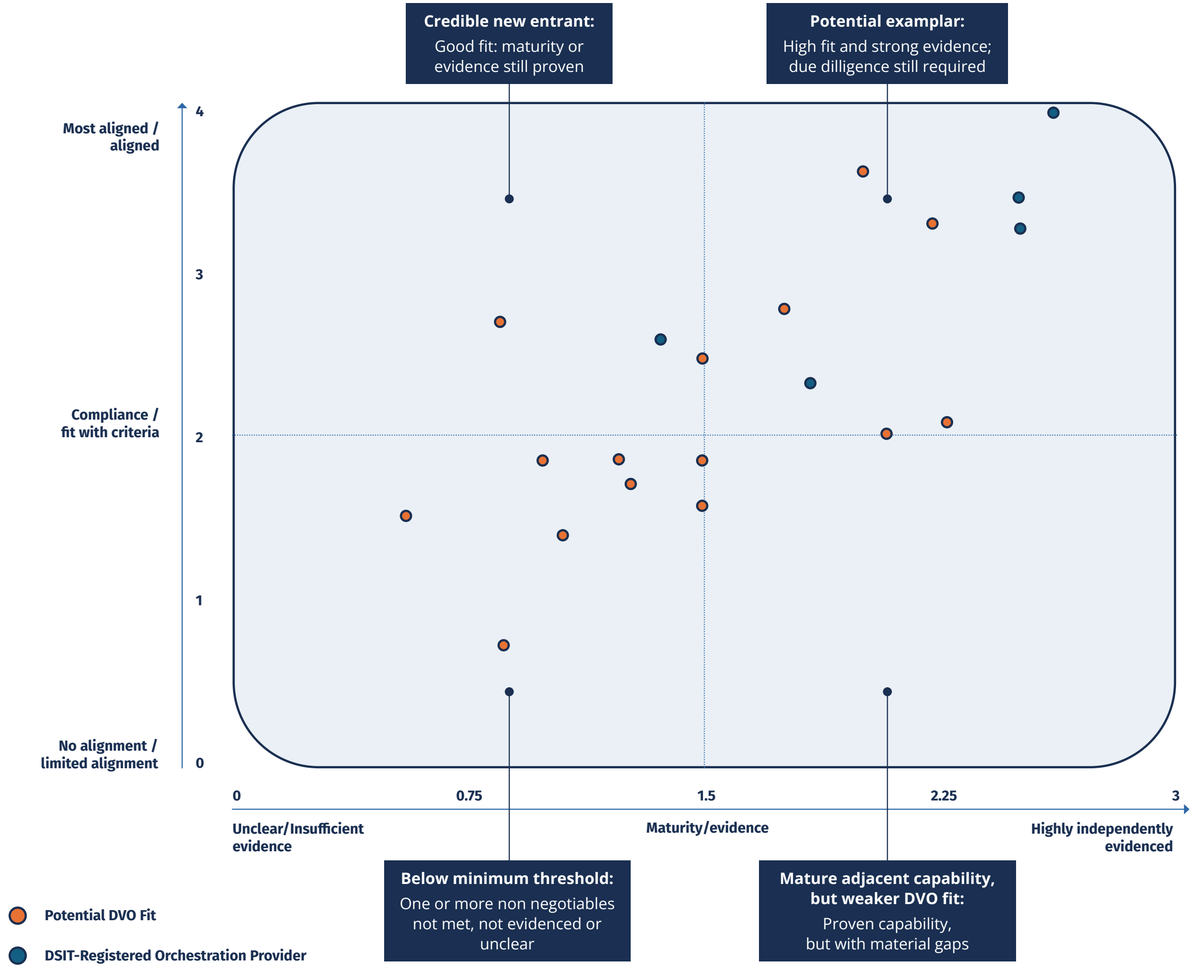


Figure 6: Boston Box showing suggested fit with criteria and strength of evidence/maturity[26].

This Boston Box is intended as a basis for discussion only. It does not substitute for independent due diligence.

The Boston Box suggests that the market contains a base of potentially relevant capability, but that delivery readiness remains uneven. Whilst a number of respondents appear broadly aligned to the proposed DVO role, fewer substantiate that alignment through sufficiently robust evidence, proven implementation experience, and mature operating capability.

This pattern suggests that the market has understood the strategic and functional requirements of a DVO, but that there is greater variation in the extent to which respondents provided evidence on live delivery, accreditation, governance, interoperability, resilience and commercial sustainability through their industry input submissions. Put differently, conceptual fit appears to be more widely distributed across the market than demonstrable operational maturity.

The respondents shown in blue are already registered by DSIT as orchestration service providers, providing an additional lens through which to interpret their position in the Boston Box. Their distribution suggests that existing orchestration registration may be associated with greater readiness to perform aspects of the proposed DVO role, particularly where those respondents are positioned more strongly on both fit and evidence/maturity.

However, the spread of blue respondents also indicates that DSIT registration alone is not sufficient to demonstrate full readiness to act as a DVO, given the broader requirements of the role in relation to governance, interoperability, neutrality, commercial sustainability and stakeholder coordination.

The respondents shown in orange are not currently registered by DSIT as identity, attribute or orchestration service providers. Their position in the Boston Box indicates that some non-accredited respondents may show strong alignment with the proposed DVO role and some operational maturity, based on the evidence submitted. However, further independent due diligence would be required to validate this assessment. Industry feedback suggests that obtaining DSIT accreditation is likely to provide increased confidence in capabilities to deliver orchestration services.

Overall, the Boston Box indicates that the market is not starting from a low capability base, but nor does it yet demonstrate uniformly mature delivery readiness. A small number of candidates positioned in the top right quadrant appear, on the basis of the evidence submitted, to be more advanced in demonstrating readiness to perform the proposed DVO role.

26 Only 20 of the 22 anonymised industry input submissions are shown in the Boston Box as two responses were received from consultancy firms rather than prospective DVO candidates. Of these 20, five companies are accredited as orchestration service providers on the DSIT DVS register (shown in blue). The remaining companies are not accredited on the DSIT DVS register (shown in orange). https://www.digital-identity-services-register.service.gov.uk/register/all-providers. Accessed 9 June 2026.

8. Next steps and recommendations

Taken together, the evidence gathered through the DVO Initiative points to four practical priorities for moving from blueprint to implementation. The recommendations below are intended to support an actionable next phase by focusing on implementation pathways, market conditions and the key issues that will determine adoption.

Recommendation 1: Launch a time-bound DVO pilot programme with committed IDPs, RPs and candidate DVOs.

Who: Industry

What: Within 12 months from the release of this blueprint the following should have occurred; (i) participating financial services institutions (FSIs) should agree the scope of two to three pilots; (ii) participating IDPs, RPs and candidate DVOs should run live or near-live tests across priority use cases; and (iii) the pilots should produce an implementation pack covering secure routing of verified identity and attribute signals, technical interoperability, consent, auditability, data integrity, customer experience, operational resilience, liability, commercial model and scale-up requirements.

Why: This will help move the initiative from blueprint to implementation, strengthen the evidence base through practical testing, and help the potential DVOs reach operational maturity. This will also build the level of institutional commitment needed to support a credible next phase.

Recommendation 2: Confirm the use of verifiable credentials within existing KYC, AML and consumer protection requirements.

Who: Government, regulators.

What: Review and confirm the use of verifiable credentials within the UK's existing AML (including Regulation 28)[27] and consumer protection frameworks. Discussions should focus on any updates to legislation and industry guidance needed to align new digital identity solutions with established regulatory frameworks, preventing gaps or conflicts that could lead to legal risks or enforcement issues. This should include continued review of Regulation 28 of the Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017, and where appropriate a wider review of how verified credentials and reusable digital verification can be enabled within AML processes.

Why: This will help promote industry-wide acceptance and adoption of DV methods, facilitate interoperability, and safeguard consumers by helping ensure that verifiable credentials meet rigorous standards within regulated environments.

Recommendation 3: Embed DVO blueprint capabilities and responsibilities into the DSIT framework to support a neutral, open and interoperable market for orchestration.

Who: Government and industry.

What: Industry should actively engage with government, including DSIT, to establish the DVO as complementary to, and part of, the overall DV framework.

This engagement should ensure that market-led orchestration is recognised and supported alongside any baseline checker or public sector service within the UK's DV framework.

The government approach should remain limited, interoperable, and non-exclusive, with open interfaces that enable certified private sector providers to participate on consistent terms. This includes establishing a clear basis for participation, interoperability, and oversight, whilst ensuring public-sector activities align with market standards and do not create structural advantages for any single delivery route or provider type. Rolling DVO blueprint capabilities and responsibilities into the DSIT DVS Trust Framework would support this given dependence on the Office for Digital Identity and Attributes (OFDiA)[28]. The aim should be to support the further development and practical application of the DSIT DVS Trust Framework, rather than creating a separate or competing regime.

Why: This will provide greater clarity to the market, reduce the risk of fragmentation or lock-in, and support the development of a competitive, trusted and scalable orchestration ecosystem.

Recommendation 4: Develop a liability, participation, and dispute resolution playbook.

Who: Industry, informed by pilot evidence and targeted engagement with government and regulators.

What: Industry should develop a playbook informed by targeted discussions and pilot evidence, to give financial services firms acting as RPs greater clarity on the issues that are material to DVO adoption.

On liability, the playbook should clarify how accountability should be allocated across IDPs, RPs and any orchestrator in different use cases. This should include responsibility for operational failure, quality of data attributes, data loss, data protection and privacy, international data transfers, security and encryption, retention and records, dispute resolution, and interaction with existing contractual and regulatory frameworks.

On non-discriminatory market participation, the playbook should set out the principles and practical conditions needed to support fair, voluntary and pro-competitive participation. This should include openness of access, interoperability, non-exclusivity, objective participation criteria, and safeguards against structural market advantage. The government approach should actively support these non-discriminatory market participation principles, whilst discussions should avoid direct consideration of pricing or other commercially sensitive matters.

Further work will also be required on the commercial and technical decisions that would underpin large-scale implementation, including the appropriate commercial model for priority use cases and the technical pathway needed to support scale, interoperability and resilience.

Why: This will help remove barriers to adoption, support trust in the model, and provide firms with greater confidence in assessing whether and how to participate.

27 Regulation 28 of The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 outlines requirements related to customer due diligence and record-keeping obligations for regulated entities. It mandates how firms must verify the identity of their customers and maintain records to prevent money laundering and terrorist financing.
28 OFDiA is a UK government body responsible for overseeing and regulating digital identity and attribute services to ensure they are trustworthy, secure, and interoperable. OFDiA aims to promote the adoption of digital identity solutions that protect user privacy and enhance confidence in digital transactions.

THE GLOBAL CITY

9. Conclusion and forward look

Trusted DV should be understood as strategic infrastructure for the UK's financial services sector, not simply as a tool for reducing fraud. As financial services become more digital and data-driven across the world, the ability to establish, reuse and trust verified identity and attribute signals will become increasingly important to competitiveness, resilience and innovation. The DVO blueprint provides a practical route to scale by setting out a model for trusted, interoperable verification that can support innovation, improve resilience and enable wider reuse of verified information across institutions.

The evidence gathered through the DVO Initiative suggests that high potential market capability exists, although further independent due diligence and implementation testing will be needed before any delivery model is progressed. The next phase should therefore be deliberately practical: moving from market assessment to targeted pilots that test the DVO model against priority use cases, validate technical interoperability, assess operational resilience, and demonstrate that verified information can be reused securely and efficiently across institutions.

These pilots should be designed to answer the questions that cannot be resolved on paper. They should test how the model performs in live or near-live conditions, how firms integrate into the orchestration layer, how consent and auditability operate in practice, how liability and dispute issues arise in specific use cases, and how the model adapts to emerging risks such as AI-enabled fraud and the transition to PQC.

Implementation of a DVO model will require coordinated action across government, regulators, industry and potential DVOs, but the centre of gravity should now shift from design to demonstration. If delivered well, the DVO model can form part of the trusted digital infrastructure that enables safer innovation, strengthens confidence in cross-border digital services, and positions the UK as a leading market for secure, interoperable and privacy-preserving financial services.

10. Appendix

i. Definitions

Term	Definition
Blueprint	A proposed target operating model for a DVO - defining its role, responsibilities, core capabilities, governance principles, liability considerations, priority use cases and recommended next steps for moving from concept to implementation.
Digital Identity or Digital ID	A digital representation of who a user is. It lets them prove who they are during interactions and transactions. They can use it online or in person.
Digital Verification Service (DVS)	Services that enable people to digitally prove who they are, information about themselves or their eligibility to do something.
Digital Verification Orchestrator (DVO)	An independent entity that facilitates secure information exchange among users, RPs, and IDPs. The orchestrator sets common data-sharing standards, enables the encrypted transfer of high-quality data, whilst prioritising user privacy through consent-based sharing.
Identity Data Providers (IDPs)	Organisations that hold identity data attributes for users, including name, date of birth, address details, unique identifiers such as national insurance number.
Orchestration service provider	An organisation providing a service that makes sure data can be securely shared between participants in the trust framework through the provision of their technology infrastructure.
Relying Parties (RPs)	Organisations that rely on (or 'consumes') certified products or services.
Trust framework	A set of government-approved rules, which draws mainly on existing standards, guidance, best practice and legislation, that organisations agree to follow to have their service certified as a trustworthy digital verification service.
User	A person who uses digital verification services.

ii. Acronyms

Acronym	Definition
ACP	Agentic Context Protocol
AES	Advanced Encryption Standard
AI	Artificial Intelligence
AML	Anti-Money Laundering
APIs	Application Programming Interfaces
CEOs	Chief Executive Officers
CFIT	Centre for Finance, Innovation and Technology
CIFAS	Credit Industry Fraud Avoidance System
DBT	Department for Business and Trade
DSIT	Department for Science, Innovation and Technology
DV	Digital Verification
DVO	Digital Verification Orchestrator
DVS	Digital Verification Services
eIDAS	Electronic Identification, Authentication and Trust Services
EU	European Union
EY	Ernst & Young LLP
FCA	Financial Conduct Authority
FPS	Financial and Professional Services
FSIs	Financial Services Institutions
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
ID	Identity
IDPs	Identity Data Providers
ISO	International Organisation for Standardisation

Acronym	Definition
KYC	Know Your Customer
MCP	Model Context Protocol
OAuth	Open Authorisation
OFDiA	Office for Digital Identity and Attributes
PE	Private Equity
PQC	Post-Quantum Cryptography
PSD2	EU Revised Payment Services Directive
PSR	UK Payment Services Regulations
RPs	Relying Parties
SAML	Security Assertion Markup Language
SCA	Strong Customer Authentication
SLAs	Service Level Agreements
SOC	Systems and Organisation Controls
SSO	Single Sign-On
SteerCo	Steering Committee
TLS	Transport Layer Security
UK	United Kingdom
VC	Venture Capital

iii. Assessment Criteria

The following assessment criteria were used to assess the capabilities of DVO candidates and form a view of the existing market outlook based on industry input.

Criteria	Detail
Technical expertise	• Understanding of digital identity standards and protocols (e.g., OpenID Connect[29], Open Authorisation (OAuth)[30], Security Assertion Markup Language (SAML)[31]). • Knowledge of identity verification technologies and methods (biometrics, document verification, etc.). • Familiarity with security standards (International Organisation for Standardisation (ISO) 27001[32], Transport Layer Security (TLS)[33], encryption methods like Advanced Encryption Standard (AES)-256)[34]. • Experience with integration of multiple identity providers and verification services. • Awareness of the MCP and ACP.
Regulatory and compliance knowledge	• Understanding of data protection laws (e.g., GDPR, Data Protection Act). • Awareness of relevant accreditation frameworks (e.g., DSIT Framework, ICO accreditation[35]).
Operational resilience and risk management	• Ability to manage risk related to data breaches and system vulnerabilities. • Experience in service orchestration and helping ensure high availability and reliability, including system redundancy and management of third-party suppliers. • Knowledge of audit and compliance processes (SOC reports, security audits). • Capable of compliance with Tier IV Data Centre infrastructure standard for availability and redundancy.
Interoperability and standards compliance	• Ability to help ensure interoperability between different identity verification systems and standards (eIDAS, ISO standards (e.g., ISO18013-5 and ISO18013-7[36])). • Experience with frameworks and federated identity management (Including the DSIT Framework).

Criteria	Detail
Communication and stakeholder management	• Ability to work with multiple stakeholders including technology providers, regulators, and business units. • Strong communication skills to explain technical and compliance requirements clearly. • Experience providing dispute resolution process.
Problem-solving and innovation	• Capability to design scalable and flexible orchestration solutions. • Innovative mindset to adopt emerging technologies and standards in digital identity verification.
Experience and track record	• Demonstrated experience in digital identity or verification orchestration roles. • Demonstrated success in managing complex identity verification projects or platforms.
Financial and commercial viability	• Ability to design and operate a financial and commercially viable business model. • Financial resilience, a clear track record of the ability to fund and sustain a commercially successful business. • Evidence of a clear funding plan and viable business model.
Governance and independence	• Strength to act independently among all the parties. • Experience in building and managing governance models.

29 OpenID Connect is an identity layer built on top of the Open Authorisation (OAuth) 2.0 protocol that enables clients to verify the identity of end-users based on authentication performed by an authorisation server. It allows secure and standardised user authentication and single sign-on across different applications and services.
30 OAuth is a protocol that allows third-party applications to securely access a user's resources on another service without sharing the user's credentials. It enables delegated access by issuing tokens that grant limited permissions, enhancing security and user control over data sharing.
31 SAML is an open standard for exchanging authentication and authorisation data between parties, typically between an identity provider and a service provider. It enables single sign-on (SSO) by allowing users to authenticate once and gain access to multiple applications securely.
32 ISO 27001 is a globally recognised standard for information security management systems that provides a framework for establishing, implementing, maintaining, and continually improving information security.
33 TLS is a cryptographic protocol that provides secure communication over a computer network by encrypting data transmitted between clients and servers. It helps ensure privacy, data integrity, and authentication, protecting information from tampering and forgery.
34 AES-256 is an encryption algorithm that uses a 256-bit key to securely encrypt and decrypt data, providing a high level of security.
35 The ICO accreditation is a certification granted by the ICO in the UK demonstrating that an organisation complies with data protection laws and best practices for handling personal data.
36 ISO 18013-5 and ISO18013-7 are international standards that specify the technical requirements for mobile driving licences, enabling secure and interoperable digital identification on mobile devices.

iv. DSIT DVS Register – Certified Orchestration Service Providers[37]

Company	Trading name
T4 Communications UK Limited	Rightcheck
Experian Limited	Experian Ltd
Atlantic Data Ltd	Atlantic Data Ltd
iProov Limited	iProov
Xertilox Ltd	Not applicable
DAON (UK) LTD	DAON
Yoti Ltd	Yoti
Select ID LTD	Not applicable
Nivo Solutions Limited	Not applicable
Arissian Ltd	Luciditi
Mailchain Limited	Vidos
OneID Limited	OneID
ORCHESTRATING IDENTITY LIMITED	Not applicable

v. Participants

DVO Initiative Steering Committee:

The following individuals and organisations are represented on the DVO Initiative Steering Committee:

- **Ezechi Britton MBE (Chair)**
- **Alderman Sushil Saluja (Vice Chair)**
- *Observed by Ian Phoenix, FCA, Hugh de Lusignan, Department for Business and Trade (DBT) and Zish Khan.*
- Barclays – Callum Flaherty
- ClearBank – Joe McCaughran
- Lloyds Banking Group – Rob Jones
- NatWest – Marcus Wogart
- Paragon – Michelle Bradford
- Revolut – Joseph Cordery
- Tide – Tania Tenison-Brownhill
- Visa – Alexander Pospelov

DVO Initiative Working Group:

The following organisations are represented on the DVO Initiative Working Group:

- Centre for Finance, Innovation and Technology (CFIT) - Rob Haslingden
- Innovate Finance - Andy Thornley
- NatWest - Alex Brenig-Jones
- Paragon Bank - Michelle Bradford
- Queen Mary University of London - Dr Nikiforos Panourgias
- Revolut - Joseph Cordery
- Smart Data and Technology Alliance (SDATA) - Ghela Boskovich
- Tide - Jacek Misztal
- University of Bristol - Dr Claudia Peersman
- University of Manchester - Professor Markos Zachariadis

Delivery team:

- Leighton Hughes, Senior Adviser, City of London Corporation - Delivery manager
- Mary Kyle, Head of FPS Technology, City of London Corporation
- Melissa Panszi, Head of FPS Technology, City of London Corporation
- Teresa Clark, Programme Co-ordinator, City of London Corporation
- Ivan Heard, Partner, Financial Crime & Forensics, Ernst & Young LLP
- Peter Hollas, Senior Manager, Financial Crime & Forensics, Ernst & Young LLP
- Lauren McArthur, Senior Manager, Financial Crime & Forensics, Ernst & Young LLP
- Mark Caddy, Founder, Collectively Better
- John Salmon, Partner, Hogan Lovells - Secretariat
- Daniel Lee, Associate, Hogan Lovells – Secretariat

vi. City of London Corporation Contact

- Leighton Hughes, Senior Adviser: TechInnovationTeam@cityoflondon.gov.uk

vii. EY Contact

- Peter Hollas, Senior Manager, Financial Crime & Forensics, Ernst & Young LLP: phollas@uk.ey.com

The views reflected in this article are the views of the author and do not necessarily reflect the views of the global EY organisation or its member firms.

37 https://www.digital-identity-services-register.service.gov.uk/register/all-providers. Accessed 9 June 2026.

About the City of London Corporation:

The City of London Corporation is the governing body of the Square Mile dedicated to a vibrant and thriving City, supporting a diverse and sustainable London within a globally successful UK.

We aim to:

- Contribute to a flourishing society
- Support a thriving economy
- Shape outstanding environments

By strengthening the connections, capacity and character of the City, London and the UK for the benefit of people who live, work and visit here.

www.cityoflondon.gov.uk

About the Global City campaign:

The Global City campaign is the City of London Corporation's overarching initiative to promote the UK as a world-leading international financial centre. It showcases the UK as a great place for financial and professional services firms to invest, locate and grow.

www.theglobalcity.uk

In collaboration with

EY Shape the future with confidence

Hogan Lovells

Collectively Better