Digital Investigator Training Service Definition

Document title	Digital Investigator Training Service Definition		
Reference No.	IF-SER-020	**Version**	1.0
Author	Simon Young, Digital Investigations Manager		
Reviewed by	Lisa Washer, Head of Cyber		
Issue date	27/01/2026		

Digital Investigator Training Service Definition

Document Control

Version	Name	Comment	Date
0.1	Lisa Washer	Initial Draft	07/01/2026
0.2	Simon Young	Review and amendments	27/01/2026
1.0	Lisa Washer	Final review and publish	27/01/2026

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

Digital Investigator Training Service Definition

Contents

1. Digital Investigator Training Service

1.1 Service Overview

1.1.1 The Digital Investigator Training Service provides structured training designed to develop and enhance digital investigation capabilities within organisations. The service equips participants with the knowledge, practical skills, and investigative methodologies required to identify, collect, analyse, and interpret digital information in a lawful, ethical, and defensible manner.

1.1.2 The training includes core digital investigation techniques alongside specialist modules such as Open-Source Intelligence (OSINT)**,** enabling investigators to gather, assess, and contextualise publicly available information to support investigations, intelligence development, and decision-making.

1.1.3 The training content is developed to be bespoke to the needs of the client. Typically the training is appropriate for the following organisations:

a) Law enforcement agencies, including certain public sector agencies with a law enforcement responsibility.

b) Military and armed forces personnel.

c) Private sector companies which may include corporate businesses, journalists, researchers and cyber security & threat intelligence professionals,

1.2 Service Objectives

1.2.1 The objectives of the Digital Investigator Training Service are to:

a) Develop practical digital investigation skills and investigative mindset

b) Enable lawful and ethical use of digital and open-source information

c) Improve accuracy, efficiency, and defensibility of investigations

d) Enhance capability to identify leads, patterns, and risks

e) Support consistent investigative standards across teams

f) Build confidence through structured learning

2. Service Features

2.1.1 Key features of the Digital Investigator Training Service include:

a) **Structured Training Modules** – Internet Intelligence & Investigation, Open Source and Social Media Intelligence (OSINT and SOCMINT), Cloud data investigation

b) **Hands-On Exercises** – Realistic scenario, tool-based exercises and investigative case studies

c) **Role-Based Content** – Tailored for investigators, analysts, compliance, or security teams

d) **Legal and Ethical Emphasis** – Lawful, proportionate, and defensible investigation practices

e) **Flexible Delivery** – On-site, virtual, or hybrid training formats

3. Service Benefits

3.1.1 The training delivers the following benefits:

a) Improved investigative capability and confidence

b) Reduced risk of unlawful or unethical information gathering

c) Better identification of leads, risks, and intelligence gaps

d) Consistent investigative approaches across teams

e) Stronger documentation and reporting standards

f) Demonstrates Continuous Professional Development

4. Scope of Service

4.1.1 The training emphasises lawful, ethical, and proportionate investigation practices, including compliance with data protection, privacy, and organisational policies. Clear guidance is provided on the boundaries of OSINT, use of publicly available information, and avoidance of intrusive or unlawful activity.

4.2 In-scope activities

4.2.1 The Digital Investigator Training Service may include the following modules, tailored to audience and maturity:

a) Fundamentals of digital investigations and evidence handling

b) Legal, ethical, and regulatory considerations in digital investigations

c) Investigative strategies, planning, and hypothesis development

d) Open-Source Intelligence (OSINT) techniques, tools, and methodologies

e) Social media and online platform investigations

f) An awareness of communications data available from Telecoms Operators

g) Data which can be acquired from motor vehicles

h) Best practice in preserving digital data and chain-of-custody principles

i) Digital footprint and online identity analysis

j) Email, messaging, and communication data awareness

k) Reporting, documentation, and presentation of findings

l) Risk management and investigative governance

4.3 Out-of-scope activities

4.3.1 Unless agreed separately, the training does not include:

a) Live investigations or operational tasking

b) Provision of legal advice

c) Certification or accreditation examinations

d) Continuous mentoring beyond the training engagement

4.4 Assumptions, Dependencies and Constraints

4.4.1 Delivery of the Digital Investigator Training Service is based on the following assumptions:

a) Participants are nominated by the client and have roles or responsibilities relevant to digital investigations, intelligence, compliance, or security functions.

b) The client has appropriate policies, governance frameworks, and legal authority in place to support the application of investigative techniques covered during training, including OSINT activities.

c) Training objectives, participant experience levels, and required outcomes are clearly defined and agreed prior to delivery.

d) Participants will engage actively with training content, exercises, and discussions to maximise learning outcomes.

e) Any jurisdiction-specific legal or regulatory considerations relevant to the client's operating environment are identified and communicated in advance.

4.4.2 Delivery of the Digital Investigator Training Service is dependent on the following factors:

a) Availability of participants for the agreed training dates and duration.

b) Access to suitable training facilities or virtual platforms, including internet connectivity and systems required for practical OSINT exercises.

c) Provision of accurate contextual information by the client to tailor scenarios and examples appropriately.

d) Timely confirmation of training scope, format (on-site, virtual, or hybrid), and logistical arrangements.

e) Cooperation from client IT or security teams where technical access or restrictions may affect training exercises.

4.4.3 The following constraints may impact delivery or outcomes:

a) Training provides knowledge and skills but does not replace legal advice or organisational policy enforcement.

b) OSINT techniques rely on publicly available information; availability, accuracy, and platform access may change over time.

c) Practical exercises may be limited by platform terms of service, geographic restrictions, or organisational security controls.

d) Training cannot guarantee investigative outcomes, as effectiveness depends on participant application and organisational context.

e) Delivery timelines may be affected by participant availability, technical issues, or changes to agreed scope.

f) Content reflects best practice at the time of delivery and may require periodic refresh due to evolving technologies, platforms, and legal considerations.

5. Service Delivery Model

5.1.1 The Digital Investigator Training Service is provided on an ad-hoc or programme basis. Scope, delivery format, timelines, and fees are agreed per engagement.

5.2 Training Delivery

5.2.1 Training is delivered by experienced digital investigators and intelligence practitioners. Sessions combine structured instruction, demonstrations, interactive discussion, and practical exercises.

5.2.2 Delivery may be:

a) Classroom-based (on-site)
b) Virtual instructor-led
c) Hybrid (combined in-person and remote)
d) Training content and duration are tailored to organisational needs, participant roles, and experience levels.

5.3 Training Formats

5.3.1 Available formats may include:

a) Foundation digital investigator course
b) Advanced OSINT and online investigations workshops
c) Scenario-based investigative simulations
d) Executive and management briefings
e) Refresher or capability uplift sessions

5.4 Training Materials and Outputs

5.4.1 Participants may receive:

a) Training slides and reference materials
b) Practical exercise workbooks
c) OSINT frameworks and checklists
d) Guidance on tools, techniques, and limitations
e) Certificates of attendance

6. Exit and Offboarding

6.1 Final evaluation of competence

6.1.1 Training concludes with scenario-based exercises and a final assessment to evaluate learner understanding and practical application. This ensures participants understand relevant policies, tools, and support channels and are able to apply new skills appropriately in real investigations. Where appropriate, outcomes may be discussed with supervisors or training coordinators.

6.2 Learner feedback

6.2.1 Participants are encouraged to provide feedback on training content, delivery, and effectiveness to support continuous improvement.

6.3 Continued Professional Development

6.3.1 Learners are signposted to further development opportunities, refresher training, or advanced modules to support ongoing professional growth.

7. Roles and Responsibilities

7.1 Service Provider Responsibilities

7.1.1 The service provider is responsible for the design, delivery, and quality of the Digital Investigator Training Service. This includes developing training content that reflects recognised digital investigation and OSINT best practice, current legal and ethical considerations, and practical investigative methodologies.

7.1.2 The service provider will deliver training through qualified and experienced instructors, facilitate practical exercises and case studies, and provide supporting materials to reinforce learning outcomes. The provider is responsible for ensuring training is delivered in a structured, professional manner, aligned to the agreed scope, objectives, and participant experience levels. The provider will also highlight limitations, risks, and governance considerations associated with digital investigations and OSINT activities.

7.2 Client Responsibilities

7.2.1 The client is responsible for defining training objectives, selecting appropriate participants, and ensuring that attendees have roles relevant to the application of digital investigation techniques. The client will ensure that organisational policies, legal frameworks, and governance arrangements are in place to support lawful and ethical application of the training content.

7.2.2 The client is also responsible for providing suitable facilities or access to virtual platforms, ensuring participants have the necessary technical access for training exercises, and supporting post-training application of skills within operational contexts.

7.3 Participant Responsibilities

7.3.1 Participants are responsible for engaging actively with the training, adhering to ethical and legal guidance provided, and applying techniques in accordance with organisational policies and applicable laws. Participants must not use training content or OSINT techniques for unauthorised, intrusive, or unlawful activity.

7.4 Joint Responsibilities

7.4.1 The service provider and client share responsibility for effective communication, timely coordination of logistics, and escalation of issues that may impact training delivery or outcomes. All parties are responsible for maintaining confidentiality, respecting intellectual property, and ensuring that training is delivered and applied in a professional and responsible manner.

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