G-Cloud 15

Cyber Incident Response Service

January 2026

Contents

Cyber Incident Response Service

This section describes in more detail the service features and benefits included within this service definition document.

Cyber Incident Response Service

We provide a comprehensive, end-to-end cyber incident response capability that helps organisations prepare for, detect, respond to, contain, and recover from cyber security incidents across on-premise, hybrid, and cloud environments. Our services combine threat-led expertise, digital forensics, incident management, and crisis coordination to reduce impact, restore operations, and strengthen long-term cyber resilience.

Cyber Incident Response Service Features

- End-to-end cyber incident response across on-premise and cloud environments
- Incident preparation, response, recovery and post-incident review support
- 24/7 access to cyber incident response specialists
- Structured incident triage, containment and eradication services
- Coordinated technical and business incident response management
- Support for hybrid, multi-cloud and legacy environments
- Post-incident lessons learned and improvement recommendations
- Optional cyber incident response retainer services
- Integration with existing security, IT and crisis management processes.

Cyber Incident Response Service Benefits

- Reduces impact of cyber security incidents on business operations
- Enables rapid response to cyber security incidents
- Supports faster recovery of critical services after incidents
- Improves organisational preparedness for cyber incidents
- Reduces business disruption, risk and recovery costs
- Supports consistent incident response across on-premise and cloud environments
- Improves coordination during cyber incident management
- Strengthens cyber resilience through lessons learned
- Provides access to specialist cyber incident response expertise
- Supports effective incident mitigation and containment.

Our view on the service features and benefits within this service definition document are presented below.

PwC's cyber incident response capability provides organisations with a proactive and reactive service spanning preparation, detection, response, containment, eradication, recovery, and post-incident learning. Our team brings broad and deep expertise across technical forensics, crisis management, threat intelligence, cloud and hybrid environments, regulatory compliance, and stakeholder communication, enabling organisations to reduce impact, restore operations, and improve long-term resilience.

1. Incident preparedness

We provide a range of services to help businesses improve their own state of readiness and ability to respond to all types of cyber threats. This includes:

- Incident playbook development
- Forensic readiness
- Technical first responder training
- Crisis framework review
- Crisis simulation
- Threat profiling.

These services are designed to help clients build and test their technical controls and processes and can be tailored to meet the needs of the client.

2. Incident response retainer

Our IR retainers provide rapid, priority access to multidisciplinary specialists across incident response, crisis management, digital forensics, threat intelligence, and communications. PwC emphasises several differentiators in its retainer model:

- Rapid mobilisation of NCSC-assured CIR Enhanced incident responders, forensics specialists, cloud IR experts, and crisis managers
- Quarterly workshops and exercises focused on readiness, threat trends and capability uplift

- Collaboration channels such as PwC-hosted Slack workspaces for continuous communication and early advisory support even outside formal invocation
- Global scale: access to 500+ DFIR and threat intelligence professionals, enabling around-the-clock coverage across time zones
- Technology-agnostic methodologies with no dependency on specific vendors or tooling.

This retainer model promotes familiarity, speed, and seamless escalation pathways in the event of a crisis.

3. Incident response

In the event of a cyber incident, we apply a structured, battle-tested methodology to investigate, contain and remediate threats. This approach aligns with NIST lifecycle principles and the expectations of the NCSC CIR scheme:

- Rapid scoping to determine incident extent, severity and priority actions
- Immediate containment guidance tailored to the threat actor's behaviour and client environment
- Digital forensics and compromise assessment across on-premise, hybrid, and cloud platforms (including our secure GCP-hosted forensic lab)
- Threat intelligence integration, including mapping adversary activity to MITRE ATT&CK and providing attribution insights
- Crisis management and executive advisory, enabling informed decision-making during high-pressure events
- Regulatory and legal support, including guidance aligned to UK/EU data protection obligations and sector-specific requirements
- Liaison with NCSC, law enforcement, regulators and external stakeholders where appropriate.

PwC's IR work is grounded in years of hands-on experience, NCSC assurance, and deep technical IR tooling and methodologies.

4. Post incident reviews

We deliver independent, consistent and evidence-based post-incident reviews focused on identifying lessons learned and improving organisational resilience.

Our structured approach includes:

- Root cause analysis using forensic findings and stakeholder interviews
- Evaluation of incident management processes, comparing observed actions to best practice (NIST, NCSC, ISO 27035)
- Review of crisis management structures, decision-making, communications and escalation pathways
- Assessment of legal, regulatory, privacy and stakeholder engagement activities
- Actionable recommendations to embed learning and strengthen preparedness.