

Centre for Finance, Innovation and Technology (CFIT)

Digital Company ID & Fighting Economic Crime: Trust & Governance Framework Working Group

Meeting Minutes

Sprint Session 14

20th November 2025 | In-Person Meeting

Attendees:

Name	Company
<i>In-Person</i>	
Nikki Johnstone (Chair)	A&O Shearman
James McGreevy	CFIT
Sajni Shah	CFIT
Ryan Wu	CFIT
Rob Haslingden	CFIT
John Harrison	UCDx
Leighton Hughes	City of London Corporation
Cindy van Niekerk	Umazi
Glen Keller	CRIF UK
Lewis Utley	DNB
Francis O'Neill	Lloyds
Katarina Pranjic	LexisNexis Risk Solutions
Luca Britos	A&O Shearman
Calum Roberts (Secretariat)	Fuse, A&O Shearman
Katherine Pittalis (Secretariat)	Fuse, A&O Shearman
<i>Online</i>	
Stuart Young	Etive Technologies
Ghela Boskovich	Smart Data and Technology Association (SDATA)

Adrian Field	OneID
Cormac Mealey	EY
Richard Seaman	Dun & Bradstreet
James Deely	Umazi
Mark Terry	Lloyds
David Rennie	OIdentity
Florian Chevoppe-Verdier	DSIT
Daniel Jonas	Pay.UK
Georgina Stracey	A&O Shearman
Xiaodi Wang	GLEIF

Agenda:

- (1) Welcome
- (2) Existing Regulatory / Standards Architecture for Each Use-Case
- (3) Ongoing Validation: Proposed Criteria, Data Sources and Cadence
- (4) Continuous Monitoring: Fraud, Integrity and Exception Handling
- (5) Revocation and Suspension: Statuses, Reasons and Propagation
- (6) Open Discussion: Cross-Sector and Policy Alignment
- (7) Next Steps
- (8) Appendix

1. WELCOME

Speakers: James McGreevy (JM), Nikki Johnstone (NJ)

- 1.1 JM welcomed all participants to the 14th meeting of the Trust & Governance Framework Working Group.
- 1.2 JM reminded all working group members of the importance of adhering to the guiding principles on competition (as set out in the slides) and encouraged participants to engage and collaborate with the working group in an open and respectful manner.
- 1.3 NJ outlined the primary objectives of this meeting:
 - (i) [Extend existing Digital ID regulatory / standard architecture to cover Company ID.
 - (ii) Enhance existing standards / determine criteria for ongoing validation, monitoring, and revocation, including for “reusable” IDs.
 - (iii) Design the implementation roadmap.

2. EXISTING REGULATORY / STANDARDS ARCHITECTURE FOR EACH USE-CASE

Speakers: Nikki Johnston (NJ), Rob Haslingden (RH), Adrian Field (AF), Cindy Van Niekerk (CvN), John Harrison (JH), Ghela Boskovich (GB),

Figure I

	Use Case 1: Bank Onboarding	Use Case 2: Government Servicing	Use Case 3: SME-Supplier Verification	Use Case 4: SME Digital Platform Access
Digital ID regime – UK DIATF (voluntary)	Organisational verification is outside DIATF's supplementary codes; DIATF can still underpin person binding to the organisation			
Sector rules (financial crime/AML)	Corporate CDD requires verifying the legal entity, registration, ownership and control; individual checks apply to beneficial owners/controllers. JMLSG Guidance acknowledges criteria for reliance on Digital ID.	None applicable to corporates.	KYS procurement/finance controls require verifying the entity, VAT/tax status, sanctions; individual checks only for authorised reps.	None applicable to corporates (unless applied at the platform's discretion, e.g. for fraud risk management purposes).
Government supplementary codes (RtW/RtR/DBS)	Not applicable to corporates. Codes apply to individuals only.	None applicable to corporates. Codes apply for individual checks within departments/employers.	None applicable to corporates, other than "right to work" checks.	
Government GPG 45/44 (assurance)	No separate corporate assurance levels. GPG45/55 indirectly applicable to corporates.			
Data protection scope	Corporate data per se is not personal data; UK GDPR applies when processing personal data (e.g., directors, UBOs, authorised reps).	As left. Individual user journeys implicate UK GDPR; corporate attributes implicate GDPR only when linked to identifiable persons.	As left. Supplier onboarding will process both corporate and personal data; apply GDPR to the personal components.	As left. Platform accounts map to individuals; any corporate profile data sits outside GDPR unless it identifies people.

2.1 How can we ensure that Digital Company ID continues to operate in a way which incentivises user and relying party adoption?

- (a) NJ presented the table in Figure I which summarised the current UK regulatory / standards architecture and the extent to which it currently applies directly to Digital Company ID. NJ asked whether corporate-specific adaptations are required for any of the use cases, or whether existing frameworks are sufficient if supplemented by guidance or codes.
- (i) **SME Consideration.** JH highlighted the blurred boundary between very small SMEs (such as sole traders) and corporates, urging a smooth regulatory and operational pathway as businesses evolve from sole trader to a limited company. He proposed that a sole trader's wallet could incorporate a Companies House-verified credential upon incorporation, easing transition, and the regulation should acknowledge and cater for that transition. NJ recommended noting in the report that if Digital Company IDs are looking to service more mature SMEs, then it may make it more difficult for small companies to get set up.
- (ii) **Inclusion of trusts and charities.** CvN queried whether trusts and charities would be in scope for Digital Company ID, suggesting consideration of whether certain trusts should be surfaced in public corporate registries to capture underlying individuals. Participants noted the existence of the TRS (trust registration service), with observations that registries exist but may sit outside Companies House. The point was noted for consideration in the report and a potential recommendation on registry coverage.
- (iii) **Phased Implementation approach.** RH recommended a phased rollout, focusing initially on limited companies as a priority before considering how sole traders and established entities could meet the requirements.
- (iv) **Governance and regulatory coverage.** JH recommended policy action to close the gulf between 'tech' and 'fintech' regulatory regimes. NJ acknowledged that this gap is currently dealt with by regulatory bodies coming together on certain issues but noted the value of DSIT's convening role, with the group likely to recommend increased coordination.

- (v) **Organisational coverage in DIATF.** AF commented on the first line of Figure I's table, noting that the DIATF already contains organisational verification in the context of persons representing organisations. He suggested extending DIATF as the foundational layer for legal persons, rather than creating a separate supplementary code.
- (vi) **Open data and international standards.** CvN emphasised the importance of the Open Data initiative run at Department for Business and Trade (DBT) level which is expanding open banking into open data. CvN queried if the table was focused on the UK, noting that the EU had published recommendations recently. RH responded that there is an opportunity to overlay open data on the data schema for Digital Company ID and that CFIT has reached out to the relevant EU teams to discuss consistency of standards between the UK and EU proposals to leverage future interoperability. GB agreed with CvN and recommended that the DBT's Smart Data Scheme be included in Figure I.

3. ONGOING VALIDATION: PROPOSED CRITERIA, DATA SOURCES AND CADENCE

Speakers: Nikki Johnstone (NJ), John Harrison (JH), Lewis Utley (LU), Rob Haslingden (RH),

Figure II

Area	Suggested criteria	Authoritative sources	Suggested Cadence
Legal existence and status	Company exists, is active, not dissolved / struck off, not in insolvency	Companies House register and status feeds; insolvency notices	Daily pull or event-driven via register updates
Identity particulars	Legal name, registered number, registered office, incorporation date	Companies House canonical data	Daily/event-driven
Entitlements and licensing (sectoral where relevant)	Regulated status, permissions where applicable	FCA/FS Register, Charity Commission, sector registers	Weekly/event-driven
VAT/tax standing (where collected)	VAT registration active; tax reference consistency	HMRC VAT status signals via permitted gateways; HMRC validation responses	Weekly/event-driven
Beneficial ownership and control	PSC data consistent; no conflicting control declarations	PSC register, statutory filings	Event-driven (on filing changes)
Authorised representatives (role binding)	Named persons have verified identities and are entitled to act (director/secretary/appointed signatory)	Companies House verified director/PSC signals; board resolutions; mandate artefacts	Event-driven; annual attestation
Bank account details (for payables)	Account exists, is controlled by the entity	Confirmation of Payee signal, bank-provided evidence	At onboarding; on change; quarterly spot checks
Address and contact integrity	Registered office and trading address validation; registered email maintained	Companies House; address verification services	Event-driven; annual attestation

3.1 NJ presented the table in Figure II which represents standards that could potentially be applied during Digital Company ID checks and the suggested cadence. Currently, Digital Company ID checks are one-off checks and are not intended to be reusable or with ongoing validation. This means that companies cannot use the same ID to validate their identity daily or on monthly bases. The aim, however, is for individuals to use Digital Company IDs in a reusable manner. To ensure this, NJ made the point that maintaining and monitoring are important considerations for Digital IDs. NJ asked the group how realistic it would be to advance the use of reusable Digital Company IDs.

- (a) **International equivalents.** LU recommended framing sources as 'or equivalent' to accommodate non-UK sources. NJ agreed and clarified that many SMEs will rely on UK sources, but international dimensions should be considered in the report.
- (b) **Wallet versus aggregator operational models.** JH distinguished wallet and aggregator paradigms. In a pure wallet model, the SME is the data controller and can present verifiable credentials from trusted sources; the relying party can specify recency (e.g., last month) per

attribute. He noted that certain canonical records (e.g., authorised representatives) might be maintained and propagated via wallet-to-wallet protocols over time.

- (c) **Consent.** RH emphasised consent, use case content, altering, and the contractual responsibilities between the SME and aggregator for maintaining data currency. He underscored the value of user-facing consent dashboards and noted that same data (e.g., fraud flags) cannot be visible to SMEs but still requires controls and signalling.
- (d) **Allocation of responsibility and controls.** JH argued the data controller locus shifts depending on the model (wallet vs aggregator). RH responded that contractual obligations can ensure SMEs maintain accuracy while aggregators verify and signal changes. The group recognised that SMEs cannot see certain checks/data (e.g., AML flags) that may complicate controller responsibilities, supporting an aggregator's role and layered controls.
- (e) **Model presentation.** RH proposed that the report capture the different market models and the differing views each model. The report should acknowledge CFIT will not propose a single model.
- (f) **Validation exercise.** NJ asked the group whether validation should sit primarily with aggregators. The group concluded that validation can be performed by multiple trusted sources, with responsibility varying by model and contract, provided relying parties can see verifiable provenance and recency.

4. CONTINUOUS MONITORING: FRAUD, INTEGRITY AND EXCEPTION HANDLING

Speakers: Nikki Johnstone (NJ), John Harrison (JH), Rob Haslingden (RH), Cindy van Niekerk (CvN), Francis O'Neill (FoN), Mark Terry (MT), Adrian Field (AF).

Figure III

Risk vector	Monitoring control	Trigger thresholds	Required actions
Status change (strike-off, dissolution, insolvency)	Automated status watchlist	Immediate change detected	Suspend Company ID; notify relying parties; initiate re-verification
PSC anomalies	Compare PSC register vs. declared UBOs/mandates	Mismatch, sudden PSC turnover	Investigate; step-up validation; potential suspension
Disqualified/offending officers	Screen authorised reps against disqualification lists/sanctions	Positive match	Revoke rep delegation; reassess Corporate ID
Sanctions exposure	Screen entity and UBOs	Positive match	Suspend; notify; legal escalation
Bank account mismatch	CoP mismatch or frequent beneficiary changes	Repeated failure	Freeze payables attribute; enhanced due diligence
Filing irregularities	Late filings, address hopping, shell patterns	Rule-based scoring threshold	Heightened monitoring; step-up checks
Synthetic/impersonation	Cross-provider anomaly signals; credential misuse	High-risk signal	Forensic review; suspend delegated rights; re-bind reps

4.1 NJ presented the table in Figure III which captured the items that relying parties would expect to be monitored on a continuous basis and flagged by relying parties.

- (a) **Sanctions and AML.** FoN, MT and RH advised against banking 'sanctions' being included in the core Company ID monitoring due to divergent regimes, political dynamics and institution-specific appetites; these are properly part of the bank-specific AML programmes.

MT suggested that it would be sensible to discuss some aspects of sanctions in the report then explore this aspect further at a later stage in consequent discussions.

- (b) **AML / fraud signals and data sharing.** AF noted that regulated entities carry transaction and monitoring responsibility whereas non-AML regulated HSPs could be data sources but should not replicate banks' legal AML duties. He highlighted existing fraud signal-sharing ecosystems (e.g., CIFAS, Synetics) that function as networks, not single repositories. The group discussed JMLIT-like public-private intel sharing for entity risk, while recognising data protection and liability concerns. FoN and MT cautioned not to conflate onboarding with perpetual KYC (which is not the purpose of the coalition), warning of "debanking" risk if centralised adverse signals indiscriminately propagate.
- (c) **Banking mismatch and behavioural indicators.** CvN queried items grouped under the 'bank account mismatch' category, including frequent beneficiary changes and freezable payments. NJ clarified the intent to capture signals beyond CoP mismatches, including changes to ownership / authority and actions on accounts, recognising use-case dependency.

5. REVOCATION AND SUSPENSION: STATUSES, REASONS AND PROPAGATION

Speakers: Nikki Johnstone (NJ), John Harrison (JH), Rob Haslingden (RH), Cindy van Niekerk (CvN), Francis O'Neill (FoN), Adrian Field (AF).

Figure IV

Element	Proposal
Status taxonomy	Valid; Suspended (investigation/temporary non-compliance); Revoked (ceased eligibility)
Reason codes (minimum set)	Legal status change; sanctions/disqualification; verified impersonation/fraud; mandate invalidated; persistent data integrity failure; voluntary withdrawal
Scope of revocation	Entity-level Corporate ID, and/or specific delegated roles (e.g., CFO e-seal key); attribute-level (e.g., payables coordinates)
Propagation	Mandatory near-real-time publication to a trust framework revocation registry; provider-to-provider notifications; relying party webhook/API
User notification and redress	Standardised notices to the entity; appeal window; clear remediation steps; audit trail
Key and credential handling (trust services)	ETSI-aligned certificate/seal revocation and CRL/OCSP updates; rotation of organisation e-seal keys; secure archival

- 5.1 NJ presented the table in Figure IV and requested views on standardising revocation criteria and post-revocation handling, distinguishing voluntary revocation by the company and revocation following monitoring flags.

- (a) **Model-specific propagation.** JH explained that, in a wallet model, attribute authorities can switch an attribute's status which then propagates; in a CRA model, propagation paths are more complex and may not involve the SME, necessitating clarity on agency and trust.
- (b) **Avoiding unintended disruption.** Members cautioned against revocation mechanics that could inadvertently block legitimate activity (e.g., delays in public filing updates or name changes). The group agreed revocation should be attribute-scoped, proportionate, and allow remedy periods and redress for corrections.
- (c) **Supervisory checks and periodicity.** CvN queried how licence loss (e.g., a fintech's authorisation) would be detected and acted upon. FoN outlined differing bank practices:

periodic review cycles versus alert-based “perpetual KYC,” noting legal obligations once alerted and varied appetite for perpetual models. NJ noted these realities should inform revocation and recertification timelines in the framework.


- (d) **Fraud/incident management in DIATF.** AF reminded the group the DIATF already has a whole section on fraud management and incident management around account takeover, account repair, etc. He recommended that it would be useful to understand what is already captured and what corporate ID providers need to consider on top of these existing provisions in this framework.

6. OPEN DISCUSSION: CROSS-SECTOR AND POLICY ALIGNMENT


Speakers: Nikki Johnstone (NJ), James McGreevy (JM)

Figure V

Aside from the technical aspects, what are the biggest dependencies for adoption of the Digital Company ID?

 Anonymous


Government / regulators decision re future of pure play wallets in UK (John H)

 Anonymous

Clarity on the Framework underpinning Digital Company ID - centralised, vs federated vs decentralised

DIATF - extension on company ID

Articulation of benefits to UK SMEs

 Anonymous

Balance between pure wallet model (UCD) and CRA +++ model John H

 Anonymous

Government lead / backed initiative with interoperability with global initiatives

 Anonymous

Being able to effectively verify oneself via Gov One Login (which means it has to work, and not fall over because, say your DVLA-issued driving licence has spelt your middle name wrong) - DJ

6.1 Aside from the technical aspects, what are the biggest dependencies for adoption of the Digital Company ID?

- (a) NJ presented the question for the group and requested feedback via a Slido poll which is demonstrated in Figure V. She asked working group members about what their priorities are in terms of engagement and dealing with dependencies and how best these dependencies can be addressed regarding changes in regulation, government guidance or purely a market-driven perspective on what the industry can realistically achieve.
- (b) JM requested that group members complete inputting suggestions and their answers for the Slido question ahead of the next sprint.

7. NEXT STEPS

The 15th sprint will be held on 5th December 2025. This sprint will focus on gap analysis from previous sprints.

8. APPENDIX

AML – Anti-Money Laundering

CIFAS - Credit Industry Fraud Avoidance System

DBT - Department for Business and Trade

DIATF – Digital Identity and Attributes Trust Framework

DSIT – Department for Science, Innovation and Technology

JMLIT – Joint Money Laundering Intelligence Taskforce

KYC – Know Your Customer

SME – Small and Medium-Sized Enterprise

TRS – Trust Registration Service