Device Investigation Service Definition

Document title	Device Investigation Service Definition		
Reference No.	IF-SER-002	**Version**	1.0
Author	Lisa Washer, Head of Cyber		
Reviewed by	Neil Bacon, Incident Response Specialist		
Issue date	27/01/2026		

UNCONTROLLED WHEN PRINTED

Device Investigation Service Definition

Document Control

Version	Name	Comment	Date
0.1	Lisa Washer	Initial Draft	07/01/2026
0.2	Neil Bacon	Review and comments	27/01/2026
1.0	Lisa Washer	Minor amendments 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

Device Investigation Service Definition

Contents

Document Control 2
Correlation Chart 2
Contents 3
1. Cyber Incident Investigation Service 5
1.1 Service Overview 5
1.2 Service Features 5
2. Service Benefits 5
3. Scope of Service 8
3.1 In-Scope of Service 8
3.2 Out-of-scope activities 8
3.3 Assumptions, Constraints and Dependencies 8
4. Onboarding 10
5. Service Delivery Model 11
5.2 Engagement Approach 11
5.3 Delivery Phases 11
5.4 Typical Timelines 12
5.5 Delivery Modes 13
6. Support Model 14
6.2 Standard Support 14
6.3 Enhanced Support 14
6.4 Escalation Paths 14
6.5 Optional Support Services 14
7. Service Level Agreements 15
7.2 Response time 15
7.3 Investigation Commencement 15
7.4 Availability Windows 15
7.5 Delivery timeframe 15
7.6 Reporting Commitments 15
8. Roles and Responsibilities 16
8.2 Account Manager 16
8.3 Incident Manager 16
8.4 Cyber Incident Response (CIR) Specialist 16

8.5 Client Incident Lead 16
8.6 Client Stakeholders and Subject Matter Experts 16
8.7 Service RACI Matrix 17
9. Technical Requirements 18
10. Exit and Offboarding 19
10.2 Final Deliverables 19
10.3 Knowledge Transfer and Close-Out 19
10.4 Data Handling and Retention 19
10.5 Service Closure 19

UNCONTROLLED WHEN PRINTED

1. Device Investigation Service

1.1 Service Overview

1.1.1 The Device Analysis Service provides specialist digital forensic analysis of computers, mobile devices, and other digital storage media to support security, legal, regulatory, and internal investigations. Using the Strand Intelligence Platform, the service enables the structured identification, acquisition, analysis, and interpretation of data resident on digital devices in a forensically sound and defensible manner.

1.1.2 The service is designed to establish what activity occurred on a device, when it occurred, how it occurred, and the relevance of that activity to the matter under investigation. Findings support informed decision-making across legal, compliance, HR, security, and executive stakeholders.

1.1.3 The service is delivered on an ad-hoc consultancy basis and may be engaged as required, with no pre-existing contract or retainer necessary.

1.2 Service Objectives

1.2.1 The objectives of the Device Analysis Service are to:

a) Identify, preserve, and analyse device-based digital evidence using recognised forensic methodologies

b) Reconstruct user and system activity to support factual understanding of events

c) Provide defensible, evidence-based findings suitable for internal, legal, or regulatory use

d) Minimise disruption to business operations while maintaining evidential integrity

e) Deliver clear, proportionate reporting aligned to stakeholder needs

1.3 Service Features

1.3.1 Below is a list of the core capabilities and characteristics of the Device Investigation Service, describing what is delivered and how the service operates:

a) **Strand Intelligence Platform** – A centralised platform enabling efficient ingest, analysis, correlation, and reporting of device artefacts

b) **Forensic Soundness** – Evidence handling aligned to recognised digital forensic principles and standards

c) **Scalable Analysis** – Capability to analyse single devices or multiple devices within the same investigation

d) **Flexible Engagement** – Engagement scoped to the specific matter, device types, and required outcomes

e) **Stakeholder-Focused Reporting** – Outputs tailored for technical, legal, HR, compliance, or executive audiences

f) **Trusted Accredited Delivery** - Delivered by CREST- and SANS-accredited specialists operating as an NCSC CIR accredited provider.

2. Service Benefits

2.1.1 The Device Investigation Service provides organisations with timely, expert support to examine and understand activity on digital devices in support of security, legal, or internal matters. The service enables the identification, analysis, and interpretation of device-resident data to establish facts, timelines, and user activity, supporting informed decision-making and defensible outcomes.

a) Rapid clarity on device-based activity and events

b) Defensible evidence suitable for legal or regulatory scrutiny

c) Reduced investigative risk through structured, repeatable analysis

d) Improved confidence in disciplinary, legal, or remediation decisions

e) Independent expert insight delivered by experienced practitioners

3. Scope of Service

3.1 In-Scope of Service

3.1.1 The Device Analysis Service includes the following activities:

a) Case scoping and investigative planning

b) Forensic acquisition of device data using the Strand Intelligence Platform

c) Analysis of laptops, desktops, mobile devices, removable media, and external storage

d) Examination of operating system artefacts, user activity, application data, and logs

e) Timeline reconstruction of device and user activity

f) Identification of accessed, modified, deleted, or transferred data

g) Assessment of potential data exposure or policy violations

h) Advisory support for investigative outcomes and next steps

i) Production of technical and executive-level forensic reports

3.2 Out-of-scope activities

3.2.1 The following activities are not included as part of the standard Device Investigation Service scope. However, the organisation can provide support for these activities through additional services or established partner arrangements, subject to separate agreement:

a) Live remediation, system rebuild, or device recovery activities

b) Provision of legal advice or legal representation

c) Continuous monitoring or managed investigation services

d) Investigation of devices or data without appropriate authority or consent

3.3 Assumptions, Constraints and Dependencies

3.3.1 Delivery of the Device Investigation Service is subject to the following assumptions, constraints, and dependencies, which influence scope, timelines, and outcomes.

a) **Client Authority and Access** - It is assumed that the organisation has the legal authority to grant access to in-scope systems, data, and users. Investigation activities are constrained to systems and information explicitly authorised by the organisation.

b) **Availability and Accuracy of Information** - The effectiveness of the investigation depends on the accuracy, completeness, and availability of information, logs, and documentation provided. Limitations in data retention, logging, or system visibility may restrict findings.

c) **Timely Client Engagement** - Progress and timelines depend on timely engagement from nominated client contacts, including system owners, subject matter experts, and decision-makers.

d) **Point-in-Time Assessment** - Findings represent a snapshot based on the evidence available during the investigation and may not identify all historical activity or enable definitive attribution.

4. Onboarding

4.1.1 Onboarding commences immediately upon service initiation and is designed to enable rapid, structured engagement during a cyber incident. At the outset, a dedicated incident response team is established and aligned to the organisation. This team consists of an Account Manager as the primary commercial and engagement point of contact, an Incident Manager responsible for overall coordination and incident governance, and a Cyber Incident Response (CIR) Specialist responsible for technical investigation and analysis.

4.1.2 During onboarding, the incident context is captured, and a preliminary timeline of events is developed to document key occurrences from initial detection to engagement. Any actions taken prior to service commencement are identified and recorded to inform investigation planning and preserve evidential integrity. Scope, objectives, and legal authorisation to investigate are confirmed, and key stakeholders, escalation paths, and reporting requirements are agreed.

4.1.3 Communication frequency and methods, including regular status updates, escalation notifications, and reporting cadence, are defined and agreed at the outset to ensure clear, consistent engagement throughout the investigation. Access requirements, constraints, and dependencies are documented, and coordination with legal, compliance, or third-party providers is initiated where required. Onboarding ensures clarity of roles, responsibilities, and next steps, enabling effective and timely investigation activities.

5. Service Delivery Model

5.1.1 The Device Investigation Service is delivered using a structured and flexible engagement approach designed to support organisations during suspected or confirmed cyber incidents. Delivery is tailored to the nature, severity, and complexity of the incident while following recognised incident response and forensic investigation practices.

5.2 Engagement Approach

5.2.1 The service is delivered by experienced digital forensic practitioners using the Strand Intelligence Platform and industry-recognised investigative methodologies.

5.2.2 Engagement typically follows these stages:

a) Initial consultation and scoping

b) Evidence identification and acquisition

c) Device analysis and interpretation

d) Findings validation and review

e) Reporting and stakeholder briefing

5.2.3 Delivery timelines are dependent on device type, data volume, scope, and stakeholder availability.

5.2.4 All investigations are supported by a dedicated Cyber Incident Response Specialist, Cyber Incident Manager, and Account Manager.

5.3 Engagement Initiation and Scoping

5.3.1 The engagement initiation and scoping phase establishes the objectives, scope, and governance of the device analysis activity. During this phase, the context of the matter is understood, in-scope devices, users, and timeframes are identified, and investigative priorities are agreed. Legal authority, consent, and handling requirements are confirmed to ensure the investigation is conducted lawfully and proportionately. Assumptions, constraints, deliverables, and reporting requirements are defined to provide a clear and agreed framework for subsequent forensic activity.

5.4 Evidence Identification and Acquisition

5.4.1 The evidence identification and acquisition phase focuses on the forensically sound collection of data from in-scope devices. Appropriate acquisition methods are selected based on device type, condition, and investigative requirements. Data is acquired using the Strand Intelligence Platform and validated forensic tools, with integrity verified through hashing and validation processes. Throughout this phase, strict chain-of-custody

procedures are maintained to preserve evidential integrity and ensure the data remains admissible and defensible.

5.5 Device Analysis and Artefact Examination

5.5.1 The device analysis and artefact examination phase involves the detailed examination of acquired data to identify relevant artefacts and activity. Using the Strand Intelligence Platform, analysts review operating system artefacts, application data, logs, and user activity to identify actions, events, and behaviours relevant to the investigation. Automated processing is combined with expert analyst review to ensure both efficiency and depth of analysis, with findings iteratively refined as new evidence emerges.

5.6 Timeline Reconstruction and Interpretation

5.6.1 The timeline reconstruction and interpretation phase reconstructs device and user activity into a coherent chronological narrative. Multiple artefact sources are correlated to identify key events, sequences of behaviour, and points of interest. This phase distinguishes between user-driven activity, automated system processes, and background noise, enabling accurate interpretation of findings in context. The resulting timeline supports clear understanding of what occurred, when it occurred, and how events unfolded.

5.7 Findings Review and Advisory Support

5.7.1 The findings review and advisory support phase translates technical forensic results into actionable insight. Findings are validated and reviewed to ensure accuracy, consistency, and relevance to the investigative objectives. Expert advisory support is provided to assist stakeholders in understanding implications, limitations, and next steps, including considerations relating to policy, legal, or regulatory requirements. This phase supports informed decision-making and appropriate escalation or remediation actions.

5.8 Reporting and Presentation

5.8.1 The reporting and presentation phase delivers formal, evidence-based outputs aligned to stakeholder needs. Reports document the investigative approach, methodology, findings, and conclusions in a clear and defensible manner, supported by evidential exhibits where appropriate. Executive summaries are provided to highlight key conclusions and risks, and findings may be presented to stakeholders to support understanding, challenge, and decision-making.

5.9 Typical Timelines

5.9.1 The duration of the Device Analysis Service varies depending on the nature of the matter, the number and type of devices in scope, the volume of data, and the complexity of

analysis required. Timelines are agreed during the scoping phase and reviewed as the investigation progresses to ensure they remain appropriate and proportionate.

5.9.2 As a guide, a single-device investigation typically progresses through initial scoping and evidence acquisition within 1–3 business days, subject to device availability and authority confirmation. Forensic processing and analysis using the Strand Intelligence Platform generally takes 3–10 business days, depending on device type, data volume, encryption, and the depth of analysis required. Timeline reconstruction, findings validation, and advisory support are typically completed in parallel with analysis or shortly thereafter.

5.9.3 Reporting and delivery of formal outputs are usually completed within 2–5 business days following completion of analysis, depending on reporting format, stakeholder requirements, and review cycles. Where legal, regulatory, or expert witness support is required, additional time may be necessary and will be agreed separately.

5.9.4 Investigations involving multiple devices, damaged or encrypted media, third-party dependencies, or expanded scope may extend beyond these indicative timelines. The service is designed to be flexible, with phased delivery allowing interim findings to be provided where time sensitivity or operational impact requires earlier insight.

5.10 Delivery Modes

5.10.1 The service may be delivered remotely, on-site, or through a hybrid approach, depending on incident requirements, data sensitivity, and client preference. Remote delivery is used where secure access can be provided, while on-site support may be required for sensitive environments, evidence handling, or operational constraints.

6. Support Model

6.1.1 The Device Investigation Service is supported through defined levels of engagement to ensure appropriate coverage based on incident severity and client requirements. Support levels, hours of operation, and escalation arrangements are agreed at the outset of the engagement and may be adjusted as the incident evolves.

6.2 Standard Support

6.2.1 Standard support is provided during business hours and includes investigation activities, incident coordination, and regular status updates. The service is delivered by a dedicated Cyber Incident Response (CIR) Specialist, overseen by an Incident Manager**,** with an Account Manager providing engagement oversight. Standard support includes agreed reporting and access to subject matter expertise as required.

6.3 Enhanced Support

6.3.1 Enhanced support may be provided for higher-severity incidents or where extended coverage is required. This may include out-of-hours or weekend support, accelerated investigation activities, increased specialist resource allocation, and more frequent status updates. Enhanced support is delivered subject to availability and separate agreement.

6.4 Escalation Paths

6.4.1 Operational escalation is managed by the Incident Manager, who coordinates resources and resolves issues impacting investigation progress. Strategic or commercial escalation is managed by the Account Manager. Escalation to senior technical specialists or management occurs where incident severity, regulatory risk, or complexity increases.

6.5 Optional Support Services

6.5.1 In addition to the core investigation service, optional specialist support services may be provided subject to separate agreement. These include executive-level briefings, regulatory-focused reporting, extended post-incident monitoring, expert witness support, and follow-on incident response or remediation advisory services. Further specialist services may also be provided to support broader incident response and recovery activities, including eDiscovery services to support Data Protection Officers (DPOs) and data breach analysis, malware analysis, threat hunting, penetration testing, and wider cyber security consultancy services. Services may be delivered directly or through established partner arrangements, depending on scope and requirements.

7. Service Level Agreements

7.1.1 The following service levels describe indicative performance targets for the Device Investigation Service. These service levels are provided for guidance only and do not constitute guaranteed commitments unless expressly agreed in writing.

7.1.2 Where a pre-existing contract or retainer agreement is in place, including an Incident Response (IR) Retainer, the service levels and SLAs defined within that agreement shall apply and take precedence over the indicative service levels outlined below.

7.2 Response time

7.2.1 Initial response is provided following confirmation of engagement and receipt of appropriate authorisation. For high-severity incidents, initial engagement typically occurs within 4–8 business hours, with lower-severity incidents responded to within 1–2 business days, subject to availability.

7.3 Investigation Commencement

7.3.1 Investigation activities commence once scope, access, and legal authorisation are confirmed. For urgent incidents, investigative work typically begins within 24 hours of engagement approval.

7.4 Availability Windows

7.4.1 Standard service delivery is provided during business hours, with enhanced or out-of-hours support available by agreement. Availability may be extended for high-severity incidents, subject to resource availability and agreed terms.

7.5 Delivery timeframe

7.5.1 Investigation duration varies depending on incident complexity, system scope, and data availability. Indicative investigations may range from several days to multiple weeks

7.6 Reporting Commitments

7.6.1 Interim status updates are provided at an agreed frequency. Final technical and executive reports are typically delivered within 5–10 business days of investigation completion, subject to scope and review requirements.

8. Roles and Responsibilities

8.1.1 The following roles are defined to ensure effective governance, delivery, and communication throughout the Device Investigation Service engagement

8.2 Account Manager

8.2.1 Acts as the primary commercial and engagement contact for the organisation. Responsible for contract management, service coordination, and strategic escalation. Ensures the service is delivered in line with agreed scope and expectations.

8.3 Incident Manager

8.3.1 Provides overall operational leadership for the investigation. Responsible for incident coordination, prioritisation, decision-making, escalation management, and communication oversight. Acts as the primary operational point of contact throughout the engagement.

8.4 Cyber Incident Response (CIR) Specialist

8.4.1 Responsible for the technical investigation and forensic analysis. Conducts evidence collection, analysis, and documentation in accordance with recognised forensic standards. Provides expert input to support containment, remediation planning, and reporting.

8.5 Client Incident Lead

8.5.1 Acts as the organisation's primary point of contact for the investigation. Coordinates internal stakeholders, facilitates access to systems and information, and supports decision-making and escalation activities.

8.6 Client Stakeholders and Subject Matter Experts

8.6.1 Provide system access, technical knowledge, and operational context required to support investigation activities and validate findings.

UNCONTROLLED WHEN PRINTED

8.7 Service RACI Matrix

8.7.1 The following RACI matrix defines roles and responsibilities for the delivery of the Device Investigation Service. It clarifies accountability and ownership across key activities to ensure effective governance, communication, and execution throughout the engagement. The matrix identifies who is Responsible, Accountable, Consulted, and Informed for each activity, supporting clear decision-making, efficient escalation, and coordinated incident response.

Activity / Task	*Account Manager*	*Incident Manager*	*CIR Specialist*	*Client Incident Lead*	*Client SMEs*
Engagement initiation & onboarding	R	A	C	C	I
Incident scoping & prioritisation	C	A	R	C	C
Investigation planning	I	A	R	C	C
Evidence collection & preservation	I	C	R	C	I
Forensic analysis & investigation	I	C	R	I	C
Timeline & root cause analysis	I	C	R	I	C
Impact & data exposure assessment	I	A	R	C	C
Advisory support & recommendations	I	A	R	C	C
Status updates & communications	C	A	R	C	I
Escalation management	C	A	I	R	I
Reporting (technical & executive)	I	A	R	C	I
Service close-out & offboarding	R	A	C	C	I

9. Technical Requirements

9.1.1 Delivery of the Cyber Investigation Service requires appropriate technical access, information, and resources to enable effective investigation activities. The following requirements apply and are confirmed during onboarding.

a) **Authorisation and Access -** Written authorisation must be provided confirming the organisation's approval for investigation activities.

b) **Logging and Data Availability -** Access to relevant system, application, security, and network logs is required. The scope and depth of findings depend on log availability, retention periods, and data quality.

c) **System and Environment Information -** Provision of relevant technical documentation, such as network diagrams, asset inventories, system architecture, identity and access models, and security tooling in use, to support investigation planning and analysis.

d) **User and Stakeholder Availability -** Availability of system owners, administrators, and subject matter experts to support access provisioning, clarify system behaviour, and validate findings.

e) **Secure Communications -** Use of secure communication channels for information exchange, including file transfer and reporting, to protect sensitive investigation data.

f) **Forensic Handling Requirements -** Where forensic imaging or evidence preservation is required, systems must be made available in a manner that supports forensic integrity and minimises operational impact.

10. Exit and Offboarding

10.1.1 The Device Investigation Service concludes once all agreed investigation activities have been completed and final deliverables have been provided. Service closure is managed in a controlled manner to ensure clarity of outcomes, secure handling of information, and effective knowledge transfer.

10.2 Final Deliverables

10.2.1 At service completion, agreed outputs are delivered to the organisation. This typically includes technical and executive reports detailing investigation scope, findings, timelines, conclusions, and recommendations. Where applicable, additional deliverables such as evidence inventories, indicators of compromise, or expert statements are provided.

10.3 Knowledge Transfer and Close-Out

10.3.1 A close-out meeting may be held to review findings, explain conclusions, and discuss recommended next steps. This session supports knowledge transfer to relevant stakeholders, including IT, security, legal, and management teams, and provides an opportunity to address questions and clarify outcomes.

10.4 Data Handling and Retention

10.4.1 All investigation data and evidence are handled in accordance with agreed data handling, confidentiality, and retention requirements. Data is securely stored during the engagement and, following service completion, is either securely transferred to the organisation or retained for an agreed period before secure disposal, in line with contractual and regulatory obligations.

10.5 Service Closure

10.5.1 The service is formally closed once deliverables are accepted and offboarding activities are completed. Any further support required beyond service closure is subject to a new or extended engagement.

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