G-Cloud 15 Service Description

Digital Forensics and Incident Response Service

January 2026

CONTENTS

1 SERVICE OVERVIEW

1.1 Service Summary

CYPFER is an NCSC CIR Assured Provider and CREST CIR Approved Provider, recognised for delivering world-class Digital Forensics and Incident Response and Response Planning services across the globe to protect the Cloud based environments of our multiple federal / public sectors clients.

Our Cyber Incident Response service is underpinned by our 24/7/365 global cyber incident response and recovery capability, designed to mobilise immediately upon request. Our mobilisation process operates across multiple time zones, ensuring uninterrupted coverage and immediate allocation of personnel.

As an NCSC CIR Assured and CREST CIR Approved provider, CYPFER delivers verified, standards-based capability across all phases — from immediate triage and containment to recovery, reporting, and lessons learned.

This ensures the client receives not only a rapid and effective technical response, but also a governance-compliant, auditable, and confidence-building process.

1.2 Key Features

Key features of the CYPFER Digital Forensics and Incident Response service are:

- CYPFER's global expertise and 24/7/365 incident response capability
- Guaranteed immediate availability and defined response times
- Structured communication and governance, ensuring clarity, accountability, and compliance
- Risk-driven methodology that protects evidence, reduces downtime, and strengthens resilience
- Comprehensive, and auditable reporting for every incident response engagement
- Experience in commercial, government and policing environments
- Dedicated, security cleared personnel with industry recognised certifications
- Alignment to NCSC CIR, CREST CIR, and ISO/IEC 27035 standards

1.3 Key Benefits

The key benefits of the CYPFER Digital Forensics and Incident Response service are:

- Rapid and immediate triage, resource assignment and communication
- Securing of crucial evidence and prioritisation of recovery efforts
- Comprehension of nature of the breach to minimise business disruption
- Minimised financial losses, tarnished reputations, compromised product integrity
- Protection against reputational damage and regulatory non-compliance
- Specialist digital forensics to facilitate internal, legal and enforcement inquiries

2 SERVICE DESCRIPTION

2.1 Service Outline

CYPFER's Digital Forensics and Incident Response service is based around our Initial Engagement and Incident Response Process which combines speed, structure, and governance to ensure that every cyber incident is managed efficiently, transparently, and in full alignment with public-sector expectations.

Upon receipt of a client request, CYPFER initiates a four-phase mobilisation protocol:

- **Activation** – The request is received through our secure intake process and logged in our case management system with an Incident Response Manager appointed within minutes to act as the single point of contact for the client
- **Resourcing** – The Incident Response Manager identifies and deploys the most appropriate specialists based on the nature, scope, and urgency of the engagement
- **Preparation** – Our teams conduct a rapid review of the engagement parameters, confirm objectives, and align with the client's existing incident response framework and governance requirements
- **Deployment** – Staff can be deployed remotely and / or on-site typically within 24 hours within the UK, ensuring a seamless transition from request to action

This rapid mobilisation capability is underpinned by dedicated in-house resources – CYPFER does not outsource its response personnel – enabling us to guarantee immediate availability of appropriately cleared and qualified experts.

Accreditations and Certifications

As an NCSC CIR Assured Provider and CREST CIR Approved Provider, CYPFER operates to externally audited technical, procedural, and governance standards, specifically:

- Cyber Essentials Plus Certification
- ISO 9001:2015 – Quality Management Systems
- ISO 27001:2022 – Information Security Management Systems
- ISO 27035 – Information Security Incident Management Framework (implemented internally)

These accreditations require continuous compliance with stringent competency, training, and assurance obligations, ensuring that all deployed staff meet the highest levels of professionalism and expertise.

Similarly, CYPFER's staff collectively hold a wide range of recognised certifications, including but not limited to:

Discipline	Certifications Held by CYPFER Staff
Incident Response & Forensics	CREST Registered Incident Manager (CRIM); CREST Certified Incident Manager (CCIM); GIAC Certified Incident Handler (GCIH); GIAC Certified Forensic Analyst (GCFA); EnCE (EnCase Certified Examiner)
Threat Intelligence & Analysis	CREST Registered Threat Intelligence Analyst (CRTIA); GIAC Cyber Threat Intelligence (GCTI)
Governance & Risk Management	ISO 27001 Lead Implementer / Lead Auditor; CISSP; CISM; CompTIA Security+
Public Sector & Legal	ACPO Digital Evidence Practitioner; Certified Data Protection Officer; NCSC Information Assurance Training Certified
Cloud & Infrastructure	Microsoft Azure Security Engineer Associate; AWS Certified Security Specialist; CompTIA Cloud+

All certifications are tracked and monitored through CYPFER's internal Competency Management System, with automated reminders for renewals and evidence of CPD (Continuing Professional Development).

Governance

Governance is embedded at every stage of the incident lifecycle, ensuring clear client accountability, and compliance with public-sector expectations.

The key steps that are undertaken to ensure governance of the incident are:

- **Client Confirmation** – All containment or recovery actions are confirmed in writing by the designated client representative before execution
- **Action Tracking** – Every activity is logged within the case management system, including initiator, timestamp, and approval status

- **Quality Oversight** – A senior CYPFER governance lead reviews technical recommendations for alignment with NCSC and ISO 27035 standards
- **Reporting Chain** – All updates and deliverables follow the client's established Gold / Silver / Bronze hierarchy
- **Formal Documentation** – Each incident concludes with a Final Incident Report (FIR) signed by CYPFER and the client representative, confirming closure and lessons learned

This ensures all actions are properly authorised, auditable, and compliant with contractual, regulatory, and internal governance frameworks.

Risk Management

CYPFER employs a dynamic risk management model that operates continuously throughout the engagement, from triage to recovery.

Risk Identification:

- Risks are identified during scoping, triage, and analysis
- Each risk is assigned a category: Technical, Operational, Legal/Compliance, or Reputational

Risk Evaluation:

- Impact and likelihood are scored on a 1–5 scale (low to critical)
- Mitigation strategies are prioritised based on client risk appetite

Risk Register:

- Maintained live within the case management system and shared with the client
- Reviewed during daily coordination calls
- Updated after each major decision or containment milestone

Common Risk Examples:

Risk	Mitigation
Data exfiltration before containment	Immediate isolation and dark-web monitoring.

Risk	Mitigation
Ransomware encryption propagation	Rapid network segmentation and endpoint containment.
Evidence contamination	Chain-of-custody enforcement and forensic imaging.
Delayed executive decision-making	Structured escalation and real-time briefings.
Third-party coordination delays	Pre-defined contact list and delegated authorisation.

This risk-driven approach ensures all decisions are evidence-based, traceable, and aligned with the client's strategic objectives.