



G-Cloud Service Definition

Managed IT and Cloud Support

For G Cloud 15



Managed IT and Cloud Support

D2NA provides a modern, security first Managed IT Support Service designed for UK public sector organisations that require dependable, accountable, and proactively managed cloud and end-user environments.

Founded on 20 years of experience delivering managed IT and cyber security services, D2NA combines deep technical expertise with a commitment to operational excellence and measurable service improvement.

Our service is built on the Cyber Ascend Framework, our structured approach for strengthening resilience, improving service maturity, and aligning technology to organisational goals.

Security First Approach Backed by Accredited Expertise

D2NA is a security led organisation, supported by extensive accreditations and specialised cyber capabilities. We are trusted by CREST and IASME with a UK-based SOC and specialist capabilities across vulnerability management, penetration testing, and governance services.

This security pedigree directly informs our managed IT support model. Every element of our service is designed to reduce risk, strengthen resilience, and ensure compliance with public sector standards such as Cyber Essentials Plus, ISO/IEC 27001, and NCSC guidance.

Comprehensive Managed IT Support

Our Managed IT Support Service includes:

- ✓ Unlimited service remote, and onsite support desk (standard service operates 7am–7pm Monday - Friday, excluding public holidays, with UK based staff)
- ✓ Endpoint protection, patching, and vulnerability management
- ✓ 365 an Email security
- ✓ Proactive infrastructure monitoring and infrastructure patching
- ✓ Managed backups, daily checks, and monthly test restores
- ✓ Annual technology transformation reviews
- ✓ Optional full service management (Service Delivery Manager + Technical Account Manager)
- ✓ 24x7 support uplift for critical incidents

Automation Driven Service Delivery

We use an integrated tooling stack for endpoint management, infrastructure monitoring, and event alerting. Automation reduces risk, accelerates issue resolution, and ensures consistent operational governance.

Designed for UK Public Sector Requirements

Public-sector organisations choose D2NA because we consistently demonstrate:

- ✓ Security-first service delivery aligned to regulatory and assurance frameworks
- ✓ UK based staff, SOC operations, and support presence
- ✓ Modern tooling, automation, and continual improvement
- ✓ Transparent governance and strategic guidance
- ✓ A proven track record supporting organisations at scale

Our Cyber Ascend Framework ensures each customer receives a structured roadmap for maturity, resilience, and digital improvement—strengthening both operational performance and long-term organisational capability.

How we meet 98% of targets and are always improving

We are confident in our service performance and continuous improvement and include SLA results in your monthly service reports to ensure full transparency and to provide a basis for ongoing discussions regarding the fulfilment of your requirements.

Typical SLAs

The Service Level Agreement (SLA) is driven by each incident and problem being assessed and given a priority number, which is calculated by our Service Desk team. We assess urgency and impact to correctly prioritise issues. Urgency is defined by the end user reporting the incident. Impact is established by verifying the number of people affected. We use the following matrix to inform the action we take:

		Impact		
Urgency		High	Medium	Low
	High	P1	P2	P3
	Medium	P2	P3	P4
	Low	P3	P4	P4

P1 - 1 Hour Response. Target Fix 2 Hours.

P2 - 1 Hour Response. Target Fix 4 Hours.

P3 - 4 Hour Response. Target Fix 8 Hours.

P4 - 4 Hour Response. Target Fix 16 Hours.

In all cases, we escalate the case to the Service Desk Manager if 75% of the agreed response time has passed to ensure we meet our SLA as you expect.

SLA's for onsite support

- ✓ Next business day on site
- ✓ Midday cut off for requests for next day site visits