

Decision Intelligence PoC – Assurance DocumentED level

Version	Author	Description	Date
1.0	[REDACTED] [REDACTED] [REDACTED]	Initial Version to Executive Directors for review and sign-off on PoC go-ahead	15/05/2026
1.1	[REDACTED]	Updates made following questions from Sheree via email. Section 1 updated with sub-sections 1.1, 1.2, 1.3, 1.4, 1.5. Section 1.5 updated Section updated 4.2 (RR-01)	20/05/2026
1.2	[REDACTED]	Updated Executive Director Sign-off section Updated Section 10.3 and Section 11.2 Updated formatting issues on section 12. SMF Sign-offs not impacted.	22/05/2026

Executive Director/SMF Sign-offs for PoC:

Executive Director (SMF)	Email Evidence	Date
Sarah Pritchard	Sarah Pritchard Sign-off Fw ACTION Palantir Decision Intelligence Proof of Concept — Request for Executive Director Sign-off.msg	21/05/2026

Stephen Smart	<u>Stephen Smart sign-off Fw ACTION Palantir Decision Intelligence Proof of Concept — Request for Executive Director Sign-off.msg</u>	20/05/2026
Sheree Howard	<u>Sheree Howard sign-off Re ACTION Palantir Decision Intelligence Proof of Concept — Request for Executive Director Sign-off.msg</u>	21/05/2026
Jessica Rusu	<u>Jessica Rusu Sign-off Fw ACTION Palantir Decision Intelligence Proof of Concept — Request for Executive Director Sign-off.msg</u>	22/05/2026

1. Executive Summary

- 1.1 The Decision Intelligence Proof of Concept (PoC) purpose is to evaluate how emerging decision-support technologies—such as unified enterprise search, integrated analytics, harm-detection capabilities, and improved intelligence delivery—could strengthen regulatory effectiveness across Enforcement, Authorisations, Supervision, Disclosure, and Intelligence functions. As a result of market research and engagements, the direction signed off at TSG is to explore these technologies have the potential to be transformative in the fight against financial crime and to support AML reform. This also aligns with the FCA’s Architectural principles as set out by the Strategy and Architecture team [REDACTED]. In addition, where relevant, insights generated through the PoC may be shared with appropriate supervisory or intelligence teams via existing FCA governance, workflows, and decision-making processes.
- 1.2 The PoC is proposed to run over 12-week and will focus on validating data ingestion, harm identification, enterprise search and auditability of a leading Decision Intelligence platform. Through a competitive tender exercise (via the government G-Cloud

framework) Palantir has been selected to support this POC. To ensure the POC is effective TSG proposed that data from the FCA production systems and live environments is used and that this data is loaded into Foundry, Palantir's UK hosted system for data integration / mining. This POC will support the FCA's wider [Decision Intelligence Vision](#), without committing prematurely to a long-term strategic solution. Once the POC is complete the FCA instance of Foundry (and all data contained within the instance) will be destroyed. This will be evidenced to FCA upon completion of the POC as standard practice and contractual obligation (further details in Section 16).

1.3



1.4



1.5 Accountable Executives for the PoC:



- i. Decision Record: [UPDATED FW Decision Intelligence PoC — Joint Accountable Executive Appointment \(1\).msg](#)
- ii. Three AEs have been assigned for this PoC: two AEs have been chosen who are in DTI and one who is from Enforcement as the business lead. While a PoC does not formally require an Accountable Executive, the circumstances of this programme clearly warrant one. Putting named, senior accountability in place is the right governance response to the level

of attention this programme is receiving, and it is consistent with the FCA's accountability standards for programmes of this sensitivity

- iii. Digital Intelligence Solution (DIS) team leads the delivery of the PoC and the DTI assurance work. Strategy and Architecture (S&A) identified the Decision Intelligence Platform as a critical path item for our AML reform programme, led the architecture governance through TSG and FDAG. Enforcement teams have provided the SMEs which were used to build the use cases and provide the business sponsorship for this piece of work (refer to Section 9 for more details).
- iv. Second Line: Steve Smart (Executive Director of Enforcement and Market Oversight) and Jessica Rusu (Executive Director of Digital Technology and Innovation).

2. Purpose of this Document

This document provides an auditable record of all governance, assurance processes, and stakeholder engagement undertaken throughout the Decision Intelligence PoC. It specifically documents:

- i) Architecture and S&A governance
- ii) Procurement and commercial approvals
- iii) Legal, data protection, and assurance engagement
- iv) Business and external/internal stakeholder engagement activities
- v) Data Sets in Scope for PoC
- vi) Success criteria of PoC
- vii) Risk Register and Controls
- viii) Timeline
- ix) RACI
- x) Incident Management
- xi) Communication Approach

The aim is to demonstrate that appropriate and proportionate FCA governance routes were followed, consistent with expectations for a PoC involving FCA-held regulatory data.

3. Scope of the FCA Data to be used in the PoC

The PoC will use a *targeted and minimised dataset*, restricted to a [REDACTED] range and limited to sources required to validate Enterprise Search and Harm Detection use cases and wider decision intelligence capabilities within a supplier platform.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

4. Key Risks Identified

4.1 The risks set out below represent the key material risks identified through a combination of early design review, governance engagement and assurance activity undertaken in advance of the PoC. They have been derived from:

- [REDACTED]
- The Data Protection Impact Assessment (DPIA), including assessment of risks to individuals' rights and freedoms;
- C&IR security engagement, including review of hosting, access controls and supplier arrangements; and

- Architecture and governance discussions through TSG and FDAG, including consideration of data scope, hosting options and supplier risk.

The risks listed below are not intended to be a comprehensive risk register. Rather, they summarise the principal cross-cutting risks that were assessed as most material to the PoC and therefore required explicit mitigation and governance oversight. Detailed risk considerations and mitigations are documented in the referenced artefacts (including the Risk Register, DPIA, Legal advice sections).

4.2 As part of **pre-trial assessment with C&IR and TSG for the PoC**, several material risks were identified relating to:

- i) [REDACTED]
- ii) **Data Sovereignty and Political Sensitivity** – relating to the use of a US owned supplier and perceived exposure to extraterritorial legislation
- iii) **Public Trust and Ethical Considerations** – driven by external perceptions of Palantir’s association with national security and intelligence sectors

The table below summarises six key Decision Intelligence PoC risks, setting out what could go wrong, the potential harm, the assessed residual risk, and the rationale for accepting each risk. It is intended to support effective oversight and informed decision-making, with **detailed controls and analysis retained in the [full risk register](#)**. All the Owners of these risks are at Senior Manager Function (SMF) level.

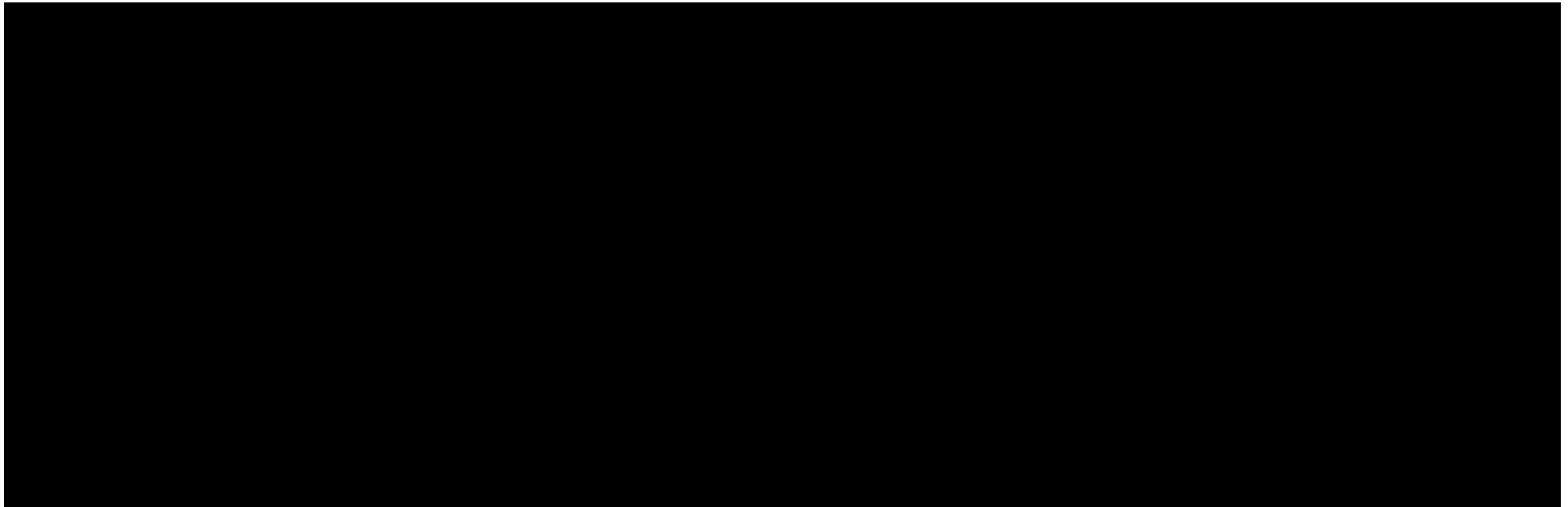
Risks were presented to TSG and FDAG, where they were all accepted. The meeting minutes are evidence of these discussions.

Risks have been accepted by Executive Directors as part of PoC sign-off (refer to sign-off table above section 1.0).

5. Mitigating Controls

To address the identified risks, the PoC adopts the FCA’s comprehensive, multi-layered control environment, aligned to the [REDACTED] and FCA operational risk standards. More details are available in further section but some of the key controls summarised here:

- i) **Legal & Regulatory Controls**
 - a. [REDACTED]
 - b. Strict data minimisation applied, with insider and whistleblowing records excluded.
 - c. RBAC inheritance, full audit logs, versioning, and justification prompts ensure defensible and auditable access.
- ii) **Data Sovereignty Controls**
 - a. All PoC data hosted exclusively in [REDACTED].
 - b. Encryption and logical segregation enforced throughout.
 - c. Customer-Managed Encryption Keys (BYOK)
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- iii) **Public Trust & Transparency Controls**
 - a. A DPIA has been reviewed by C&IR [REDACTED]
[REDACTED]. **Refer to Section 13.**
 - b. Access is restricted to selected, relevant data sources, with all datasets limited to a maximum of [REDACTED], ensuring data minimisation.
- iv) **Technical & Security Controls (reviewed by C&IR and signed off at TSG – refer to Section 7.2)**
[REDACTED]
[REDACTED]
[REDACTED]
- v) **Governance Controls**
 - a. Structured 12-week PoC lifecycle (Scoping → Build → Testing → Evaluation).
 - b. FCA data only to be loaded into FCA specific instance of Foundry
 - c. FCA instance of Foundry (and all data contained within the instance) to be destroyed at the end of the POC. This to be evidenced to FCA upon completion of the POC via certification from Palantir and manual check by FCA Architectural staff of the FCA’s domain in Foundry.
 - d. **Oversight from TSG (twice), FDAG, C&IR and Legal as part of pre-PoC assurance.**
 - e. Engagement from circa 20 SMEs and the application of formalised success criteria.



6. Strategy and Architecture

6.1 Key Activities and Artefacts prior to the PoC:

- **Decision Intelligence Workshop (July 2025)**
 - Early cross-FCA engagement workshops in July 2025 were led by [REDACTED] to establish a shared understanding of intelligence workflows - [Intelligence Architecture Review Workshop](#)
- **Decision Intelligence Architecture Vision (December 2025)**
 - The Architecture Vision and corresponding FDAG approval set the strategic direction for the Intelligence capability, ensuring alignment with FCA priorities and establishing the architectural baseline.

- **Enterprise Search Architecture Decision (December 2025)**

- The Search & Discovery – Enterprise Search PoC AD formalised the case for undertaking the supplier PoC and defined architectural constraints and expectations

6.2 Governance Assurance

- S&A's governance role is evidenced through consecutive approvals and endorsements:

Board	Minutes	Paper(s)	Type	Decision Summary	Decision	Author
FDAG	FDAG 28 Apr 2026	(1) FDAG Presentation (2) Decision Intelligence & Enterprise Search Platform AD PoC Hosting	Architecture Decision	[REDACTED]	Approved; refer to FDAG meeting minutes on the left	[REDACTED]
TSG	20 Apr 2026 Palantir PoC AD Refresh - Meeting Outcome.msg	Decision Intelligence & Enterprise Search Platform AD PoC Hosting	Architecture Decision	[REDACTED]	Approved; refer to TSG meeting minutes on the left	[REDACTED]
TSG	TSG 10 Mar 2026	Decision Intelligence & Enterprise	Architecture Decision	Use FCA Production Data for the 12-Week Palantir Foundry PoC	Approved; refer to TSG meeting	[REDACTED]

		Search Platform AD PoC			minutes on the left	
FDAG	FDAG 11 Dec 2025	Architecture Vision Decision Intelligence Briefing	Architecture Vision		Approved; refer to FDAG meeting minutes on the left	
TSG	TSG 01 Dec 2025	Architecture Vision Decision Intelligence	Architecture Vision		Supported; refer to the TSG meeting minutes	
TSG	TSG 17 Nov 2025	Search and Discovery – Enterprise Search PoC AD	Architecture Decision		Approved; refer to the meeting minutes	

Strategy and Architecture Governance Boards

7. Use of data in support of statutory objectives, legal compliance and ethical standards

- 7.1 Data used within the Decision Intelligence / Enterprise Search Proof of Concept is processed solely in support of the FCA's statutory objectives, including supervision, harm detection and enforcement, and in line with applicable legal, regulatory and ethical requirements.
- 7.2 The PoC does not introduce a new purpose for processing. It tests an alternative technical means of analysing data already lawfully held by the FCA, with use cases explicitly aligned to active supervisory and enforcement activities. Processing is

time-limited, proportionate, and subject to strong technical and organisational safeguards, ensuring that the FCA retains control over how data is accessed, used and shared throughout the PoC lifecycle.

- 7.3 Compliance with legal, data protection and ethical requirements is being demonstrated through a **Data Protection Impact Assessment (DPIA) that is in the final stages of review**, [REDACTED], [REDACTED], alignment with the FCA's published privacy notices, and oversight from C&IR, Architecture governance and accountable business owners. These artefacts collectively evidence that data use within the PoC is intended to be lawful, fair, transparent and proportionate, [REDACTED].

8. Procurement & Commercial Assurance

8.1 Supplier Selection, Scope Boundaries and Data Handling (Public Narrative):

- i. The Decision Intelligence Proof of Concept (PoC) supplier was selected through a competitive procurement process conducted under the Crown Commercial Service (CCS) G-Cloud framework, in line with FCA procurement policy and applicable procurement law. The process included formal evaluation of supplier responses against defined technical and commercial criteria. [REDACTED]
- ii. The scope of the PoC is strictly time-limited and non-operational, designed solely to evaluate decision-support capabilities rather than introduce a production system. The PoC operates within clearly defined boundaries, including UK-only hosting of data, the use of a dedicated FCA instance, and the application of strong technical and governance controls. FCA data always remains under FCA control, and the PoC explicitly prohibits the use of FCA data for model training, fine-tuning, or any purpose beyond the defined PoC use cases. Data use is restricted to a targeted and minimised dataset, aligned to specific use cases and subject to legal, data protection and security assurance processes.

- iii. At the conclusion of the PoC, all FCA data and derived artefacts—including indexed data, analytical outputs, logs (where applicable), and backups within the PoC environment—are subject to a mandatory, contractual deletion requirement. This deletion is not discretionary and is enforced through both contractual obligations and technical controls. Assurance of deletion will be provided through a combination of formal supplier confirmation, technical verification, and manual checks performed by FCA staff, with evidence retained as part of the PoC governance record. Completion of verified deletion is a precondition for formal PoC closure, ensuring that no FCA data is retained beyond the duration of the PoC.

iv.

[REDACTED]

8.2 [REDACTED] approvals below:

8.3 **Enterprise Search Decision Intelligence PoC – [REDACTED] Approval Request**

Evidence of formal procurement approval workflow.

[REDACTED]

8.4 [Contracting 2025 - C3812 - All Documents](#) – contains all documents relating to the procurement Bid Responses. Excludes the moderation documents as that is sensitive and cannot be distributed wider.

8.5 Statement of work we issued to market (06/12/2025): [Scope of Requirement - ESearch POC v2 Final.docx](#)

a.

[REDACTED]

b. [RE DUIE Decision intel procurement .msg](#): email of C&IR engagement to feed into SOW before going to market (18/1/2025).

c. Went to market on 06/12/2025 (via [REDACTED])

- 8.6 **Technical evaluation – 16/12/2025** (due to sensitivity they cannot be widely shared but the documents are stored within this folder: [Contracting 2025 - C3812 - Bid responses - All Documents](#)).
- 8.7 4 evaluators were involved in the technical evaluation where bidders responded to clarification questions.
- 8.8 **Contract award – 31/01/2026** ([REDACTED] sign-off). [CCS Call Off Contract with \(FCA\) countersigned 090226](#)
- 8.9 **FCA Reputation handling – RE DIP PoC ESG Response from Procurement.msg** – from Procurement Senior manager confirming how reputation is handled during the G-Cloud process which falls under ESG. [REDACTED]
[REDACTED]
-

9. Business & Stakeholder Engagement

9.1 Purpose of Business Engagement

- 9.2 Business engagement for the Decision Intelligence / Enterprise Search PoC was undertaken to ensure that:

Alignment between front-line teams and the use-cases (i.e. co-create use cases)

Use cases are **clearly articulated, justified, and proportionate** to the data being used;

Align with SMEs on the fact the PoC remains aligned to **active supervisory, intelligence and enforcement activities**, rather than exploratory or speculative use; and

Appropriate **business ownership and accountability** exists for the use cases, and insights generated during the PoC.

9.3 Use-Case Development and Validation

Business engagement was anchored around the development and validation of **clearly defined use cases**, documented in the following artefacts:

9.4 The table below mentions all the SMEs that will support the review of outputs from this PoC:

Business Lead		EMO Lead representative on behalf of Karen Baxter and Steve Smart
SPC engagement		Signed-off SharePoint data site: RE Decision intel proof of concept - fincrime dept .msg
EMO SME		
EMO SME		
EMO SME		
EMO SME		
SPC SME		

9.5 – contains the slides from SME engagement session

9.6 – Here are the use cases which were created with SME collaboration.

10. Staff and Union Engagement

- 10.1 The Decision Intelligence PoC has attracted internal staff and union interest, reflecting the sensitivity of the initiative and its external profile. This has included correspondence and engagement raising questions in relation to data use, supplier involvement and broader transparency considerations.

This engagement has been managed through established FCA governance, Communications, Legal and programme processes, ensuring that responses are coordinated, accurate and consistent with the FCA's legal and policy position. Responses have focused on clarifying the purpose and scope of the PoC, reinforcing that it is time-limited and non-operational, and confirming that strong governance, legal and technical controls are in place, including the application of data minimisation and appropriate safeguards for staff information.

Internal communication to FCA staff has been delivered through formal FCA channels, including Pulse articles. These communications set out the purpose of the PoC, its alignment to the FCA's statutory objectives, and the safeguards governing the use of data, including how staff information is handled in a proportionate and controlled manner. This ensures that internal messaging is transparent, consistent and aligned with external communications and legal advice.

- 10.2 Engagement with staff representative structures has been undertaken through the Staff Consultative Committee (SCC) on **25th March**. This engagement was led by senior FCA leadership, including Ian Phoenix (Director of Intelligence & Digital), Jessica Rusu (Executive Director), Steve Smart (Executive Director of Enforcement), and [REDACTED]. The purpose of this engagement was to provide transparency on the PoC, its scope and safeguards, and to enable discussion and challenge within a formal staff-representative forum.
- 10.3 The SCC has therefore been engaged and informed as part of the PoC governance process. No formal decision or approval from the SCC was required for the PoC to proceed. Letter response to Union has been sent on 22/05/2026 (please see email: [FW Decision Intelligence Proof of Concept - FCA Response to the Unite FCA Branch.msg](#)) with their automated response email received on 22/05/2026 (please see email: [FW Thank you for your email Re Decision Intelligence Proof of Concept - FCA Response to the Unite FCA Branch.msg](#)). Engagement is recorded as completed for assurance purposes.

Overall, this demonstrates that staff and union engagement has been actively managed, with correspondence formally addressed, internal communications issued through established channels, and appropriate engagement undertaken with staff representative bodies in line with FCA governance expectations.

10.4 Here are the internal communications that was sent out post engagements:

10.5 [Fighting crime and our work with Palantir](#) – Internal Pulse article to all staff which outlines the PoC and explicitly references Nikhil Rathi, Jessica Rusu and Steve Smart's Treasury Select Committee questions on this piece of work

10.6 [Update to the recent Pulse article on our work with Palantir](#) – article that explicitly relates to some staff questions about what information is being shared and responds with factual statements that *"we are not sharing any sensitive personal or HR data about FCA colleagues with Palantir."*

11. Datasets Scoped for the PoC

11.1 Applicable policy and governance framework

The use of FCA data within this Proof of Concept is governed by the FCA's Information Security and Data Classification Policy framework, FCA Data Governance principles, and established PoC assurance and architecture governance standards.

These frameworks require that:

- Data is classified and handled in accordance with FCA Official and FCA Sensitive handling requirements;
- Data shared with third-party processors for PoC purposes is subject to appropriate technical, contractual, and organisational safeguards; and
- Explicit approval is obtained from accountable Executive Data Owners.

These requirements are implemented alongside oversight from Architecture governance (TSG / FDAG), C&IR, Legal, and completion of an approved DPIA, ensuring that data use within the PoC is lawful, proportionate, time-limited, and auditable.

11.2

[REDACTED]

[REDACTED]

11.3 **Dataset choice and proportionality** - Datasets chosen for the PoC have been driven by the use cases (Enterprise Search and Harm Detection) where a mixture of structured and unstructured data has been chosen along with data from multiple

repositories. Data Minimisation will be applied to certain datasets, to exclude Staff information, as per DPIA. Please refer to dataset details on which datasets. [DIP ES PoC Data Set Scope](#)

11.4 Data Owner Sign-off will occur with EDs as the ultimate owners of data based on division across the FCA, at Senior Manager Function level (SMF).

- i. Sign-off by EDs means we will ingest into Foundry data stored in [REDACTED] and selected sites records from [REDACTED] (from slide above) to be processed for harm detection and indexed for enterprise search to help us identify patterns of harm not currently known and verify past harm patterns and discover records.
- ii. Executive Directors to seek sign-off: Jessica Rusu, Sheree Howard, Sarah Pritchard, Steve Smart
- iii. **Once sign-off is given by Executive Directors, date and name will be recorded in page 1 of the file.**
- iv. **Following Executive Director review, a list of data owners and confirmation of their awareness of the trial will be maintained as part of the ongoing governance record based on the names listed in the file in section 11.2.**
- v. **Maintenance of the ABO, DMO, Data Owner lists are an on-going maintenance activity due to Joiners Movers and Leavers**

11.5 Policy basis for dataset inclusion in the PoC

The inclusion of datasets within this Proof of Concept has been assessed in line with the **FCA Data Management Policy** (link: [04.10.24 Data Management Policy CLEAN FINAL V2.1.pdf](#)), which applies to all secondary use of data, including Proofs of Concept.

The Policy does not prescribe a fixed list of datasets that may or may not be used in PoCs. Instead, it requires that any secondary use and data sharing is governed through **Data Owner accountability, oversight of access and usage, adoption of applicable data sharing and data usage standards, and demonstrable assurance that data will be registered, controlled, used and disposed of appropriately.**

In line with **Requirement 6** (oversight and control of data usage), **Requirements 19 and 20** (adoption of data sharing, data protection and security standards), and **Control 7 (Data Usage Standards)**:

- the intended use is understood and aligned to FCA statutory functions (Sections 11 and 12 covering the DPIA [REDACTED]);
- risks associated with secondary use have been identified and assessed (C&IR reviewed as part of TSG sign-off in Section 6.2);
- proportionate technical, organisational, and contractual controls are in place (refer to the Call of Contract with Palantir and DPIA); and
- data disposal at PoC completion can be assured (refer to Section 16).

As the PoC involves sharing FCA data with an external supplier environment, it constitutes **data sharing for the purposes of the Data Management Policy as Palantir engineers will be required to see data to delivery this PoC**. The formal data sharing arrangement for the PoC is provided through the **G-Cloud 14 Framework Agreement (RM1557.14)** and the associated **Call-Off Contract**, rather than a bespoke data sharing agreement. In particular:

- **Clause 28 (Data protection and disclosure)** establishes the lawful basis for sharing FCA data and mandates compliance with data protection legislation.
- **Schedule 7 (Processing Data)** sets out the binding data sharing terms, including controller/processor roles, permitted processing, security requirements, audit rights, international transfer restrictions, and data retention and deletion obligations; and
- **Annex 1 (Processing Personal Data)** to Schedule 7 defines the scope, purpose, duration, and categories of personal data processed for the PoC, as completed through the Call-Off Contract.

This reflects a **risk-based and policy-compliant application** of the FCA Data Management Policy, rather than a distinction based solely on system, platform, or data classification. **FCA staff personal data will not included in the PoC, where a risk based approach will be taken as well to be proportionate.**

Given that scope of data required for the PoC, approval will be sought Senior Manager Functions (SMFs), Executive Directors, whom are, Jessica Rusu (Executive Director and CDIO), Sarah Pitchard (Executive Director and Deputy CEO) and Sheree Howard (Executive Director of Authorisations) and Steve Smart (Executive Director of Enforcement).

11.6 [RE DIP POC - data owner governance.msg](#) email confirming data sharing agreement covered under the contract and reviewed with Legal.

11.7 In addition, explicit confirmation that:

- No additional Data Governance or AI Governance forums or IGBs were required for the PoC. Email: [FW DIP ES PoC with Palantir Data Gov AI Gov.msg](#)

13 Data Protection Impact Assessment (DPIA) for the PoC

13.1 DPIA Document Link: [Data Protection Impact Assessment \(DPIA\) Template v3 DIP PoC.xlsm](#)

Email correspondence reharding DPIA:

[RE DIPES PoC with Palantir.msg Legal correspondence.msg](#)

[RE DIPES PoC with Palantir.msg C&IR correspondence.msg](#)

Sign-off: Kevin Thrope (DPO): 28/04/2026. Email:

13.2 [RE catch up re DPIA - PalantirUS cloud act.msg DPO Sign-off.msg](#) - its agreed that DPIA is a living document.

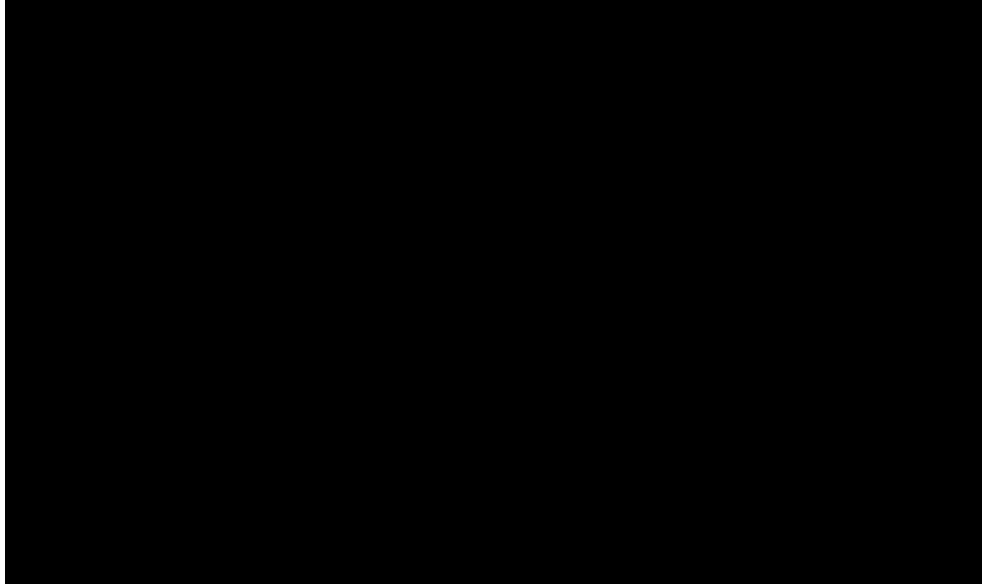
13.3 *Summary of DPIA:*

The DPIA confirms that the Decision Intelligence PoC represents a lawful, fair and proportionate use of personal data in support of the FCA's statutory functions. The processing is time limited and subject to strong technical, contractual and organisational controls, with low residual risk to individuals' rights and freedoms.

However, given the use of production data to measure value, any new harm identified will thus be acted upon through the relevant internal processes, giving this supervisory purpose as well.

The DPIA has been reviewed by C&IR and provides sufficient assurance for the PoC to proceed on the documented basis.

13.4 [Re DIP PoC Question regarding Hosting.msg Palantir to FCA email.msg](#) about data sovereignty on the AI components



- 13.5 [RE DIP PoC with Palantir - Privacy Notice Query.msg](#): Kevin Thrope (Data Protection Officer, FCA) has confirmed via email that the purposes for processing data have been continuous and **consistent with the current and previous versions of the Privacy Notices**, and the PoC is a continuation of existing functions, with transparency provided through staff updates and external publicity. This falls within the current period of data the PoC will be using (Jan 2024 to Dec 2025). If the PoC is successful and a permanent solution is considered, the processing position will need to be revisited in the future again.

14. Retention and deletion

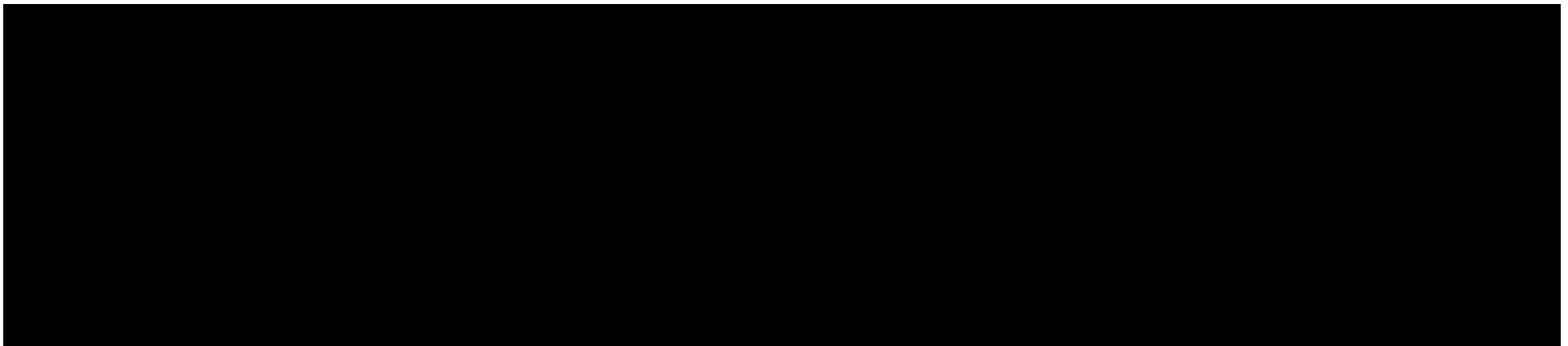
- 14.1** The FCA remains the sole Data Controller for all data used within the Decision Intelligence PoC. Palantir acts strictly as a Data Processor and may process FCA data only in accordance with the FCA's documented instructions and contractual obligations.
- 14.2** All FCA data ingested into the PoC environment is subject to a mandatory, time-limited retention period aligned to the 12-week PoC lifecycle. No FCA data may be retained, reused, copied, or repurposed beyond the PoC.
- 14.3** Deletion of all FCA data and any derived artefacts (including indexes, logs, analytical outputs, and backups) is a contractual and technical requirement, not a discretionary activity. Deletion will be executed immediately upon PoC completion and is enforceable through contractual terms, platform controls, and FCA oversight.
- 14.4** Palantir as per the contract will retain security logs, which are deemed standard industry practice and has been reviewed and accepted by C&IR (refer to TSG approval in Section 6.2 under TSG 10th March).
- 14.4.1** Data cannot be recreated from these security logs as they contain no FCA identifiers as per email: [Re DIP PoC Question regarding Hosting.msg Palantir to FCA email.msg](#)
- 14.5** Assurance of deletion will be evidenced through a combination of:
- Formal confirmation from the supplier that all FCA data has been securely deleted in line with contract requirements;

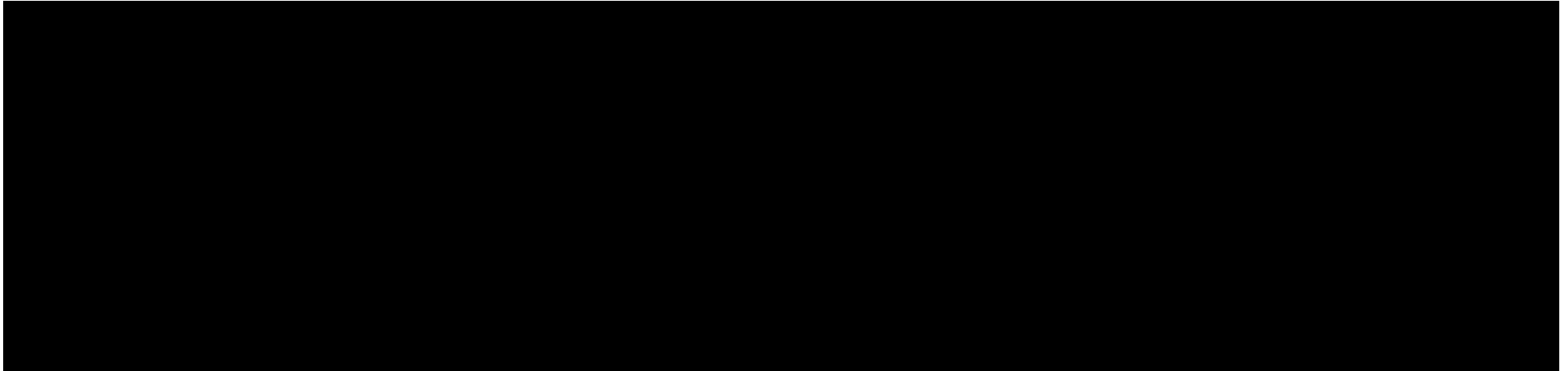
- Technical verification and manual checks performed by FCA staff with appropriate access; and
- Retention of deletion evidence as part of the PoC assurance record.

14.6 Completion of data deletion, and receipt of satisfactory evidence, is a pre-condition for formal PoC closure.

15. Success Criteria for PoC sets out how the PoC outcome will be judged in conjunction with the use cases that have been collected.

- I. The PoC is considered successful if it demonstrates that decision intelligence capabilities can meaningfully improve FCA workflows and inform future Search & Analytics (S&A) and technology decisions.
- II. [DIP PoC Success Criteria.docx](#) – document that contains all the success criteria in detail.
- III. Summary of key success criteria





IV. Sign off will be taken from various stakeholders:

Business Sign-off will be from EMO SMEs at Use Case Level and by HoD as Business Lead

Analytical Sign-off will come from DIS/DUIE HoD and Lead

Security and Audit Sign-off will come from C&IR consultant and Director as second line

Architectural Sign-off will come from S&A senior manager and HoD

16. Incident Management Process

- I. Incident management during the DIP PoC will be undertaken in line with established FCA processes. Operational incidents will be managed in accordance with the FCA Incident Management Process (A5), including prioritisation based on impact and urgency and formal tracking through the ITSM toolset. Any control failures, policy breaches or near-miss events will be recorded and managed as Risk Events in line with the [FCA's Approach to Risk Event Management \(March 2026\)](#), ensuring consistent identification, capture, assessment and escalation in accordance with the FCA Risk Management Framework.

Scenario	FCA Process Applied	Reference
Operational incident (e.g. service disruption, system issue)	Managed in line with FCA Incident Management Process, including prioritisation, incident ownership and resolution tracking	A5. Incident Management Process (V1.24)
Control failure, policy breach or near miss	Recorded and managed as a Risk Event, including capture, assessment and escalation	FCA's Approach to Risk Event Management (March 2026)

18. RACI

Appendix X – RACI Matrix (Decision Intelligence PoC)

Roles: Project Lead | Lead Architect (FCA) | Lead 3rd Party | Accountable Exec | 2nd line | Executive Director

Project Lead(s): [REDACTED]

Lead Architect (FCA): [REDACTED]

Lead 3rd Party: [REDACTED] (Palantir)

Accountable Exec: [REDACTED] (decision email: [FW Decision Intelligence PoC — Joint Accountable Executive Appointment.msg](#)).

Executive Director: Steve Smart, Jessica Rusu

Activity / Deliverable	Project Lead	Lead Architect	3rd Party	Accountable Exec	2 nd line (C&IR / Legal)	Exec Director
PoC scope definition	R	A	C	C	C	I
Architecture design & approvals	C	R	C	A	C	I

Production data approval	C	R	C	A	C	I
Dataset selection	R	C	C	A	C	C
Data Owner sign-off	C	C	I	C	I	A
Legal & regulatory compliance	R	C	I	A	C	I
DPIA	R	C	I	A	C	I
Procurement	R	C	C	A	C	I
Security assurance	C	R	C	I	A	I
Technical controls	C	A	R	I	C	I
PoC delivery	R	A	R	C	I	I
Monitoring & logging	C	A	R	I	C	I
Business engagement	R	C	C	A	I	I
Output validation	R	C	I	A	C	I
Risk & acceptance	C	R	I	A	C	I
Incident management	R	C	C	A	C	I

Evaluation	R	C	C	A	C	I
Data deletion	C	A	R	C	C	I
Deletion verification	R	A	C	C	C	I
PoC closure	R	C	C	A	C	I

