Open Source Intelligence Support Service Definition

Document title	Open Source Intelligence Support Service Definition		
Reference No.	IF-SER-025	**Version**	1.0
Author	Simon Young, Digital Investigations Manager		
Reviewed by	Lisa Washer, Head of Cyber		
Issue date	28/01/2026		

Open Source Intelligence Support Service Definition

Document Control

Version	Name	Comment	Date
0.1	Lisa Washer	Draft Template	07/01/2026
0.2	Simon Young	Review and updated/amended	27/01/2026
1.0	Lisa Washer	Final Review and Publish	28/01/2026

Correlation Chart

Clause	FSR Code of Practice v2	ISO/IEC 17025:2017	ILAC-G19 :06/2022	ISO 9001:2015	ISO/IEC 27001:2022
Review of Requests, Tenders and Contracts	16	7.1	4.1, 4.7	8	4.2

Open Source Intelligence Support Service Definition

Contents

1. Open Source Intelligence Support Service

1.1 Service Overview

1.1.1 The Open Source Intelligence (OSINT) Support Service provides structured, lawful, and ethical collection and analysis of publicly available information to support investigations, intelligence development, risk assessment, and decision-making. The service focuses on identifying, validating, and contextualising open-source information from online and publicly accessible sources to develop actionable intelligence and evidential insight.

1.1.2 The service is delivered using recognised OSINT methodologies and governance controls to ensure transparency, proportionality, and defensibility. All activities are limited to information that is lawfully accessible without deception, impersonation, or circumvention of access controls.

1.2 Service Objectives

1.2.1 The objectives of the OSINT Support Service are to:

a) Identify and collect relevant open-source information

b) Analyse online data to develop intelligence and insight

c) Preserve relevant data in a timely manner

d) Establish timelines, patterns, and relationships

e) Support investigative, legal, and regulatory decision-making

f) Provide clear, defensible intelligence outputs

2. Service Features

2.1.1 Key features of the OSINT Support Service include:

a) **Lawful OSINT Methodology** – Collection limited to publicly accessible information

b) Multi-Source Coverage – Social media, websites, forums, applications and online registries

c) **Structured Analysis** – Timeline, pattern, and relationship analysis

d) **Defensible Capture** – Transparent documentation of sources and methods

e) **Audit-Ready Outputs** – Clear reporting suitable for scrutiny

3. Service Benefits

3.1.1 The service delivers the following benefits:

a) Improved visibility of online activity and risk indicators

b) Identification of relationships, networks, and behaviours

c) Reduced risk of unlawful or unethical information gathering

d) Actionable intelligence to support investigations and decisions

e) Defensible outputs suitable for legal or regulatory review

4. Scope of Service

4.1.1 The OSINT Support Service is delivered in alignment with applicable data protection, privacy, and investigatory laws, as well as platform terms of service. All activities are conducted lawfully, ethically, and proportionately. Engagements may be coordinated through legal counsel where required.

4.2 In-scope activities

4.2.1 The OSINT Support Service includes:

a) Engagement scoping and definition of intelligence requirements

b) Identification of relevant open-source platforms and data sources

c) Collection of publicly available information from websites, social media, applications, forums, and online services

d) Analysis of digital footprints and online presence

e) Timeline reconstruction of online activity

f) Link and relationship analysis between online entities

g) Validation and corroboration of open-source findings

h) Intelligence reporting and briefings

i) Advisory support to investigators and decision-makers

4.3 Out-of-scope activities

4.3.1 Unless agreed separately, the following are excluded:

a) Access to private accounts, closed groups, or restricted content

b) Use of deception, impersonation, or intrusive techniques

c) Circumvention of technical or security controls

d) Interception or monitoring of communications

e) Provision of legal advice or regulatory interpretation

4.4 Assumptions, Dependencies and Constraints

4.4.1 Delivery of the Open Source Intelligence (OSINT) Support Service is based on the following assumptions:

a) The client has lawful authority and a valid legal basis to conduct OSINT activities, including the collection and analysis of publicly available information.

b) All OSINT activities are limited to information that is lawfully accessible without deception, impersonation, or circumvention of technical or security controls.

c) Investigative objectives, scope, subjects of interest, platforms, jurisdictions, and timeframes are clearly defined and agreed prior to commencement.

d) The client will provide timely contextual information, including background, risk considerations, and intended use of intelligence outputs, to support accurate analysis and interpretation.

e) Any legal privilege, confidentiality, sensitivity, or disclosure considerations are identified and communicated at the outset or as they arise during the engagement.

f) Investigations are conducted in accordance with applicable laws, organisational policies, and platform terms of service.

4.4.2 Delivery of the OSINT Support Service is dependent on the following factors:

a) Availability and accessibility of relevant publicly available online content, platforms, and data sources at the time of investigation.

b) Stability of social media platforms, websites, and online services, including continued access to publicly accessible information.

c) Cooperation and timely input from client stakeholders, including legal, compliance, HR, security, or investigation teams.

d) Timely decision-making by the client regarding scope changes, prioritisation, escalation, or investigative focus.

e) Availability of suitably experienced OSINT practitioners and secure systems appropriate to the sensitivity of the engagement.

f) Accurate identification of subjects, entities, or online profiles to avoid misattribution or false association.

4.4.3 The following constraints may impact scope, timelines, certainty, or outcomes of OSINT activities:

a) Publicly available online content is inherently volatile; posts, profiles, and websites may be modified, restricted, or removed without notice.

b) Privacy settings, platform restrictions, or jurisdictional limitations may limit visibility into certain content or interactions.

c) OSINT relies on open-source information and cannot access private communications, closed groups, or restricted accounts.

d) Attribution of online activity may be limited by anonymity, pseudonymous accounts, shared devices, or impersonation by third parties.

e) Platform terms of service and legal requirements may constrain collection methods or use of certain tools.

f) Findings represent a point-in-time assessment based on the information available at the time of collection and analysis.

g) OSINT findings identify indicators, patterns, and relationships but do not, in isolation, establish intent, causation, or wrongdoing.

h) Best practice prioritises lawful, ethical, and defensible investigation over speed, which may affect delivery timelines.

i) Service delivery is subject to specialist availability, technical feasibility, and agreed commercial terms.

5. Service Delivery Model

5.1.1 The OSINT Support Service is provided on an ad-hoc or project basis. Scope, timelines, service levels, and fees are agreed per engagement.

5.1.2 All collected information is handled using secure systems, controlled access, and confidentiality safeguards. Data is processed solely for the agreed purpose and retained only for the agreed duration.

5.2 Engagement Model

5.2.1 The OSINT Support Service is delivered through a structured, phased approach:

a) **Engagement Initiation and Scoping** – Confirmation of objectives, lawful basis, and constraints

b) **Source Identification and Collection** – Identification and capture of relevant open-source material

c) **Analysis and Intelligence Development** – Pattern, timeline, and link analysis

d) **Validation and Quality Review** – Corroboration and review of findings

e) **Reporting and Briefing** – Delivery of intelligence outputs and advisory support

5.2.2 Delivery may be remote, on-site, or hybrid depending on engagement requirements.

5.3 Reporting and Deliverables

5.3.1 Deliverables may include:

a) OSINT intelligence reports and summaries

b) Source logs and capture records

c) Timeline and relationship analysis outputs

d) Methodology and limitation statements

e) Briefings for investigators or decision-makers

6. Exit and Offboarding

6.1.1 Upon completion, collected data is securely returned, retained, or destroyed in accordance with agreed instructions and applicable legal obligations. Access is revoked and formal engagement closure confirmed.

7. Roles and Responsibilities

7.1 Service Provider Responsibilities

7.1.1 The service provider is responsible for delivering the OSINT Support Service in accordance with the agreed scope, applicable legal and regulatory requirements, and recognised OSINT best practice. This includes advising on intelligence objectives, proportionality, and lawful approaches to the collection and analysis of publicly available information.

7.1.2 The service provider will identify relevant open-source platforms, websites, social media channels, forums, and online resources and conduct structured collection and analysis of publicly accessible information only. Responsibilities include validating sources, documenting provenance, analysing digital footprints, reconstructing timelines, identifying patterns and relationships, and developing intelligence-led insights supported by transparent methodology.

7.1.3 The service provider is responsible for maintaining secure handling of all collected material, ensuring auditability, and documenting sources, methods, assumptions, limitations, and confidence levels. Quality assurance activities are undertaken to corroborate findings and minimise misattribution or reliance on unreliable sources. Any legal, ethical, or reputational risks identified during OSINT activities are escalated promptly. The service provider does not engage in deception, impersonation, or unauthorised access and operates strictly within lawful and ethical boundaries.

7.2 Client Responsibilities

7.2.1 The client is responsible for confirming lawful authority and legal basis to conduct OSINT activities and for defining the objectives, scope, and intended use of the intelligence outputs. This includes identifying subjects of interest, relevant jurisdictions, platforms, and timeframes, and providing contextual information necessary to support accurate interpretation.

7.2.2 The client retains responsibility for investigative decisions, legal interpretation, escalation actions, and any operational or disciplinary outcomes arising from the intelligence findings. The client is also responsible for ensuring that OSINT outputs are used in accordance with organisational policies, applicable laws, and regulatory requirements.

7.3 Legal, Compliance, and Governance Responsibilities (Where Applicable)

7.3.1 Where legal counsel, compliance, privacy, or governance stakeholders are involved, these parties are responsible for advising on applicable legal and regulatory frameworks, including data protection, privacy, employment law, and platform terms of service. They may review OSINT outputs for compliance risk, advise on disclosure or reporting obligations, and oversee legally privileged handling where appropriate.

7.4 Joint Responsibilities

7.4.1 The service provider and client share responsibility for effective communication, timely decision-making, and escalation of issues that may impact scope, timelines, legal compliance, or the reliability of intelligence outputs. All parties are responsible for maintaining confidentiality, ensuring proportionality, and supporting transparent, auditable, and ethical OSINT practices.

*****END OF DOCUMENT*****