D2NA

G-Cloud Service Definition

Cyber Security Assurance Services

For G Cloud 15

CREST SECURITY TESTING — Penetration Testing

CREST SECURITY OPERATIONS — Security Operations Centre

CREST SECURITY TESTING — Vulnerability Assessment

CYBER ESSENTIALS PLUS

Vanta PARTNER

PEERS QUALITY ASSURANCE LTD — UKAS MANAGEMENT SYSTEMS — ISO 9001:2015 9940

PEERS QUALITY ASSURANCE LTD — UKAS MANAGEMENT SYSTEMS — ISO/IEC 27001:2022 9940

Who We Are

D2NA is a UK-based cybersecurity specialist with over 20 years' experience supporting public and private sector organisations.

We're trusted by CREST and IASME to deliver Cyber Essentials/Plus, Penetration Testing, SOC and Managed Support Services. We are proud to be one of only 41 UK-based Security Operations Centres (SOCs) accredited by CREST, the gold standard for security assurance.

Our team holds key industry certifications, including ISO/IEC 27001:2022 for information security, ISO 9001 for quality management, and Cyber Essentials Plus. These accreditations demonstrate our commitment to the highest standards of security, quality, and continual improvement.

Cyber Security Assurance Services

Part of D2NA's Cyber Ascend Framework

D2NA's Security Assurance Services provide UK public-sector organisations with a complete, accredited and intelligence-led capability for assessing, validating, and strengthening their security posture. Delivered through our Cyber Ascend Framework, every engagement is designed to provide measurable assurance, reduce risk, and demonstrate alignment with government security and compliance standards.

Our services include **Penetration Testing, Red Teaming, Purple Teaming, Cyber Essentials / Cyber Essentials Plus, Cyber Security Health Checks, Governance Risk & Compliance, Cyber-Attack Simulation ("Exercise in a Box"), Phishing Testing & User Awareness Training, and Virtual CISO advisory support.**

Our Approach

All testing is delivered by **CREST-certified specialists** using proven methodologies. Our approach emphasises **safe delivery**, **zero operational disruption**, and **clear scoping**, ensuring that tests reflect real-world attacks while respecting service availability and operational constraints. Engagements include a structured scoping workshop, rules of engagement, risk assessment, and a detailed post-engagement briefing with prioritised remediation actions.

Designed specifically for the UK public sector, our services support compliance with **Cyber Essentials Plus, ISO 27001, NCSC guidance, GDPR,** and **sector-specific regulatory requirements**, and help organisations validate controls, strengthen resilience, and assure stakeholders. With a **UK-based team** and deep partnerships with vendors such as **Microsoft**, D2NA provides trusted, high-quality assurance that is transparent, evidence-driven and aligned to public-sector expectations for accountability.

Penetration Testing

D2NA's CREST-certified penetration testing provides organisations with measurable evidence of their exposure to real-world attack methods. Using safe, controlled testing aligned to public-sector assurance expectations, we identify vulnerabilities across networks, infrastructure, applications and internal environments, then prioritise them by risk. Outcomes include reduced attack surface, improved patching effectiveness, and clearer investment decisions. Our approach supports compliance with UK standards and demonstrates due diligence to internal audit and oversight bodies.

Red Teaming

Red Teaming simulates advanced, persistent adversaries to reveal how attackers could infiltrate, move laterally, and target critical assets. D2NA evaluates people, processes, and technology, providing a realistic view of organisational resilience. The measurable outcomes include improved incident detection, enhanced security awareness, strengthened response coordination, and validation of existing controls. These exercises help organisations understand genuine attacker pathways and prioritise high-value improvements.

Purple Teaming

Purple Teaming directly accelerates defensive maturity by pairing D2NA's offensive specialists with your defensive teams in collaborative exercises. Every activity generates measurable uplift in detection capabilities, SOC effectiveness, SIEM tuning, and response workflows. Public sector teams benefit from immediate knowledge transfer, clear skill uplift, and tangible improvements to defensive capability aligned with modern threat behaviours.

Cyber Essentials & Cyber Essentials Plus

As an IASME approved certification body, D2NA helps organisations achieve and maintain Cyber Essentials and CE Plus. Our process identifies gaps early, supports efficient remediation, and ensures controls are implemented correctly. Outcomes include faster certification cycles, consistent compliance, reduced vulnerability to common attack vectors, and clearer assurance for internal audit, boards, and regulators.

Cyber Security Health Checks

D2NA's Health Checks provide a holistic and comprehensive review of infrastructure, identity, endpoints, cloud configuration, policies, processes and people. The output is a prioritised, evidence based roadmap aligned with UK public sector frameworks. Outcomes include reduced configuration risk, clearer governance, improved policy alignment, strengthened

access-control posture, and practical next steps that support immediate and long-term resilience improvements.

Cyber Attack Simulation (Exercise in a Box)

Our cyber attack simulations provide leadership teams and operational staff with realistic, scenario-driven practice in managing modern threats. Outcomes include improved decision-making under pressure, refined communication paths, validated incident-response plans, and enhanced organisational readiness. These exercises deliver measurable improvements in response coordination, confidence, and alignment with NCSC expectations.

Governance, Risk & Compliance (GRC)

D2NA's GRC services help organisations implement, simplify, and maintain governance structures aligned with ISO 27001, NIST, Cyber Essentials, GDPR, and internal control frameworks. Measurable outcomes include reduced audit findings, improved risk prioritisation, clearer accountability, and better alignment between security controls and service delivery expectations. We help build sustainable governance models that stand up to scrutiny from internal and external auditors.

Phishing Testing & User Awareness (D2Aware)

D2Aware combines realistic phishing simulations with targeted training programmes to measurably improve user behaviour (one of the highest-risk vectors in most public-sector organisations). Outcomes include reduced click-rates, improved incident reporting, stronger culture of vigilance, and demonstrable progress against security awareness KPIs. This supports audit requirements and aligns to organisational obligations to educate staff against common attack vectors.

Virtual CISO (vCISO)

D2NA's Virtual CISO provides organisations with access to senior, accredited security leadership without the cost of a full time post. Outcomes include accelerated policy maturity, improved prioritisation of security investments, strengthened governance reporting, clearer security strategy, and reduced organisational risk. Public sector leadership teams gain measurable improvements in oversight, documentation, and long-term planning.

Service benefits

- ✓ Reduces breach risk through D2NA Cyber Ascend Assurance penetration testing
- ✓ Improves threat readiness using D2NA Red Teaming threat-validation exercises
- ✓ Strengthens defences via Purple Teaming accelerating control effectiveness
- ✓ Ensures compliance through expert Cyber Essentials and CE Plus support
- ✓ Identifies critical weaknesses using UK public-sector cyber health checks
- ✓ Enhances preparedness through realistic cyber attack simulation exercises
- ✓ Reduces governance risk using structured GRC aligned to UK standards
- ✓ Improves user behaviour with targeted phishing testing and D2Aware training
- ✓ Strengthens strategy using Virtual CISO guidance for public-sector resilience
- ✓ Accelerates improvement using Cyber Ascend data-driven security roadmaps

Support levels

D2NA's Security Assurance Services are delivered as project-based engagements designed specifically for UK public-sector organisations requiring predictable, transparent, and independently validated security outcomes.

Support begins with pre-sales technical scoping, delivered by senior consultants to ensure requirements, risks, dependencies, and objectives are clearly understood before any work begins.

Every engagement is assigned a Technical Account Manager who acts as the customer's primary technical contact, ensuring alignment with security objectives, UK government standards, and organisational risk appetite.

All Penetration Testing, Red Teaming, Purple Teaming, Cyber Essentials/CE Plus, Health Checks, and Cyber Attack Simulation engagements include a detailed scoping session, risk review, and post-engagement advice meeting, ensuring findings are understood and remediation actions can be effectively implemented.

A Project Manager can be added as an uplift for complex or multi-phase programmes.

Customers also benefit from D2NA's high-level access to vendors such as Microsoft, enabling efficient issue escalation, licensing optimisation, and assurance that services align to best practice.

Administrative support is available for tasks such as licence management and coordination.

Pricing is project-based, fixed per engagement, and fully scoped before commencement to ensure transparency and eliminate unforeseen cost. This approach provides clarity, confidence, and demonstrable value for leadership.