Cyber Incident Investigation Service Definition

Document title	Cyber Incident Investigation Service Definition		
Reference No.	IF-SER-011	**Version**	1.0
Author	Lisa Washer, Head of Cyber		
Reviewed by	Holly Jackson, Cyber Manager		
Issue date	23/01/2026		

Cyber Incident Investigation Service Definition

Document Control

Version	Name	Comment	Date
0.1	Lisa Washer	Initial draft	07/01/2026
0.2	Holly Jackson	Review and amendments	13/01/2026
1.0	Lisa Washer	Final review and publish	23/01/2026

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

Cyber Incident Investigation Service Definition

Contents

1. Cyber Incident Investigation Service

1.1 Service Overview

1.1.1 The Cyber Investigation Service provides specialist cyber and digital forensic investigation support to organisations experiencing suspected or confirmed cyber incidents. The service helps establish what occurred, how it occurred, and the impact, enabling informed decision-making, regulatory response, and recovery. Services are delivered by CREST- and SANS-accredited specialists operating as part of an NCSC Cyber Incident Response (CIR) accredited provider. This service is provided to clients on an ad-hoc consultancy basis and is engaged as required, with no pre-existing contract required.

1.2 Service Features

1.2.1 Below is a list of the core capabilities and characteristics of the Cyber Incident Investigation service, describing what is delivered and how the service operates:

a) **Incident Scoping and Triage -** Rapid assessment to understand incident type, scope, severity, and priorities.

b) **Digital Forensic Investigation -** Forensic analysis of endpoints, servers, cloud services, and network activity.

c) **Evidence Identification and Preservation -** Secure collection and handling of digital evidence in line with forensic best practice.

d) **Timeline and Root Cause Analysis -** Reconstruction of attacker activity to determine how the incident occurred.

e) **User and Account Activity Analysis -** Review of user actions, credential misuse, and privilege escalation.

f) **Malware and Artifact Analysis -** Identification and analysis of malicious files, persistence mechanisms, and indicators.

g) **Log and Network Traffic Analysis -** Examination of logs and network data to identify compromise and lateral movement.

h) **Impact and Data Exposure Assessment -** Determination of affected systems, data types, and potential data exfiltration.

i) Advisory Support for Containment and Recovery - Expert guidance to support effective containment, remediation planning, and recovery.

j) **Technical and Executive Reporting -** Clear, evidence-based reports suitable for technical teams, management, and regulators.

k) Regulatory and Stakeholder Support - Support for regulatory notification, audit response, and stakeholder communications.

l) **Accredited Specialist Delivery -** Investigations conducted by CREST- and SANS-accredited specialists operating under an NCSC CIR accredited provider

2. Service Benefits

2.1.1 The Cyber Investigation Service provides organisations with timely, expert support to understand and respond effectively to cyber security incidents. Key benefits include:

a) **Rapid Clarity on Incidents -** Establishes what occurred, how the incident unfolded, and the full scope of impact.

b) **Reduced Business Disruption -** Supports effective containment and recovery to minimise operational downtime.

c) **Evidence-Based Decision Making -** Provides reliable forensic findings to inform response, recovery, and escalation decisions.

d) **Regulatory and Legal Confidence -** Supports compliance with regulatory, contractual, and reporting obligations.

e) **Preservation of Evidential Integrity -** Ensures evidence is handled in accordance with recognised forensic standards.

f) **Improved Risk Management -** Identifies root causes and control weaknesses to reduce the likelihood of recurrence.

g) **Executive and Stakeholder Assurance -** Delivers clear reporting to support board-level, customer, and regulator confidence.

h) **Independent Expert Support -** Provides objective analysis delivered by accredited specialists independent of internal teams.

i) **Improved Incident Response Maturity -** Informs enhancements to incident response processes, controls, and organisational readiness.

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

3. Scope of Service

3.1 In-Scope of Service

3.1.1 The Cyber Investigation Service covers the investigation and analysis of suspected or confirmed cyber security incidents affecting the organisation's systems, data, and users. The scope of the service includes the following activities:

a) Incident Scoping and Assessment - Initial assessment to confirm the nature, severity, and potential impact of the incident and to define investigation priorities.

b) Digital Forensic Investigation - Forensic analysis of endpoints, servers, cloud platforms, network infrastructure, and user accounts within the agreed scope.

c) Evidence Identification and Preservation - Identification, collection, and preservation of digital evidence in accordance with recognised forensic best practice.

d) Log, Network, and Activity Analysis - Review of logs, network traffic, and system activity to identify indicators of compromise, lateral movement, and attacker behaviour.

e) Impact and Data Exposure Assessment - Assessment of affected systems and data, including potential exposure of sensitive or regulated information.

f) Root Cause and Timeline Reconstruction - Analysis to determine how the incident occurred and to reconstruct the sequence of events.

g) Advisory Support - Provision of expert advice to support containment, remediation planning, recovery activities, and stakeholder decision-making.

h) Reporting and Findings - Delivery of technical and executive-level reports documenting findings, conclusions, and recommendations.

i) Legal and Regulatory Support - The Cyber Investigation Service includes advisory support to assist organisations in meeting legal and regulatory requirements arising from a cyber incident. This includes support for legally privileged reporting where engagement is coordinated through external legal counsel, assistance to Data Protection Officers (DPOs) in assessing personal data impact and regulatory notification obligations, and preparation of investigation outputs suitable for legal review. Where required, suitably qualified specialists may provide expert witness services, including written statements and court or tribunal testimony, subject to separate agreement.

3.2 Out-of-scope activities

3.2.1 The following activities are not included as part of the standard Cyber 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 system remediation, rebuild, or recovery activities

b) Provision of legal advice or legal representation

c) Continuous monitoring, managed detection, or managed response services

d) Investigation of third-party systems without appropriate authorisation

3.3 Assumptions, Constraints and Dependencies

3.3.1 Delivery of the Cyber 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) **Third-Party Dependencies** - Investigations involving cloud providers, suppliers, or external platforms rely on third-party cooperation and legal processes, which may introduce delays or limit access to evidence.

e) **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.

f) **Operational Constraints** - Investigation activities are conducted to minimise business disruption; certain actions may be limited by operational, safety, or business continuity requirements.

g) **Resource Availability** - Delivery is subject to specialist availability and agreed engagement terms, including scheduling and priority requirements.

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 Cyber 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 Service delivery begins upon formal engagement approval and completion of onboarding activities. A dedicated incident response team is assigned, comprising an Account Manager, Incident Manager, and Cyber Incident Response (CIR) Specialist. The engagement is led by the Incident Manager, who coordinates activities, manages priorities, and acts as the primary operational point of contact. The approach is collaborative and evidence-led, with regular communication and agreed reporting throughout the engagement.

5.3 Delivery Phases

5.3.1 The service is typically delivered across the following phases:

a) **Initial Triage and Scoping -** Rapid assessment to confirm incident type, scope, severity, and immediate priorities. This phase includes review of initial indicators, validation of incident status, and confirmation of investigation objectives.

b) **Investigation and Analysis -** Detailed forensic investigation of in-scope systems, accounts, and data. Activities may include endpoint, server, cloud, network, and log analysis, evidence preservation, and reconstruction of attacker activity.

c) **Impact Assessment and Advisory Support -** Assessment of business, operational, and data impact, including potential regulatory considerations. Advisory support is provided to inform containment, remediation planning, and recovery decisions.

d) **Reporting and Close-Out -** Delivery of technical and executive reports detailing findings, timelines, conclusions, and recommendations. A close-out discussion is held to review outcomes and next steps.

5.4 Typical Timelines

5.4.1 Timelines vary based on incident complexity, scope, and data availability. Initial triage typically occurs within the first 24–48 hours of engagement. Investigation and analysis may range from several days to multiple weeks, depending on severity and scale. Reporting is delivered in line with agreed timescales following completion of investigation activities

5.4.2 Investigation effort is determined by the nature and severity of the incident and confirmed through initial scoping. As a guide, the following approach is used:

a) **Low Severity** (1–2 days): Phishing analysis, suspicious login activity, single-endpoint malware alerts, or user error reviews.

b) **Moderate Severity** (3–5 days): Confirmed malware infections, business email compromise, limited data exposure, or internal misuse affecting a small number of systems.

c) **High Severity** (6–10 days): Ransomware incidents, confirmed data breaches, privileged account compromise, or multi-system intrusions.

d) **Critical / Major Severity** (10–20+ days): Enterprise-wide ransomware, advanced persistent threat activity, large-scale data exfiltration, or incidents requiring regulatory or legal reporting. A 30-day post-incident monitoring period is recommended to confirm effective recovery. All investigations are supported by a dedicated Cyber Incident Response Specialist, Cyber Incident Manager, and Account Manager.

5.5 Delivery Modes

5.5.1 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 Cyber 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 Cyber 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 Cyber 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.

8.7 Service RACI Matrix

8.7.1 The following RACI matrix defines roles and responsibilities for the delivery of the Cyber 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. Secure access to in-scope systems, applications, networks, cloud environments, and data sources is required, including administrative or read-only access as appropriate.

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.

g) **Third-Party Platforms -** Access to cloud providers, software vendors, or external platforms may require additional approvals or legal processes and may impact investigation timelines

10. Exit and Offboarding

10.1.1 The Cyber 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*****