

Cyber Security

Service Overview



About i3Secure

i3Secure is a trusted cyber security and information assurance consultancy. We help public and private sector organisations manage risk, meet regulatory requirements, and operate securely in today's complex digital environment. Our team is driven by ingenuity, integrity and innovation, working closely with clients to deliver meaningful, lasting outcomes.

We support organisations at all stages of their security journey, from early strategy and assurance through implementation, transition, operational maturity and decommissioning. Whether acting as a trusted advisor, delivery partner or embedded team, we create lasting value by establishing effective governance, compliance, and risk management frameworks that allow our clients to focus on their core objectives.

What we deliver

Our consultants bring deep industry knowledge and experience across defence, healthcare, government, critical national infrastructure, and commercial sectors. We've supported everything from agile SME projects to large-scale enterprise security transformations. Our approach is collaborative and pragmatic, designed to deliver outcomes that work in practice, not just on paper.

We provide a comprehensive suite of cyber security and data protection services tailored to each company's size and complexity. From preparation and protection to detection, response and recovery, our services cover the full security lifecycle. Delivered individually or as integrated programmes, our support ensures a holistic approach aligned to regulatory obligations and business goals.

These services include strategic risk management, security architecture, technical assurance, incident response, data protection, supply chain risk management and security culture development; all underpinned by leading standards such as ISO 27001, NIST, GDPR and Cyber Essentials.

Qualifications

All i3Secure consultants hold industry-recognised certifications and relevant security clearances (SC and above). Our team includes CISSP, CISM, CRISC, ISO 27001 Lead Auditors, CEH, GDPR practitioners, and NCSC-assured consultants, among others such as those below. This ensures we have the expertise to address complex challenges and deliver solutions tailored to your needs.

🔑 NIST Practitioner	🔑 COMPTIA Security+	🔑 Remedy	🔑 TOGAF
🔑 CISM	🔑 COMPTIA Network +	🔑 Azure Fundamentals	🔑 NIST CSF Foundation
🔑 CISSP	🔑 CRISC	🔑 ISC2	🔑 SAFe®
🔑 CISM	🔑 ITIL	🔑 PRINCE2®	🔑 INCOSE ASEP

We bring decades of experience delivering cyber security projects across diverse sectors. Our consultants are trained in proven methodologies and frameworks, and we invest in continuous professional development, at no cost to our clients, so you always benefit from current, high-performing expertise.

Working with you

We work collaboratively, embedding seamlessly within your organisation and ways of working. Our consultants engage effectively with stakeholders at all levels, supporting knowledge transfer, sustainable capability, and strong governance.

Flexible by design, we can operate on-site, remotely or in hybrid models. We support short-term advisory engagements, long-term programmes, embedded project teams and fully managed services. Our support scales to fit your organisation's size, complexity and evolving needs, ensuring you're positioned to manage cyber security and information assurance well beyond our engagement.

As an organisation, i3Secure is externally certified to **Cyber Essentials Plus**, **ISO 9001** and **ISO 27001**, reflecting our commitment to robust quality management and information security.



What We Can Do For You



Public sector organisations continue to transform the way they design, deliver and operate digital services, improving user experience, increasing efficiency and meeting evolving policy and regulatory demands. With **Cloud First** policies embedded across government, departments are at different stages of their cloud and digital transformation journeys.

We understand the complexity, risks and opportunities this presents. Whether you are shaping strategy, delivering change or transitioning into business as usual, we provide practical, experienced support at every stage.

- + End-to-end support from project onboarding through transition, handover and off-boarding into business as usual
- + Rapid stand-up and stand-down of teams to meet changing priorities and delivery demands
- + Seamlessly embedded consultants delivering value from day one
- + Knowledge transfer and capability building to strengthen and grow internal teams
- + Collaborative, agile delivery aligned to your governance and ways of working
- + Clear accountability and assured delivery through a dedicated Engagement Partner

When you work with us, you get far more than a consultancy. Our values of **flexibility**, **reliability** and **competitiveness** are underpinned by exceptional industry knowledge and experience. This allows us to hit the ground running and embed lasting change across the projects, programmes and portfolios we support.

Our consultants adapt quickly to your environment, applying proven approaches and innovative thinking to deliver solutions that meet your specific needs while fully aligning with Government Digital and Cloud policies.



Our Experience

Client:

MINISTRY OF DEFENCE

Project/Programme:

MODNet Modernisation

The MOD launched the MODNet Modernisation programme in 2020 to transform how 220,000 users operate. After two years of limited security oversight, i3Secure was invited in late 2022 for assurance support, based on our proven track record in large-scale Defence programmes and deep experience with Secure by Design (SbD) and governance, risk, and compliance. Three consultants joined as Security Managers, bringing strong credentials and qualifications including CC, CISM, CISSP, CRISC, and NIST CSF.

The MOD required rapid deployment of skilled Security Managers to embed a robust assurance function across delivery and live service phases. This included overseeing secure migration of 220,000 users by March 2026, with no existing cohesive security framework in place.

- + **Conducted** a two-week discovery phase including gap analysis against NIST 800-37, review of security documentation, and assessment of progress toward JSP 604 (453) Joining Rules.
- + **Implemented** a six-month “get to green” plan after delivering a second-line assessment that returned a red rating.
- + **Identified** and filled security resource gaps, including Security Architects and Delivery Team Security Leads.
- + **Embedded** the NIST 800-37 framework to integrate security into all delivery phases.
- + **Facilitated** risk workshops, SbD self-

assessments, security working groups, and reviews with the Senior Risk Owner.

- + **Managed** compliance with JSP 440 and JSP 604 (453), led test readiness activities, and supported security alignment with programme gateways.
- + **Produced** key assurance documentation including risk treatment plans, DPIAs, incident response plans, tailored NIST 800-53 controls, supplier assurance (DCPP), and a migration assessment for 600+ applications.

i3Secure has provided sustained security assurance to the MODNET Modernisation programme, resulting in five contract extensions and continued engagement through January 2026. Our consultants have embedded SbD practices, established approved governance frameworks, and supported critical testing and remediation activities.

Key outcomes include early Authority to Test (ATO) approval, rapid turnaround of eight ATO submissions, and uninterrupted programme progress. With 130,000 users migrated and the rest due on target, our support has transformed security from reactive to resilient, enabling long-term, compliant delivery at scale.



Our Experience



Client:

CROWN HOSTING FRAMEWORK AUTHORITY

Project/Programme:

CyberArk

The Crown Hosting Framework Authority (CHFA), on behalf of the Crown Commercial Service (CCS), needed to ensure the delivery of secure, resilient, and high-performing data centre services across the public sector, in line with Crown Hosting frameworks (RM1069 & RM6262). Their priorities included maintaining operational excellence, meeting strict compliance standards, and driving sustainable value for public sector customers.

To support these objectives, we worked closely with CHFA to strengthen governance, enhance service assurance, and promote a culture of resilience, transparency, and strategic oversight. Our consultants combined deep technical expertise with strategic insight to ensure delivery aligned with best practice in critical national infrastructure.

- + **Conducted** detailed audits of critical infrastructure and energy efficiency to validate resilience, availability, and sustainability.
- + **Assessed** physical, personnel, and cyber security against national standards, supported by independent assurance.
- + **Delivered** market pricing analysis, benchmarking specifications, and procurement support to ensure value for money and commercial competitiveness.
- + **Led** governance forums and working groups to drive collaboration, transparency, and measurable service improvements.



- + **Produced** a widely adopted BCDR Advisory Note providing actionable guidance to strengthen resilience and continuity planning across the public sector.

Our thorough approach delivered significant benefits to CHFA:

- + **Delivered** measurable improvements in service assurance, operational resilience, and customer confidence.
- + **Provided** clear, actionable BCDR guidance that improved continuity planning across multiple public sector customers.
- + **Fostered** collaboration, shared best practices and enabled a more standardised, proactive approach to risk management.
- + **Cultivated** a culture of continuous improvement and strengthened stakeholder engagement and trust.
- + **Reinforced** CHFA and Crown Hosting's position as trusted, secure, and resilient public sector partners.

This successful delivery demonstrates our proven capability to support government clients with secure, resilient, and compliant infrastructure solutions that meet the highest standards of public sector governance.

Our Experience

Client:

MINISTRY OF DEFENCE

Project/Programme:

Defence Developer Services

Defence Developer Services (D2S), part of the UK Defence Digital Foundry, is a cloud-based Platform as a Service (PaaS) supporting Defence and wider government teams through the software development life cycle. The platform operates at both OFFICIAL and SECRET classifications. i3Secure consultants were embedded in the programme for approximately three years as Security Architect and Cyber Risk Management specialists to enable secure, timely service development and delivery.

D2S was the first Defence Digital programme to fully adopt the Secure by Design (SbD) methodology and remains the only one awarded Continuous Authority to Operate (CATO). The programme required a compliant, risk-managed platform that enabled developer teams to build and deploy secure applications quickly while maintaining visibility and control over evolving cyber threats.

i3Secure played a central role in shaping and applying both the SbD and CATO processes:

- + **Applied** key industry (NIST, FIPS, NCSC) and MOD (JSP 440, 453, 892) standards to ensure compliance while tailoring the platform to D2S's specific needs.
- + **Designed** a continuous risk management strategy to support the CATO decision, providing the Senior Responsible Owner (SRO) with clear visibility of current and emerging threats.
- + **Delivered** a full-spectrum cyber risk assessment, resulting in a comprehensive

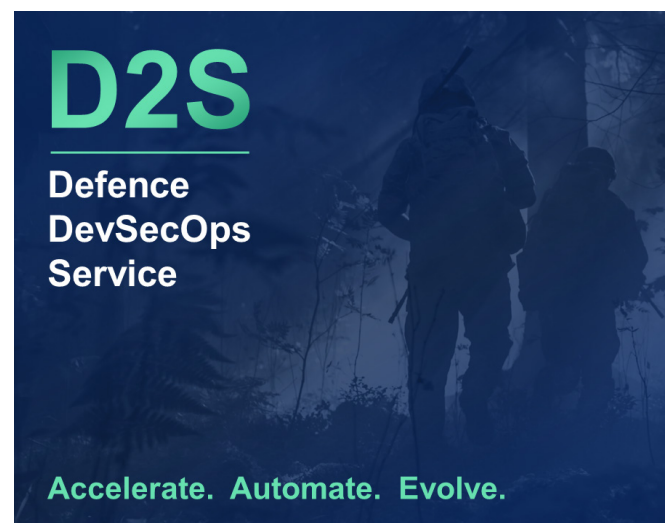
Risk Register and Risk Treatment Plan covering cyber and enterprise-level risks.

- + **Developed** a dynamic 'single-pane' risk dashboard displaying risk levels, mitigations, technical controls, policies, and governance; widely praised and now under consideration for broader adoption across the Defence Digital Foundry.

Through this project, our consultants delivered substantial, long-term benefits to D2S:

- + **Delivered** an effective, adaptable risk management process that continues to evolve with the platform.
- + **Implemented** risk mitigations that protect the platform's confidentiality, integrity, and availability.
- + **Enabled** continuous, secure platform operation without major security incidents.

In recognition of our contribution, i3Secure consultants have been actively engaged in shaping future Defence and Government cyber policy, helping create a more collaborative, efficient model for delivering secure cloud-based solutions in Defence.



Our Experience



Client:

NATIONAL HEALTH SERVICE

Project/Programme:

NHSx COVID Pass and Letter Service

Launched in 2021, the NHSx COVID Pass and Letter Service was a critical NHS initiative providing digital COVID-19 vaccination certificates and official vaccination letters. Now part of the NHS England Transformation Directorate following the NHSx-NHS Digital merger, it played a vital role in enabling safe travel and venue access during the pandemic.

To safeguard the Service, NHSx required a dedicated Cyber Security Risk Manager to take ownership of the Cyber Risk Register and manage the full lifecycle of cyber risk. Under tight time constraints, the role demanded rapid onboarding, immediate prioritisation of critical threats, and mitigation of vulnerabilities that may impact the Service's security and integrity.

i3Secure was selected to support the Service due to our proven expertise in healthcare cyber security, extensive experience working with the NHS, and flexible, collaborative approach to addressing the NHS's unique challenges.

We quickly deployed an experienced Cyber Risk Manager for a four-month engagement to work with the NHSx team to deliver both tactical and strategic cyber risk management.

- + **Identified**, analysed, evaluated, and mitigated cyber security risks ongoingly
- + **Prioritised** and responding to imminent threats while implementing responsive risk treatment strategies and controls
- + **Conducted** threat modelling and strategic vulnerability management



- + **Provided** fraud risk guidance to protect service integrity
- + **Assessed** digital infrastructure, data handling processes, and third-party integrations to pinpoint vulnerabilities and implement mitigation strategies
- + **Implemented** a healthcare-aligned cyber security framework, including data encryption, access management, intrusion detection, and incident response
- + **Delivered** tailored cyber security awareness training for NHSx staff
- + **Performed** security assessments and penetration testing to proactively identify and remediate vulnerabilities
- + **Developed** a thorough incident response plan covering communication, containment, recovery, and post-incident review

This work delivered tangible improvements across the Service, strengthened its security posture, and ensured sensitive health data was protected during a critical phase of the COVID-19 pandemic.

At contract close, our consultant completed a comprehensive handover to the Programme Management Office RAID Lead, ensuring continuity in risk management and oversight.

Client Testimonial

Client:

MINISTRY OF DEFENCE

Project/Programme:

MODNet Official



"An integral part of the MNO Security Function and wider MNO team, i3Secure has demonstrated exceptional leadership qualities along with a strong work ethic in their approach to the management and coordination of security requirements across the programme. Not without challenge, the team has navigated the programme through multiple complex issues and worked tirelessly to establish crucial stakeholder relationships, as well as to restore and maintain those previously damaged. Their positive attitude and collaborative approach has contributed to a more cohesive working environment.

Arriving at a crucial time in the programme, the i3Secure team has worked diligently to retrospectively plan and communicate MNO's approach to security assurance, developing strategic methodology to adopt and transition to Secure by Design. Furthermore, the team's organised and pragmatic approach to an unexpected CySASS assessment of the programme not only ensured that stakeholders were prepared but that work could get underway to improve processes and remedy some of the points raised ahead of the report being received.

Respected across the MNO team, i3Secure's security consultants are highly regarded for their honest and open conversations, clearly articulating options, providing advice and guidance to move forward, and offering constructive challenge to inefficient and unnecessary processes."

MNO Delivery Manager, Defence Digital, UK Strategic Command



All Services on G-Cloud



P3M



Digital Services



**Business Change &
Transformation**



Architecture



Project Controls



**Climate Security, ESG and
Sustainability**



Assurance



Data and AI Automation



Service Management



Cyber Security

Driving Public Sector Transformation Since 2014

Who We Are

i3Works Ltd is a leading UK-based management consultancy, specialising in Project, Programme, and Portfolio Management (P3M), digital delivery, and transformation within the public sector.

The i3Group comprises [i3Works](#), [i3Secure](#), [i3NetZero](#) and [i3Data](#). We combine deep expertise with innovative thinking to deliver sustainable solutions that create measurable organisational improvement.

Our Expertise

We partner with major public sector organisations such as the MoD, HMRC, DEFRA & Home Office, applying best-practice frameworks like Agile, Waterfall, and hybrid methodologies to ensure flexibility and efficiency.

Our services include:

- + P3M
- + Business Change & Transformation
- + Project Controls
- + Assurance
- + Service Management
- + Digital Services
- + Architecture
- + i3NetZero (Climate Security, ESG and Sustainability Services)
- + i3Data (Data and AI Automation)
- + i3Secure (Cyber Security)

All delivered by specialist and accredited consultants, ensuring tailored solutions for every client.

Our Vision

i3Works is committed to shaping the future of consultancy through integrity, collaboration, and impact. We strive to be the consultancy of choice for public sector transformation, delivering exceptional results that exceed expectations and create lasting value for the communities we serve.

Forward thinking

The public sector is evolving—and so are we. Our future strategy focuses on:

- AI-driven delivery and automation for smarter, faster outcomes
- Digital resilience and cybersecurity to protect critical services
- Net Zero and sustainability initiatives embedded in transformation programmes
- Data-driven insights and predictive analytics for evidence-based decisions
- Workforce capability building to prepare teams for a digital-first future

By embracing our priorities, i3Works will continue to lead the way in delivering innovative, secure, and sustainable solutions that empower public sector organisations to thrive in a dynamic world.

Let's Shape the Future Together

Discover how i3Works can help your organisation achieve its strategic goals.

Visit: <https://i3works.co.uk>

Email: info@i3works.co.uk

