G-Cloud 15 Service Description

Incident Response Planning 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 environment of our clients.

These clients include those that operate within multiple federal / public and private sectors, including commercial, finance and insurance, law enforcement, legal and other regulated industries.

Our Cyber Incident Response Planning service ensures that every client receives a bespoke, operationally aligned Cyber Incident Response Plan (CIRP) – one that goes beyond documentation to become an actionable, tested, and auditable framework capable of defending, responding to, and recovering from modern cyber threats.

1.2 Key Features

Key features of the CYPFER Cyber Incident Response Planning service are:

- Technically sound and practical Cyber Incident Response Plan
- Bespoke CIRP aligned to client structure and threat landscape
- Alignment with internal and external governance standards
- Establishment of the current maturity, risk exposure, and critical dependencies
- Support for the rollout, communication, and adoption across the organisation
- Testing, review, and continuous improvement of the CIRP
- Demonstrable readiness and compliance with frameworks
- Adherence to NCSC Cyber Assessment Framework, ISO 27001 / 27035
- Aligned with the Government Cyber Security Strategy (2022–2030)
- Resource from NCSC CIR Assured Provider and CREST CIR Approved Provider

1.3 Key Benefits

The key benefits of the CYPFER Cyber Incident Response Planning service are:

- Bespoke, operationally integrated Cyber Incident Response Plan
- CIRP aligned to your unique governance and infrastructure

- Improved organisational readiness, governance visibility, and compliance
- Proactive roadmap for continuous improvement and cyber resilience
- NCSC CIR, CREST CIR, and ISO 27035 best practice assurance
- Access to CYPFER's global expertise and 24/7 incident response capability

2 SERVICE DESCRIPTION

2.1 Service Outline

CYPFER's Cyber Incident Response Planning service ensures that every client receives a comprehensive, tailored, and operationally ready Cyber Incident Response Plan (CIRP) that prepares the organisation to anticipate, withstand, and recover from cyber incidents effectively.

Through our NCSC CIR assurance, CREST CIR accreditation, and extensive experience, we provide the assurance of a partner with verified capabilities, recognised governance, and proven real-world expertise.

The result is a plan that not only meets compliance requirements but enhances resilience, strengthens accountability, and ensures that the client is ready to respond with confidence when it matters most.

Risk Management in Plan Development

CYPFER applies a risk-led approach throughout the planning lifecycle to ensure that the CIRP addresses both known and emerging risks.

A live Risk Register is created at project inception and maintained throughout delivery and CYPFER's risk management process follows ISO 31000 principles, incorporating both technical and project delivery risk considerations around:

- **Identification** – Risks captured during scoping and stakeholder interviews
- **Assessment** – Categorised by severity and likelihood
- **Mitigation** – Actions defined with responsible owners
- **Review** – Risk Register updated weekly and shared with the client

Key Risk Considerations:

Category	Description	Response
Technical Risks	Identification of vulnerabilities or outdated systems during planning	Documented in the Risk Register and referred to the client's IT team for remediation

Governance Risks	Misalignment with internal approval or oversight frameworks	Early engagement with governance stakeholders and defined sign-off criteria
Operational Risks	Lack of resource availability or staff turnover affecting plan ownership	Defined role redundancies and backup contacts in the CIRP
Compliance Risks	Failure to meet data protection or regulatory obligations	Integration of GDPR, DPA 2018, and NCSC CAF principles

The risk register is maintained throughout development, reviewed weekly, and shared with the client to ensure visibility and proactive mitigation.

Supporting Organisational Readiness

Beyond technical documentation, CYPFER focuses on organisational resilience and cultural readiness. We work closely with leadership and operational teams to embed security awareness and incident preparedness across all layers of the client.

Our approach includes:

- **Executive Briefings** – Ensuring senior leaders understand their governance and decision-making roles during a cyber incident
- **Cross-Functional Coordination** – Supporting integration across IT, HR, legal, and communications functions
- **Experience** –Leveraging our experience with police forces, local authorities, and government agencies to align response structures with established governance frameworks
- **Awareness Campaigns** – Reinforcing the importance of timely reporting, evidence preservation, and structured escalation

CYPFER's multidisciplinary approach ensures that the CIRP is owned by the entire organisation and not just by IT or security teams.