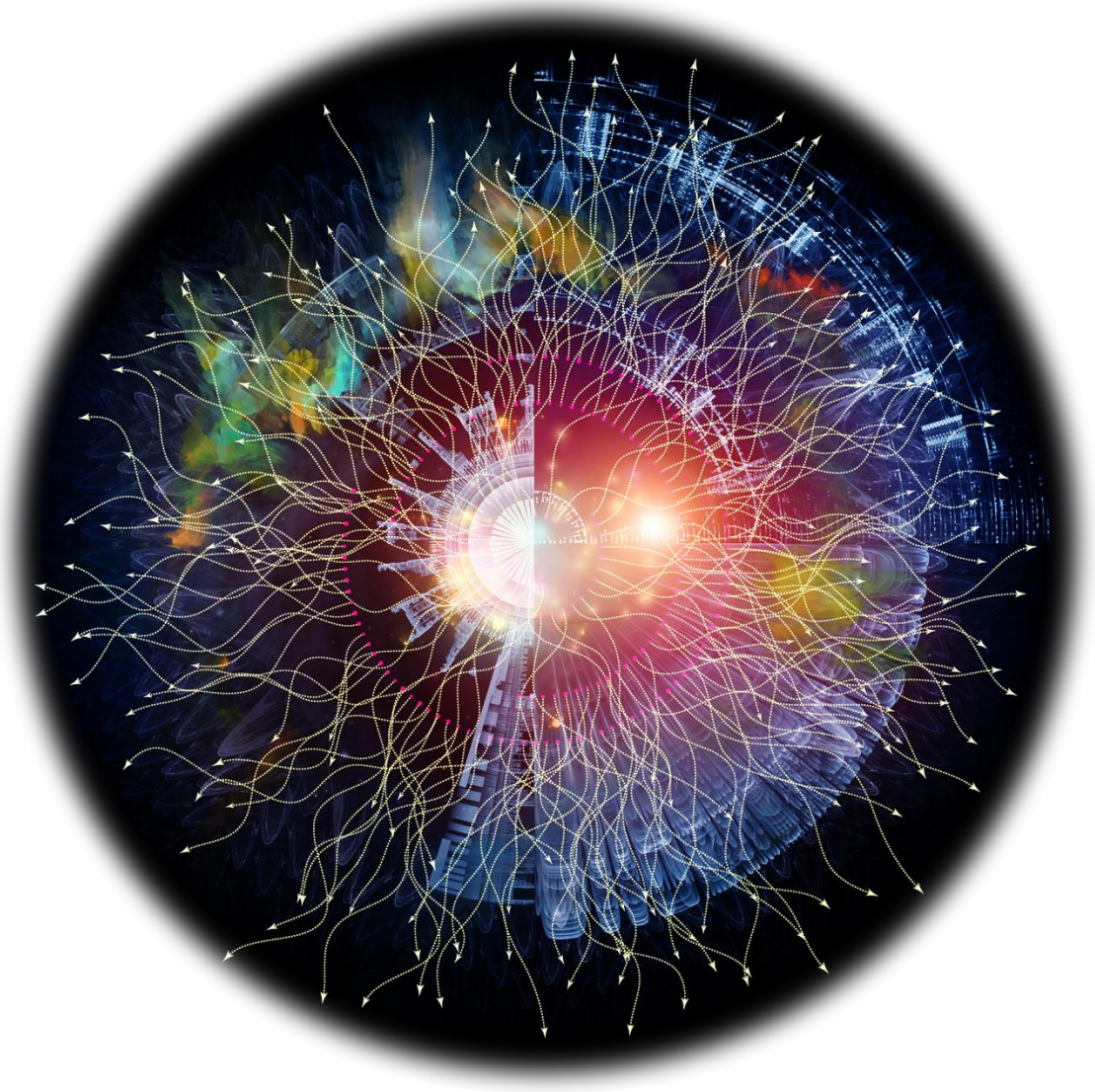
Deloitte.



Cyber Incident Response

G-Cloud 15 Service Definition Document

January 2026

Contents

1 Deloitte Overview

As a leader in professional services, Deloitte LLP is committed to making an impact to our clients, our people and for society. We have over 27,000 staff based across the UK providing audit, risk advisory, tax, consulting, financial advisory and legal services to public and private clients across multiple industries. We work together to build trust, support inclusive growth, and build capability, enabled by our **breadth and depth of expertise across advisory, delivery, engineering and managed services.**

Our **public sector practice** serves Central Government, Government Agencies, Local & Regional Government, Defence, Security and Justice, Health and Social Care, Transport, Education and Housing. We also provide services to the Northern Ireland Office, Scottish Government, Welsh Government and Crown Dependencies.

Our Cloud Capability

At Deloitte, we help our clients **Imagine, Deliver** and **Run** the businesses of the future through the power of **Cloud**. We have deep Cloud architecture, engineering, operational, commercial, and business transformation expertise delivered by a team of more than 26,000 Cloud Practitioners globally. We have delivered over 2,000 cloud implementations over the past 5 years and have 60+ cloud centres of excellence supporting the delivery of cloud services to our clients.

In the UK, we have a team of over 100 Cloud managed service specialists plus the following certifications across AWS, Microsoft Azure, Google Cloud and Oracle Cloud Infrastructure (OCI):

We help our clients with all aspects of their journey-to-cloud and optimisation of their cloud and cloud-services investments. Our Cloud practice can support you to optimise your client investments, and to navigate your organisations cloud journey, providing specialist cloud architecture, engineering, and operational skills at all stages, with a large proportion of our team holding the clearances required to meet your specific security requirements.

Our AI Capability

Deloitte stands at the forefront of AI transformation and was recognised as a Leader in the 2025 IDC MarketScape for Artificial Intelligence (AI) services for the fourth consecutive time. Supported by a £3 billion investment in AI, Data, Automation, Cloud, and Cyber, we seamlessly integrate our deep AI expertise with our extensive cloud capabilities. Our UK team is part of 339K AI-fluent practitioners globally, and includes over 1,300 AI specialists and engineers, many of whom hold the necessary security clearances for public sector delivery.

Through the Deloitte AI Institute, our hub for cutting-edge research and innovation, and strategic alliances with leading hyperscalers, we empower public sector clients to optimise costs, streamline processes, and navigate their AI journey. We achieve this by leveraging our ReadyAI™ models, which provide end-to-end support for AI solution implementation, and our Trustworthy AI™ framework, providing responsible and ethical deployment.

© 2026 Deloitte LLP. All rights reserved.

Our alliances & ecosystems

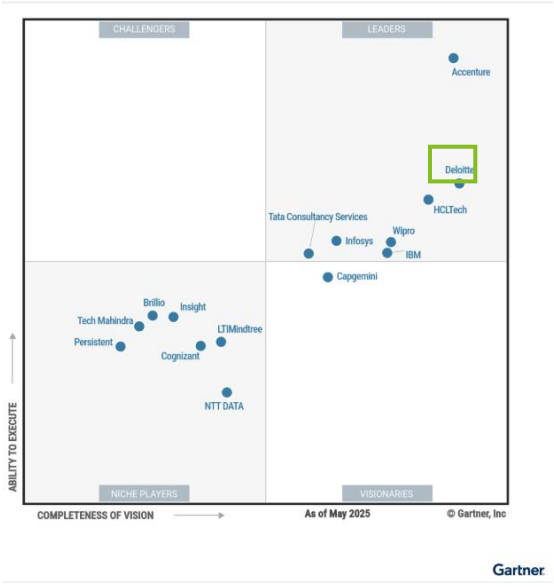
To bring full value to our clients, Deloitte is a premier consulting partner with all the leading hyper-scale cloud vendors in the market including AWS, Google, Microsoft[1], and SAP. A selection of our partners and alliances are presented below:

What the analysts say

Don't just take our word for it. Deloitte is recognised by the analyst community as being **leaders in cloud transformation services.** This reflects the wealth of experience we have in delivering cloud services across the public sector and wider private sector combined with our out-of-the-box templates, tools and assets.

Gartner

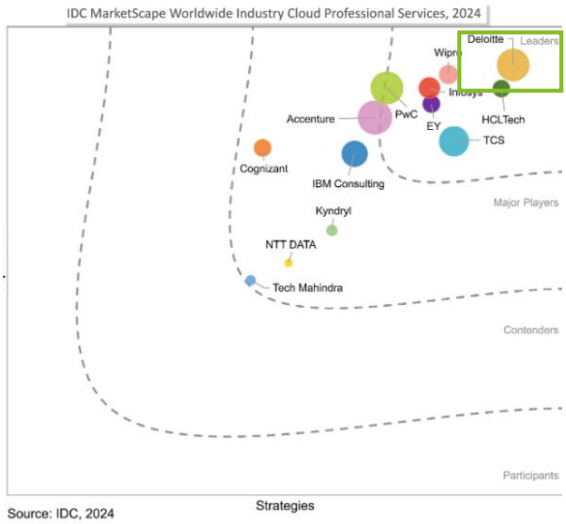
Originating in 2021, Deloitte has been recognised as a Leader in this category for four years in a row. Deloitte was also positioned as a Leader in the **Gartner Magic Quadrant for Public Cloud Infrastructure Professional and Managed Services, Worldwide** in 2021, 2020 and 2019, the previous form of this category.



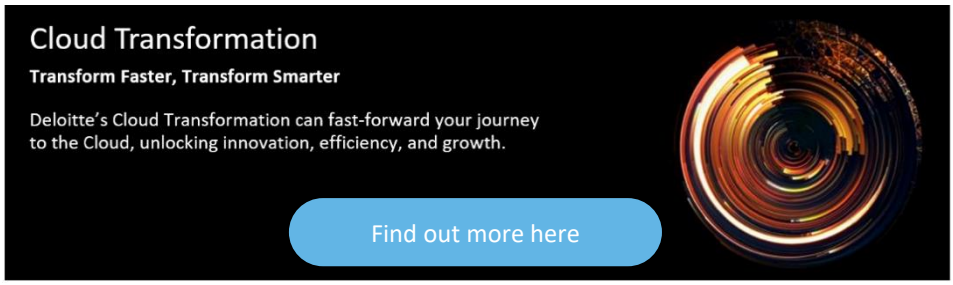
Gartner: Magic Quadrant for Public Cloud IT Transformation Services. © Gartner inc. 2025

IDC

Deloitte has been awarded Leader status in the **IDC MarketScape: Worldwide Industry Cloud Professional Services 2024** Vendor Assessment. We have also been recognised as Leaders in **Hybrid IT Consulting & Integration Services** and **Software Engineering Services**.



IDC MarketScape: Worldwide Industry Cloud Professional Services Vendor Assessment
© IDC inc. 2024



[1] As Microsoft's Independent Auditor, Deloitte cannot have a direct or material indirect business relationship with Microsoft, such as having an alliance or being a registered partner. Nonetheless, Deloitte can provide Microsoft-related technology services and invests heavily across its global business building technical skills and capabilities to develop world-class consulting and solution delivery capabilities.

© 2026 Deloitte LLP. All rights reserved.

2 Service Overview

Our NCSC Enhanced Cyber Incident Response Service is designed to assist security teams with the effective management of security incidents, breaches, or attacks from either internal or external threats. We provide critical support when organisations may lack the necessary resources, technology, or expertise to resolve incidents effectively.

Our primary goal is to limit the impact of any cyber incident, enabling your business to resume normal operations as swiftly as possible, with the aim of emerging stronger. Our offering includes a range of capabilities across incident response and retainer services.

Features

- Cyber Incident Response Retainers
- Cyber Incident Response Emergency Technical Support
- Cyber Incident Recovery
- Crisis Management

Benefits

- Cyber Incident Response Retainer and response SLAs.
- Access to skilled incident management expert when a crisis occurs.
- Support with technical analysis, containment and post-incident management.
- End to end incident lifecycle coverage from preparation to recovery.
- Analysis of root causes, response effectiveness and adequacy of remediation.
- Industry-aligned methodologies, facilitating effective response.
- Safe recovery of critical business services.

© 2026 Deloitte LLP. All rights reserved.

3 Detailed Service Description

We deliver a **NCSC Enhanced incident response** and retainer services, providing robust and trusted cyber resilience. Our quality is underpinned by a multidisciplinary team of industry-leading experts and extensive experience, honed across diverse sectors including government, public services, defence, telecommunications, transport, and the private sector. This deep, practical expertise, gained from **navigating complex incidents** like ransomware, Advanced Persistent Threats (APTs), network intrusions, and data breaches, means we deliver **proven methodologies** and rapid, effective solutions, prioritising your operations.

Assured Service Provider

in association with National Cyber Security Centre

Cyber Incident Response: Enhanced Level

We can provide you with **rapid and on-demand** access to a pool of highly skilled and experienced incident response professionals to help you when your cyber security is breached.

Incident Response

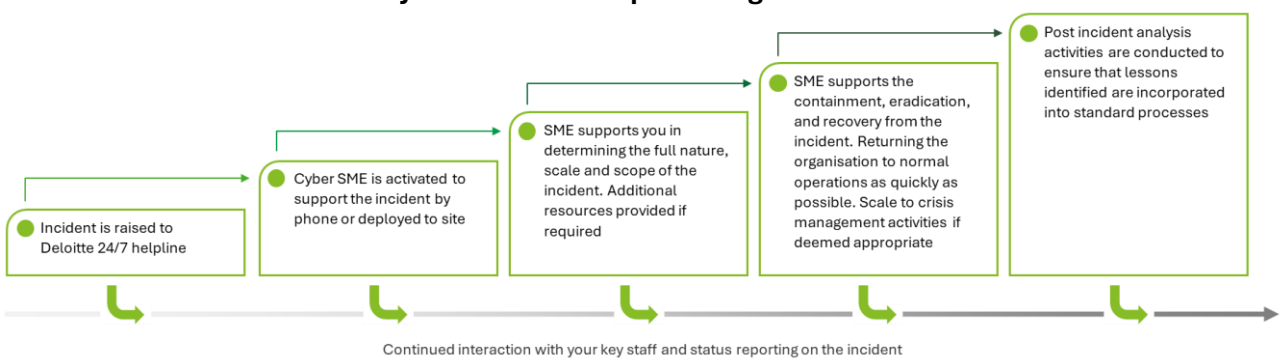
Our **24/7** incident response capabilities **mean** you have immediate access to our expertise when a cyber incident occurs, underpinned by a structured **methodology** to **contain, investigate and recover.**

Our Incident Response Service

Our capabilities include, but are not limited to:

- **Incident Management & Coordination**: We establish an overarching governance, project management, and coordination workstream, seamlessly integrated with your existing processes and recovery structure, providing comprehensive management and coordination throughout the incident and recovery lifecycle.
- **Digital Forensics & Technical Response**: Our Digital Forensics and Technical Response specialists identify and investigate cyber incidents to efficiently determine root-cause, informing your containment and recovery strategy, and allowing you to resume operations quickly following an incident. Services they provide are, but not limited to the following:
    - **Endpoint forensics** – collecting, preserving and analysing information gathered from systems.
    - **Malware analysis** – detecting and analysing pieces of advanced malicious malware, that may threaten client infrastructure.
    - **Log file analysis** – collecting and analysing large volumes of log data from various systems using automated and manual techniques.
- **Remediation & Recovery:** Our recovery and technology transformation specialists support in stabilising and securing the business in the aftermath of a cyber incident, augmenting your team to restore trust and emerge stronger than before.
- **Cyber Threat Intelligence**: Our threat intelligence analysts work alongside our investigation team to contextualise threats and their implications and operate a deep/dark web surveillance capability to identify instances of compromised data.

Our Cyber Incident Response High Level Process



© 2026 Deloitte LLP. All rights reserved.

Additional Services

In addition to our core incident response capabilities, our teams can provide the following services in an incident:

- **Cyber Crisis Executive Support**: Our senior cyber experts provide decisive leadership during a cyber crisis, aiding in strategic decision-making and offering advice and challenge on planned courses of action.
- **Privacy Breach Support**: Our managed offering helps organisations minimise the impact of a data breach by putting those impacted at the heart of the response, including breach notification plans, communications, and trained resources to engage, support and those impacted.
- **Electronic Discovery:** Our experts will help you with a fully integrated range of services, from collection, filtration, review, production and presentation of structured data to help you successfully respond to litigation, regulatory requests or disclosure, and classification of data.
- **Vulnerability Management:** Our experts will support you in mapping your attack surface, identifying and remediating vulnerabilities and prominent exposures, addressing weaknesses in your external perimeter and internal technology estate.
- **Threat Monitoring:** Our Security Operations analysts can mobilise quickly to provide you with critical burst capacity for enhanced surveillance and greater visibility of activity across your networks.
- **Restoration & Takeback:** Our comprehensive recovery services focus on securely restoring your environment post-incident, including critical 'takeback' activities. This involves rebuilding and hardening Identity & Access Management (IAM) infrastructure and core identity and directory services, facilitating Network Takeback by establishing secure access paths and advising on recovery strategy, and rebuilding and securing Endpoints through management, secure zoning, and baseline configuration.
- **Strategic Rebuild**: We help you determine the Minimum Viable Company (MVC) and establish a Business Advisory Board to set a recovery schedule. This includes infrastructure rebuild to secure and clean existing infrastructure, restore site services, and applications rebuild with recovery strategy, architectural updates, and application uplift.

Retainers

A retainer is a preplanned contract that allows the rapid mobilisation of resources to support a client quickly in response to a cyber incident. When we establish a retainer, you will be on-boarded so our Cyber Incident Response teams get to know you, your technology and your processes, facilitating a more seamless and effective deployment when we are invoked. Pricing of the retainer will be based on factors including the pre-agreed SLAs, volume of hours purchased and applicable service fees. We will help you determine a pre-defined number of hours up-front that are used in the event of a response so that you can mobilise the applicable services articulated above. This flexible model also allows for unused hours to be repurposed for proactive advisory services, enhancing your overall cyber resilience.

Core Retainer Service

We provide essential support including:

- **24/7 Emergency Response Hotline**: Provides rapid, round-the-clock access to incident response specialists who can respond to cyber incidents and deliver on the services above with speed, efficiency, and scale.
- **Dedicated Technical Point of Contact (POC)**: Offers access to Deloitte's technical expertise and insights across Cyber Defence, Security Operations, and Technical Incident Response.
- **Retained Service Onboarding**: A kick-off workshop to introduce your Deloitte retained service and dedicated account manager, sharing an operations manual and current state observations.
- **Ongoing Service Management & Continuous Excellence**: Includes regularly scheduled check-ins and formal quarterly service reviews with Deloitte's Cyber Incident Response specialists to discuss developments in your cyber threat landscape, Deloitte's insights and lessons from recent response activities, and your organisational context and cyber posture.

© 2026 Deloitte LLP. All rights reserved.

- **Advanced Threat Surveillance**: We offer comprehensive monitoring services including Dark Web Monitoring of criminal communities and marketplaces, Credential Breach Reporting for proactive resets, Dedicated Leak Site (DLS) Monitoring for data breach tracking, Breached Data Downloads for impact assessment, and Critical Threat Monitoring of discussions involving your brands, executives, and other pertinent terms, all to proactively identify and assess threats to your organisation and data.

Standard Service Level Agreements (SLAs)

We establish agreed SLAs for critical reactive capabilities, providing critical skills precisely when required. SLAs will be agreed with you upon engagement, however indicative timelines include:

- **Initial Response**: Remote triage from an incident response SME within 2 hours.
- **On-site Mobilisation**: Response specialists and SMEs in transit within 24 hours, if required.

Incident Readiness

We also offer Incident preparedness and capability building services. These can be found in our Cyber Incident Readiness G-Cloud 15 Service Definition Document.

© 2026 Deloitte LLP. All rights reserved.

4 Contact Details

Please send your requirement to publicsectorbidteam@deloitte.co.uk. Alternatively, if you wish to discuss your requirements in more detail, please send us the following information and we will be happy to contact you:

- Your organisation name
- The name of this service
- Your name and contact details
- A brief description of your business situation
- Your preferred timescales for starting the work.

© 2026 Deloitte LLP. All rights reserved.

Deloitte.

This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London, EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

© 2026 Deloitte LLP. All rights reserved.