

i3Secure

G-Cloud 15 Catalogue

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 P	+ 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

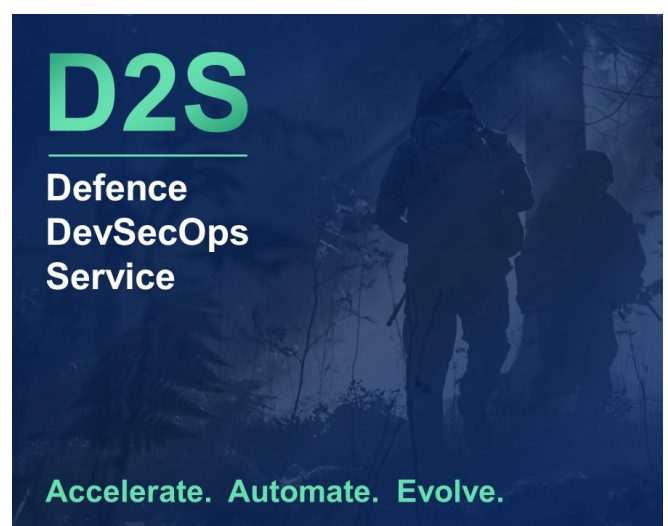
Risk Register and Risk Treatment Plan covering cyber and enterprise-level risks.

- + **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

- + Business Analysis
- + Chief Information Security Officer (CISO) as a Service
- + Cloud and Critical National Infrastructure (CNI) Security Consultancy
- + Cloud Cyber Security Consultancy
- + Cloud Security Engineering
- + Cyber Essentials & Cyber Essentials Plus (CE & CE+) Consultancy
- + Cyber Security Architecture
- + Cyber Security Risk Management
- + Cyber Security Strategy Design & Implementation
- + Data Analytics
- + DevSecOps
- + Governance, Risk & Compliance Consultancy
- + ISO 9001 Consultancy
- + ISO 22301 Consultancy
- + ISO 27001 Consultancy
- + ISO 27701 Consultancy
- + ISO 42001 Consultancy
- + JSP 453 Service Transition Officers
- + NCSC Cyber Assessment Framework (CAF) Consultancy
- + Penetration Testing & Vulnerability Services
- + Product Manager
- + Programme and Technical Assurance Support
- + Programme Management
- + Project Management
- + Resilience by Design
- + SCIDA (Site Co-ordinating Infrastructure Design Authority) Services
- + Secure by Design Awareness, Behaviour & Culture
- + Secure by Design Consultancy
- + Secure by Design Training
- + Security Assurance as a Service
- + Solution Architecture
- + Supply Chain Assurance

i3Secure provides expert Business Analysis to drive Digital transformation and business change. We support Agile (Scrum or Kanban) and Waterfall delivery across the lifecycle (Discovery, Alpha, Beta to Live). We assure benefits realisation through robust requirements engineering, and strategic alignment, compliant with GDS standards and Governance.

Features

- + Business analysis at project, programme, portfolio or enterprise levels
- + Agile (Scrum and Kanban) and Waterfall delivery support
- + Requirements engineering: elicitation, validation, documentation, and management
- + Stakeholder management, workshop facilitation, and communication planning
- + Gap Analysis including “As is” and “To be” process mapping
- + User story creation, acceptance criteria, and prioritisation
- + Support Product Owners, Delivery Managers, Engineers and UCD teams
- + Business Case development that aligns with strategic objectives
- + Integration of social value, sustainability, and low carbon practices

Benefits

- + Clear benefits realisation, ROI tracking, and value optimisation
- + Ensures complete transparency of requirements from strategic vision to delivery
- + Documentation that bridges the gap between technical teams and stakeholders
- + De-risks delivery through accurate requirements and acceptance criteria
- + Options analysis, business cases, support definition of Minimum Viable Product
- + Supports Change Adoption & Learning (CAL)
- + Transfers capability to internal teams (Upskilling and Training)
- + Optimises business processes to remove waste and improve efficiency
- + Aligns Digital solutions with GDS Service Standards
- + Incorporating social value, sustainability and low carbon practice

Chief Information Security Officer (CISO) as a Service

Chief Information Security Officer (CISO) as a Service and Virtual CISO (vCISO) as a Service provides a practical, cost-effective solution for organisations to meet security obligations. Our experienced accredited CISO consultants operate across public and private sectors, delivering cyber strategy, leadership, governance, and security management aligned specifically to business goals.

Features

- + CISO and Virtual CISO services tailored to organisational requirements.
- + CISO leadership of your cyber resilience and transformation programme.
- + Publishing and deployment of cyber security policies, standards and procedures.
- + CISO to manage cyber risk, incidents and crisis events.
- + Recommendation of services and technology to meet technical security needs.
- + Development and delivery of organisations cyber security strategy and roadmap
- + Management and leadership of security and data privacy function.
- + NCSC and DSPT Cyber Assessment Framework (CAF) alignment
- + Board-level cyber security and information assurance advice and reporting.
- + Achievement of Cyber Essentials, ISO 27001 certifications and other frameworks.

Benefits

- + Fulfilment of CISO role and responsibilities, delivered remotely, hybrid, on-demand.
- + Experienced CISOs with experience and credentials.
- + Access to trusted specialists with proven Cyber Security experience.
- + Service can be tailored to meet your specific requirements.
- + Practical solutions to achieve and maintain compliance.
- + Cost-effective compared to full time appointment.
- + Enhanced Cyber Security posture with reduced risk of Cyber Incidents.
- + Cyber and Privacy Strategy and Framework to enable the organisation.
- + Effective knowledge transfer to your organisation.
- + No conflict of interest with other duties in your organisation.

Cloud & Critical National Infrastructure (CNI) Security Consultancy

i3Secure's Critical National Infrastructure service delivers independent advice and assurance on protective security for critical national assets. Through risk-based audits, surveys, and inspections across client and supplier sites, we identify CNI, assess threats and vulnerabilities, and define proportionate, cost-effective controls aligned to JSP 440 and UK government CNI assurance expectations, ensuring operational resilience.

Features

- + Specialists in Critical National Infrastructure and JSP 440.
- + Focused or full organisational CNI assessments, including a managed service.
- + Risk based corrective advice supporting protection and resilience of CNI.
- + Services aligned to JSP 440 and government CNI security/assurance requirements.
- + Identification, prioritisation, and management of corrective actions.
- + All specialists are Security Check or Developed Vetting cleared.
- + CNI security awareness and risk culture training addressing organisational shortfalls.
- + Independent CNI assurance at third party and supply chain sites.
- + Expertise across ISO27001, CISM, DCNI, BCI CBCI, and PCI DSS.
- + Supports all classifications, including OFFICIAL, SECRET and TOP SECRET

Benefits

- + Trusted specialists with extensive JSP 440 and CNI assurance experience.
- + Services tailored to meet specific organisational and CNI operational requirements.
- + Improved CNI security and resilience with reduced risk of disruption/compromise.
- + Independent assurance that third party/supply chain CNI controls meet UK government requirements.
- + Clear mitigation plans addressing identified security, resilience, or assurance shortfalls.
- + Demonstrable alignment with JSP 440 and governmental CNI security standards.
- + Support for achieving certification against industry and government security frameworks.
- + Protection of Critical National Infrastructure, classified, and sensitive operational information.
- + Effective transfer of CNI security knowledge and assurance capability internally.

Cloud Cyber Security Consultancy

i3Secure's certified Cloud Cyber Security Consultancy delivers cost effective, scalable security for public/private/hybrid cloud environments throughout the system lifecycle. Applying industry best practice and solution specific expertise, our Cloud Cyber Security Consultants deliver robust, pragmatic IT security outcomes that manage risk, emphasise defence in depth, and drive lasting organisational resilience.

Features

- + Public/Private/Hybrid cloud cyber security for organisational risk assessment and control.
- + Posture assessments with remediation and best-practice optimisation.
- + Resilience, defence, and security by design cloud architecture.
- + Development of high-quality, industry best-practice security policies, standards, and procedures.
- + Support for security risk decision-making, incident management, and crisis response.
- + Specialist guidance on security frameworks and risk-mitigation technologies.
- + Multi-cloud, Azure/AWS, and on-premises solution architecting.
- + Threat and vulnerability assessments, including penetration testing.
- + Cloud security architecture design and integration for secure systems/services

Benefits

- + Independent assessment and validation of security posture.
- + Specialist management of data breaches, security incidents and attack-surface mapping.
- + Pragmatic, cost-effective Cloud and On-Premises cyber security support maximising ROI.
- + Accurate, risk-based decision-making with a focus on continuous improvement.
- + Access to deep technical skills, regulatory insight and best-practice expertise.
- + Access to specialist technical skills and resources for continuous improvement
- + Threat horizon scanning with strategic guidance for continuous improvement.
- + Effective knowledge transfer through embedded Cloud Cyber Security consultancy.
- + Stronger governance through development of robust cloud/IT security policies.
- + Proven delivery experience across complex hybrid IT estates.

Cloud Security Engineering

CSE is one of the high-quality services that i3Secure offers. We engineer cloud security controls aligned to organisational and regulatory frameworks. Our CSE specialists design and implement secure by default platforms, strengthen identity, harden workloads and embed continuous compliance for defence, central government and regulated environments.

Features

- + Establishes cloud cost governance and guardrails.
- + Implements tagging, telemetry and allocation models.
- + Delivers showback/chargeback processes and tooling.
- + Optimises compute, storage and licensing continually.
- + Forecasts and budgets using historical trends.
- + Identifies carbon hotspots and reduction options.
- + Aligns optimisation with SLO and resilience needs.
- + Creates playbooks for rightsizing and scheduling.
- + Trains teams on FinOps operating model.
- + Reports savings and sustainability outcomes.

Benefits

- + Lower total cost of cloud ownership.
- + Clear accountability for spend and usage.
- + Reduced waste through proactive optimisation.
- + Forecasts aligned to business demand.
- + Improved sustainability performance and reporting.
- + Balanced cost, performance and reliability.
- + Faster decisions with transparent data.
- + Consistent practices across business units.
- + Measurable savings tracked and verified.
- + Continuous optimisation cadence established.

Cyber Essentials & Cyber Essentials Plus (CE & CE+) Consultancy

i3Secure's Cyber Essentials & Cyber Essentials Plus Consultancy helps organisations understand, assess, and achieve CE/CE+ certification. Through structured gap analysis, we assess current security posture against requirements, identify gaps, and deliver prioritised, cost-effective remediation; enabling informed decisions, improved resilience, and successful certification.

Features

- + Support for CE, CE+, and ISO 27001 alignment.
- + Cyber Essentials (Plus) gap analysis defining objectives, current state, and required controls.
- + Evidence collection and assessment including configuration checks and system settings.
- + Technical and vulnerability testing, scoping, reporting and coordination.
- + Prioritised remediation plans addressing people, process, and technology gaps.
- + Support implementing security improvements to meet CE/CE+ requirements.
- + Recommendation of proportionate security controls, tools, and technologies.
- + Information Security Management System establishment and maintenance.
- + Cyber risk, incident, governance and crisis management support.
- + Development, deployment and integration of security policies, standards, and procedures.

Benefits

- + Successful achievement of Cyber Essentials and Cyber Essentials Plus certification.
- + Access to experienced Cyber Essentials consultants and specialists.
- + Availability of National Security Vetting-cleared security professionals.
- + Independent validation of organisational cyber security posture.
- + Clear insight into cyber security gaps, risks, and priorities.
- + Informed, risk-based decision-making and effective resource allocation.
- + Stronger cyber security governance and baseline controls.
- + Reduced likelihood and impact of cyber incidents and data breaches.
- + Pragmatic, cost-effective security improvements delivering maximum ROI.
- + Increased customer confidence in cyber security practices.

i3Secure Cyber Security Architecture services for the full system lifecycle, leveraging frameworks such as TOGAF guiding strategy, design, and implementation. Cyber Security architects collaborate with stakeholders to deliver secure on/off prep cloud, network, and system solutions aligned with GDS standards, reducing risk, ensuring compliance, aligning to requirements and strengthening resilience.

Features

- + Develop strategic security architecture roadmaps aligned with objectives.
- + Apply TOGAF principles for structured architecture development and governance.
- + Analyse requirements and translate them into secure, scalable designs.
- + Conduct architecture assessments, gap analysis, and infrastructure evaluations.
- + Design resilient solutions addressing scalability, integration, and performance.
- + Create architecture patterns using Zero Trust and Defence-in-Depth frameworks.
- + Identify and document risks aligned to recognised security standards.
- + Provide governance and lifecycle oversight for secure architecture delivery.
- + Offer vendor-neutral optimisation, policy development, and security governance support.
- + Future-proof architectures against emerging technologies and evolving threats.

Benefits

- + Clear strategy definition enabling secure transition and modernisation.
- + Security architecture aligned with business goals and measurable outcomes.
- + Embedded consultants ensuring streamlined communication and delivery efficiency.
- + Improved quality, consistency, and governance across all architectures.
- + Comprehensive migration strategies ensuring secure transitions within enterprise-scale environments.
- + Enhanced data insights supporting informed, evidence-based decision-making
- + Embedded risk mitigation within migration and transformation strategies.
- + Continuous innovation and improvement delivering long-term organisational value.
- + Improved ROI through collaboration with cloud and security architects.
- + Cost optimisation via efficient, scalable architecture design solutions.

Cyber Security Risk Management- a core i3Secure service. Delivery of pragmatic, cost effective threat and risk assessments aligned to recognised industry frameworks. Using proven methodologies, our Cyber Security Risk Management activities identify, analyse, and treat risks, delivering clear remediation plans that strengthen governance, reduce exposure, and enhance organisational resilience.

Features

- + Task-specific or organisation-wide Cyber security risk management services.
- + Threat assessments and security risk posture evaluation with remediation support.
- + NIST, ISO, COBIT aligned risk assessment, treatment, and risk remediation planning.
- + Integrated/proactive continual risk management enabling secure, trustworthy, and resilient systems.
- + Development and deployment of security policies, standards, and procedures.
- + Independent expertise to strengthen governance, compliance, and resilience.
- + Management of security incidents, monitoring, and crisis events.
- + Ongoing, day-to-day risk management, continuous improvement and assurance activities.
- + Supplier assurance and third-party risk assessments.
- + Recommendations for risk controls, technologies, and mitigation services.

Benefits

- + Tailored information security risk management aligned to threats and objectives.
- + Pragmatic, cost-effective risk management and remediation maximising return on investment.
- + Independent validation of security posture and risk exposure.
- + Improved incident, breach, and crisis management capabilities.
- + Technique agnostic, prioritised, risk insight supporting informed, risk-based decisions.
- + Clear, detailed, constructive stakeholder risk engagement, explanation and management.
- + Support for regulatory, contractual, and certification requirements.
- + Proactive threat horizon scanning and strategic risk planning.
- + Reduced costs through proportionate, effective risk treatment.
- + Enhanced organisational resilience through specialist risk expertise.

Cyber Security Strategy Design & Implementation



Our Cyber Security Strategy Design & Implementation service provides a practical, cost-effective and proven approach to designing, embedding and refining a winning cyber strategy. With extensive cross-sector experience, our specialists ensure your cyber security strategy is designed to strengthen resilience, support informed risk-based decision-making and align with wider organisational objectives.

Features

- + Cyber security strategy services for specific engagements or organisation-wide programmes.
- + Establish and maintain a robust, sustainable cyber security strategy.
- + Publish and deploy cyber security policies, standards and procedures.
- + Manage cyber security risk, incidents and crisis events effectively.
- + Recommend vendor-agnostic security services and technologies.
- + Assess current technology capabilities and identify improvement options.
- + Design and review technology roadmaps, including technology stack evaluation.
- + Identify digital and technology trends influencing security direction.
- + Identification of obsolesces and implementation of removal roadmap.
- + Develop and deliver cyber security transformation implementation plans.

Benefits

- + Pragmatic, cost-effective support that maximises return on investment.
- + Independent oversight and validation of your cyber security strategy.
- + Enables informed, risk-based decision-making across the organisation.
- + Access to specialist technical skills and resources for continuous improvement.
- + Reduced costs through adoption of appropriate cyber security measures.
- + Effective transfer of cyber strategy knowledge to your organisation.
- + Roadmap implementation for defence, resilience, and Secure by Design.
- + Enhanced capability across IT and cloud services.
- + Increased efficiency, effectiveness and agility of cyber security operations.
- + Continuously improved performance and value from cyber security controls.

i3Secure Data Analytics empowers organisations to turn data into actionable insights. Our Data Analytics service includes requirement capture, use case creation, wireframes, metric definition, model build and testing, predictive analytics, machine learning, and insight sharing – supported by documentation and knowledge transfer to drive smarter decisions and accelerate data transformation.

Features

- + Knowledge transfer
- + Documentation
- + Data connections
- + Data analytics design
- + Data analytics build/test
- + AI
- + Data science
- + Insight
- + Machine learning
- + Predictive analytics

Benefits

- + Gives confidence to business leaders
- + Reduces risk
- + Fast-tracks delivery
- + Augments in-house team
- + Brings data analytics expertise + lessons learnt
- + Brings design expertise + best practice

DevSecOps is one of the high-quality services that i3Secure offers. We provide DevSecOps practitioners at all levels, from lead to support. Our experience spans defence, home affairs, central government, infrastructure and regulated industries, embedding security into DevOps pipelines to accelerate delivery, strengthen resilience and ensure compliant, secure digital operations.

Features

- + Integrate security controls across automated CI/CD delivery pipelines
- + Implement secure-by-design patterns within cloud and hybrid environments
- + Conduct threat modelling and vulnerability detection across services
- + Embed compliance checks and policy-as-code frameworks
- + Automate security testing throughout build, deploy, run phases
- + Provide DevSecOps tooling configuration, optimisation and governance
- + Enable continuous monitoring, observability and incident detection
- + Deliver security-focused engineering practices with development teams
- + Support cultural adoption of secure agile delivery principles
- + Integration of social value, sustainability and low carbon practices

Benefits

- + Reduced risk through continuous security embedded into delivery workflows
- + Faster delivery enabled by automated security testing and controls
- + Stronger resilience via proactive detection and rapid response capabilities
- + Improved compliance with repeatable, audited DevSecOps processes
- + Lower remediation costs through early vulnerability identification
- + Enhanced system integrity using standardised secure-by-design practices
- + Greater stakeholder confidence in secure digital transformation outcomes
- + Reduced operational noise with automated monitoring and alerting
- + Increased organisational maturity in secure cloud-native operations
- + Incorporating social value, sustainability and low carbon practices

Governance, Risk and Compliance Consultancy is i3Secure's core service, providing pragmatic, cost effective support across governance, risk, information security, and data protection. Acting as trusted Security and Risk Management partners, our Governance, Risk and Compliance capability embeds Secure-by-Design principles to manage cyber risk, protect assets, implement ISMS, and achieve compliance and assurance.

Features

- + Enterprise-wide or targeted GRC consultancy aligned to organisational needs/risk appetite.
- + Establishment and operation of integrated GRC frameworks and governance structures.
- + Secure-by-Design (SbD) embedded across processes, technology, and data protection.
- + Cyber, information security, and data protection risk assessments with remediation.
- + Risk assessment delivery, asset registers, CIA analysis, and risk registers.
- + ISMS design, implementation, and ongoing governance management.
- + Development and deployment of GRC, security, and data protection policies/standards.
- + Security Manager and Risk Manager leadership for incidents and crises.
- + Supplier assurance and third-party risk management.
- + Design, Development, implementation, and testing of Business Continuity Disaster Recovery.

Benefits

- + Pragmatic, cost-effective GRC consultancy delivering strong return on investment.
- + Trusted, independent expertise across governance, risk, compliance, and data protection.
- + Clear visibility and independent validation of organisational risk posture.
- + Continuously improved cyber security maturity and reduced incident impact.
- + Actionable risk insight enabling informed, risk-based decision-making.
- + Stronger alignment between business objectives and security controls.
- + Proactive identification of emerging threats through horizon scanning.
- + Defined risk treatment plans delivering measurable risk reduction.
- + Improved regulatory and contractual compliance confidence.
- + Knowledge transfer building a sustainable, resilient security culture.

i3Secure's ISO 9001 Consultancy provides end-to-end support for Quality Management System (QMS) implementation, certification, and continual improvement, including managed service delivery. Our specialist ISO 9001 consultants deliver gap analysis, risk assessment, internal audit assurance, and practical, pragmatic guidance to improve process consistency, service quality, customer satisfaction, and effective quality governance.

Features

- + ISO 9001 scoping, gap analysis, and QMS readiness assessment.
- + Quality Management System (QMS) design, implementation, and certification support.
- + Process mapping, optimisation, and controlled documentation development.
- + Integration of risk-based thinking and quality risk assessment.
- + Development of quality policies, objectives, KPIs, and performance measures.
- + Internal audit planning, delivery, and corrective action management.
- + Supplier quality management and third-party assurance.
- + Management review facilitation and continual improvement planning.
- + Integration with ISO 27001, ISO 22301, and governance frameworks.
- + Managed QMS services and ongoing quality advisory support.

Benefits

- + Improved service quality, consistency, and customer satisfaction.
- + Compliance with ISO 9001 and recognised quality management standards.
- + Reduced rework, inefficiency, and operational risk.
- + Clear, repeatable processes supporting scalable and sustainable growth.
- + Enhanced governance, accountability, and management oversight.
- + Improved supplier performance and quality assurance.
- + Risk-based decision-making embedded into day-to-day operations.
- + Cost savings through targeted process optimisation and continual improvement.
- + Increased customer, partner, and regulator confidence.
- + Access to specialist ISO 9001 and quality management expertise.

i3Secure's ISO 22301 Consultancy delivers comprehensive support for Business Continuity Management System implementation, certification, and optimisation. Our ISO 22301 specialists provide gap analysis, risk assessment, internal audit assurance, and best-practice guidance to help organisations identify critical services, manage operational risk, and strengthen resilience through effective continuity, crisis, and disaster-recovery planning.

Features

- + ISO 22301 scoping, gap analysis, and BCMS readiness assessment.
- + Business Impact Analysis (BIA) and operational risk assessment facilitation.
- + Business Continuity Management System (BCMS) design and certification support.
- + Development of business continuity, disaster recovery, and crisis management plans.
- + Integration with cyber security, IT resilience, and enterprise risk management.
- + Defining recovery time objectives (RTO) and recovery point objectives (RPO).
- + Continuity strategy development for people, facilities, suppliers, and technology.
- + Exercising, testing, and validation of continuity arrangements.
- + Internal audit, management review, and continual improvement support.
- + Managed BCMS services and ongoing assurance.

Benefits

- + Improved organisational resilience and business continuity capability.
- + Reduced operational disruption, downtime, and financial impact of incidents.
- + Compliance with ISO 22301 and regulatory resilience requirements.
- + Clear understanding of critical activities, dependencies, and vulnerabilities.
- + Faster recovery from cyber incidents, outages, and supply chain disruption.
- + Enhanced crisis management, decision-making, and leadership confidence.
- + Protection of reputation, customers, and critical services.
- + Cost-effective, risk-based investment in continuity and resilience.
- + Increased stakeholder, customer, and regulator confidence.
- + Access to specialist business continuity and resilience expertise.

i3Secure's ISO 22301 Consultancy delivers comprehensive support for Business Continuity Management System implementation, certification, and optimisation. Our ISO 22301 specialists provide gap analysis, risk assessment, internal audit assurance, and best-practice guidance to help organisations identify critical services, manage operational risk, and strengthen resilience through effective continuity, crisis, and disaster-recovery planning.

Features

- + ISO 22301 scoping, gap analysis, and BCMS readiness assessment.
- + Business Impact Analysis (BIA) and operational risk assessment facilitation.
- + Business Continuity Management System (BCMS) design and certification support.
- + Development of business continuity, disaster recovery, and crisis management plans.
- + Integration with cyber security, IT resilience, and enterprise risk management.
- + Defining recovery time objectives (RTO) and recovery point objectives (RPO).
- + Continuity strategy development for people, facilities, suppliers, and technology.
- + Exercising, testing, and validation of continuity arrangements.
- + Internal audit, management review, and continual improvement support.
- + Managed BCMS services and ongoing assurance.

Benefits

- + Improved organisational resilience and business continuity capability.
- + Reduced operational disruption, downtime, and financial impact of incidents.
- + Compliance with ISO 22301 and regulatory resilience requirements.
- + Clear understanding of critical activities, dependencies, and vulnerabilities.
- + Faster recovery from cyber incidents, outages, and supply chain disruption.
- + Enhanced crisis management, decision-making, and leadership confidence.
- + Protection of reputation, customers, and critical services.
- + Cost-effective, risk-based investment in continuity and resilience.
- + Increased stakeholder, customer, and regulator confidence.
- + Access to specialist business continuity and resilience expertise.

i3Secure's ISO 27001 Consultancy provides end-to-end support for Information Security Management System (ISMS) implementation, certification, and managed services. Our expert ISO 27001 consultants deliver gap analysis, risk assessment, internal audit assurance, and practical best-practice guidance, helping organisations achieve, maintain, and continually improve ISO 27001 compliance and effective information security governance.

Features

- + ISO 27001 and ISMS scoping and boundary definition.
- + ISMS design, implementation, and certification support.
- + ISO 27001 advisory services and best-practice guidance.
- + ISMS gap analysis and maturity assessment against ISO 27001.
- + Information security risk assessment and risk management.
- + Internal audit and assurance services.
- + Remediation planning with prioritised improvement actions.
- + ISMS policy, procedure, and documentation development.
- + ISO 27001 managed service delivery.
- + Project management and external audit support.

Benefits

- + Pragmatic, cost-effective ISO 27001 consultancy maximising return on investment.
- + Trusted, independent assurance from qualified ISO 27001 Lead Auditors/Implementers.
- + Improved cyber resilience through robust information security governance.
- + ISMS aligned with organisational strategy and risk appetite.
- + Efficient, prioritised implementation across cloud and on-premises environments.
- + Clear roadmap for achieving and maintaining ISO 27001 certification.
- + Informed security investment and certification planning decisions.
- + Optimised certification scope balancing risk, cost, and operational impact.
- + Fully tailored ISMS policies, procedures, and documentation.
- + Reduced security risk through effective, proportionate controls.

i3Secure's ISO 27701 Consultancy provides implementation and certification support for establishing, maintaining, and continually improving a Privacy Information Management System (PIMS). Our expert ISO 27701 consultants deliver gap analysis, risk assessment, internal audit assurance, best-practice guidance, and managed services, helping organisations achieve effective privacy governance and ongoing compliance.

Features

- + ISO 27701 scoping and Privacy Information Management System boundary definition.
- + Interpretation of ISO 27701 requirements, terms, and controls.
- + Organisational context, stakeholder, and privacy obligation assessment.
- + Privacy governance, leadership, and accountability alignment.
- + Privacy risk assessment and planning aligned to regulatory needs.
- + Competence, awareness, and operational support processes.
- + Integration of privacy controls into business operations.
- + Performance monitoring, measurement, and internal audit support.
- + Continuous improvement of the Privacy Information Management System (PIMS).
- + Advisory and implementation support for ISO 27701 certification.

Benefits

- + Pragmatic, cost-effective ISO 27701 consultancy delivering maximum ROI.
- + Trusted privacy expertise from ISO 27701 qualified consultants.
- + Reduced operational and compliance costs through effective information governance.
- + Enhanced protection of personal and sensitive data.
- + Structured support for ISO 27701 certification planning and delivery.
- + Improved third-party trust, assurance, and organisational reputation.
- + Reduced complexity through practical, proportionate privacy controls.
- + Clear pathway to achieving and sustaining privacy compliance.
- + Fully customised ISO 27701 policies and documentation.
- + Lower privacy risk through timely, effective remediation.

i3Secure's ISO 42001 Consultancy delivers end-to-end support for Artificial Intelligence Management System (AIMS) implementation, certification, and ongoing managed services. Our expert ISO 42001 consultants provide gap analysis, risk/impact assessment, internal audit assurance, governance design, and best-practice guidance, helping organisations deploy trustworthy, ethical, and compliant AI aligned with ISO 42001 requirements.

Features

- + ISO 42001 AIMS scoping and readiness assessment.
- + Artificial Intelligence Management System (AIMS) implementation and certification consultancy.
- + AI risk, impact, and ethical assessment.
- + AI governance, accountability, and policy framework development.
- + Alignment with legal, regulatory, and organisational AI requirements.
- + AI lifecycle controls covering design, development, deployment, and monitoring.
- + Gap analysis against ISO 42001 requirements.
- + Internal audit and assurance support.
- + Performance evaluation and continual improvement of AI systems.
- + Managed AIMS services and ongoing advisory support.

Benefits

- + Enables trustworthy, ethical, and responsible use of artificial intelligence.
- + Supports compliance with ISO 42001 and emerging AI regulations.
- + Reduced AI-related legal, operational, and reputational risk.
- + Stronger governance, accountability, and oversight of AI systems.
- + Improved transparency, traceability, and explainability of AI decisions.
- + Increased confidence from customers, regulators, and stakeholders.
- + AI risk management embedded into organisational strategy and operations.
- + Supports scalable, sustainable, and responsible AI innovation.
- + Independent assurance from specialist AI governance experts.
- + Continuous improvement across the AI lifecycle.

JSP 453 Service Transition Officers



Our JSP 453 Service Transition Officers liaise with the Network Operating Authority, assessing capabilities and guiding programmes through migration/integration onto the MOD Core Network. Throughout the JSP 453 service transition lifecycle, they manage evidence, support Authority to Test/Operate submissions, and present applications to approval boards, ensuring secure, authorised network connectivity.

Features

- + Provision of experienced Service Transition Officers.
- + Focused or enterprise-wide digital transition assessments, including managed service delivery.
- + Alignment of transition activities with JSP 453/604 requirements.
- + Liaison and consultancy between capabilities, control/rule owners and the DEAB.
- + Assessment of capabilities preparing for migration/connection to MOD Core Network.
- + Management, tracking, and closure of corrective actions and transition issues.
- + Development and assurance of evidence for Authority-to-Test through to Authority-to-Operate.
- + Unrivalled experience of Continuous Authority to Operate (CATO).
- + Assurance of legacy JSP 604 compliance across third-party/supplier environments.
- + Delivery by JSP 453/604 specialists supporting secure, authorised integration.

Benefits

- + Trusted Service Transition Officers with deep JSP 453/604 expertise.
- + Tailored digital transition support aligned to organisational and programme needs.
- + Improved understanding of JSP 453/604 requirements and MOD network obligations.
- + Independent assurance that third-party/supplier controls meet JSP 453/604 standards.
- + Clear mitigation plans addressing identified gaps and transition risks.
- + Demonstrable compliance with JSP 453/604 and related defence security standards.
- + Support for achieving required MOD approvals and certifications.
- + Protection of business, classified, and customer information and assets.
- + Effective knowledge transfer building internal transition capability.
- + Reduced risk and increased confidence connecting to MOD Core Network.

NCSC Cyber Security Framework (CAF) Consultancy



i3Secure's Cyber Assessment Framework (CAF) Consultancy supports organisations in assessing, improving, and demonstrating cyber resilience against the NCSC CAF and DSPT requirements. Our specialist Cyber Assessment Framework consultants deliver structured gap analysis, risk-based prioritisation, remediation planning, and assurance, helping organisations strengthen essential services, meet regulatory expectations, and improve cybersecurity maturity.

Features

- + NCSC CAF and DSPT scoping and readiness assessment.
- + CAF- and DSPT-aligned maturity and gap assessment with evidence review.
- + Risk-based analysis of threats, vulnerabilities, and business impact.
- + Review of governance, leadership, accountability, and cyber risk management.
- + Assessment of protective security controls and cyber hygiene.
- + Evaluation of identity and access management, data-protection, and asset management.
- + Review of monitoring, detection, and incident response capabilities.
- + Assessment of recovery, resilience, and business continuity capability.
- + Prioritised remediation roadmap aligned to CAF outcomes.
- + Independent assurance, executive reporting, and ongoing advisory support.

Benefits

- + Improved cyber resilience aligned to NCSC CAF and DSPT requirements.
- + Clear visibility of cyber security maturity and risk exposure.
- + Reduced likelihood, impact, and recovery time from cyber incidents.
- + Stronger governance, accountability, and ownership of cyber risk.
- + Increased regulatory assurance and stakeholder confidence.
- + Improved protection of essential services and critical systems.
- + Risk-based prioritisation of cyber security investment.
- + Enhanced detection, response, and recovery capabilities.
- + Cost-effective improvement planning focused on highest-risk areas.
- + Access to specialist CAF, DSPT, and regulatory cyber expertise.

Penetration Testing & Vulnerability Services



i3Secure delivers independent Penetration Testing and Vulnerability Assessments, identifying, remediating, and managing risk across applications, infrastructure, and information systems. Our vulnerability assessments complement expert penetration testing by CREST and CHECK certified specialists, combining deep industry experience and HMG aligned qualifications to deliver robust, repeatable, and reliable security assurance.

Features

- + Ad-hoc/routine penetration testing services providing assurance on new/existing IT assets.
- + Support your IT Health Check (ITHC) requirements.
- + Web application and mobile device testing services.
- + Cloud services security reviews and assessments.
- + External vulnerability scanning services.
- + PCI DSS Approved Scan Vendor (ASV) scanning
- + Testing to meet HMG standards.
- + Internal network and Wi-Fi testing services.
- + Clear penetration testing reports enabling pragmatic risk-based decisions.
- + Detailed penetration test scoping and full post-test remediation support.

Benefits

- + Penetration testing specialists with deep industry expertise.
- + Provision of independent oversight and validation of IT security posture.
- + Penetration testing enabling accurate and informed risk-based decision making.
- + Facilitates effective management of data breaches and IT security incidents.
- + Post-test support and plans for effective remediation plans
- + Realise and reduce your attack vectors and attack surface.
- + Penetration testing delivered to recognised industry standards/certifications (CREST/CHECK).
- + Our penetration testers hold a high National Security Vetting standard.
- + Increase in service up-time through pro-active prevention and detection.
- + Increased quality assurance through regular penetration testing.

Expert Product Management services to define product vision, strategy, and roadmap aligned with organisational goals. Our specialists lead cross-functional teams, prioritise features, and ensure stakeholder engagement throughout the agile lifecycle. Proven success across government, defence, and infrastructure projects delivers measurable outcomes and accelerated delivery under our Product Managers.

Features

- + Prioritise customer needs via market research, interviews, and usability testing
- + Align product vision, strategy with market opportunities for success
- + Define compelling product vision, strategy aligned with business objectives
- + We develop product roadmap with key milestones and deliverables
- + We develop a product roadmap to achieve the product vision
- + We collaborate with cross-functional teams for successful product launch
- + Continuously monitor and analyse product performance and gather feedback
- + Continuously leverage insights to drive product improvements and iterations
- + Integration of social value, sustainability and low carbon practices

Benefits

- + Clear and compelling product visions aligned with business objectives
- + Clear and compelling product visions aligned with user needs
- + Conduct market analyses, identifying opportunities for informed decision-making
- + Cross-functional Collaboration: Coordinating teams, fostering effective communication and alignment
- + Create structured roadmaps that balance goals with long-term objectives
- + Prioritise understanding and addressing customer needs, maximising product adoption
- + Using Product Ownership skills to guide product development
- + Leverage data to inform product strategy for positive outcomes
- + Share best practices with organisations, improving agile maturity
- + Incorporating social value, sustainability and low carbon practices

Programme & Technical Assurance Support



Our Programme and Technical Assurance Support provides expert leadership across delivery, security, and controls. Acting as Programme Technical Lead and Security Officer, we oversee technical execution, embed robust security controls, manage risk, conduct audits, assure compliance, and apply best-in-class project controls insight to strengthen programme, project, and portfolio outcomes.

Features

- + Technical planning, architecture, and design assurance across programmes and projects.
- + Delivery Management providing Programme Technical direction and delivery oversight.
- + Integrated security controls embedded throughout programme and project SDLCs.
- + Comprehensive risk management identifying vulnerabilities and mitigating threats.
- + Quality assurance through audits, assessments, and control validation.
- + Incident response planning, threat monitoring, and real-time security management.
- + Regulatory, contractual, and standards compliance assurance.
- + Strong stakeholder communication and cross-team collaboration.
- + Continuous improvement of technical and security controls.
- + Delivery by accredited professionals in Agile, Prince2, MoR, and PP&C.

Benefits

- + Programme outcomes realised, major projects delivered to budget, risks minimised
- + Improved technical and risk-based decision-making through independent assurance.
- + Reduced delivery, security, and compliance risks across programmes and projects.
- + Higher quality, secure deliverables protecting critical assets and information.
- + Enhanced productivity using Primavera P6, MS Project, ARM, Unifier, Tableau.
- + Effective communication enabled by clear reporting, artefacts, and governance structures.
- + Cost-effective assurance delivering measurable return on investment.
- + Improved adaptability, innovation, and resilience to emerging threats.
- + Stronger security awareness and compliance culture within delivery teams.
- + Effective management of incidents, data breaches, and regulatory obligations.

Programme Management is one of the high-quality services that i3Secure offers. We provide Programme Management at all levels, from lead to support. Our experience of Programme Management and capability knowledge has been demonstrated across defence, home affairs, central government, infrastructure and local organisations.

Features

- + Experienced and proven programme management and leadership
- + Quality programme level business cases, business planning and strategic alignment
- + Programme planning and scheduling using proven approaches
- + Programme management of risks, assumptions, issues, dependencies and opportunities
- + Transformation and change management delivery
- + Programme management capability building and upskilling
- + Benefits management and realisation support with programme management
- + Reporting, dashboards, metrics and strategic insight support
- + Programme management provides intelligent customer support
- + Integration of social value, sustainability and low carbon practices

Benefits

- + Programme management that quickly embeds cost reduction and improved efficiency
- + Ability to design methodology to best suit your business environment
- + Fully realised, quantifiable, reportable benefits using Programme Management best practice
- + Effective client team development via knowledge management
- + Improved process control and maturity by improved programme management
- + Ability to operate in fully controlled project environment
- + Accurate understanding of project status with Programme Management
- + Enhanced business performance and organisational success
- + Programme Management provides effective stakeholder community engagement
- + Incorporating social value, sustainability and low carbon practices

Programme Management

Project Management is one of the high-quality services that i3Works offers. We provide Project Management at all levels, from lead to support. Our experience of Project Management and capability knowledge has been demonstrated across defence, home affairs, central government, infrastructure and local organisations.

Features

- + Project management and leadership using agile, waterfall and hybrid methodologies
- + Investment appraisals, business cases, business planning and strategic alignment
- + Schedule development including critical paths, 3 point-estimates and dependencies
- + Risk management, assumption documentation and project control implementation
- + Transformation, change management and change control utilising best practice techniques
- + Benefits management and realisation with Project management
- + Reporting, dashboards, metrics and strategic insight
- + Intelligent customer support with Project management
- + Project handover management, mentoring and coaching
- + Integration of social value, sustainability and low carbon practices

Benefits

- + Quickly embedded cost reduction and efficiency improvements with Project Management
- + Provides the ability to design methodology to suit environment
- + Fully realised, quantifiable and reportable benefits with Project Management
- + Project Management provides improved process control and maturity
- + Ability to operate in fully controlled project environments
- + Accurate understanding of project status with Project Management
- + Enhanced business performance and organisational success
- + Project Management offers effective stakeholder community engagement
- + Soft landing project transition back to client with Project Management
- + Incorporating social value, sustainability and low carbon practices

i3Secure's Resilience by Design service embeds resilience into systems, infrastructure, and policies, strengthening your organisation's preparedness to withstand, adapt to, and recover from disruption. Through a Resilience by Design approach, our consultants address natural hazards and human made threats, including cyber-attacks, pandemics, and economic shocks, ensuring sustainable, long-term operational continuity.

Features

- + Technical planning, architecture, and design assurance across programmes and projects.
- + Identification of critical assets and site-specific risk evaluation.
- + Integrated security controls embedded throughout programme and project SDLCs.
- + Comprehensive risk management identifying vulnerabilities and mitigating threats.
- + Incident response planning, threat monitoring, and real-time security management.
- + Design, Development, implementation, and testing of Business Continuity Disaster Recovery.
- + Conduct architecture assessments, gap analysis, and infrastructure evaluations.
- + Tailored attack playbooks and testing for diverse scenarios.
- + Redundancy, fail-over, hot/warm/cold-site, and data back-up readiness evaluations.
- + Continuous learning, improvement and adaptation to controls and processes.

Benefits

- + Reduced delivery, security, and compliance risks across programmes and projects.
- + Protection of business, classified, and customer information and assets.
- + Reduced likelihood, impact, and recovery time from cyber incidents.
- + Improved protection of essential services, critical systems, and data.
- + Improved incident, breach, and crisis management capabilities.
- + Continuously improved cyber security maturity and reduced incident impact.
- + Improved incident response and resilience supporting business continuity.
- + Reduction of down-time in the event of an incident.
- + Effective, tailored, and tested incident playbooks.
- + SC/DV vetted personnel with experience across OFFICIAL, SECRET, TOP SECRET

Site Co-ordinating Infrastructure Design Authority (SCIDA) Services



i3Secure's Site Co-ordinating Infrastructure Design Authority (SCIDA) Services provides oversight, authority and assurance for critical MoD ICT and communications infrastructure. Our SCIDA specialists assess, coordinate, and govern protective security measures across client/supplier sites, identifying critical assets, evaluating risk, and defining proportionate, cost-effective controls aligned to JSP440 and government security expectations.

Features

- + SCIDA-led site and infrastructure security assessments and audits.
- + Focused or enterprise-wide reviews, including managed SCIDA services.
- + Identification of critical assets and site-specific risk evaluation.
- + Design authority oversight of protective security solutions.
- + Alignment with JSP 440 and government security requirements.
- + Corrective action planning, tracking, and governance.
- + Security assurance by SC/DV cleared personnel across supplier sites.
- + Development of SCIDA Policy, and secure control/technical documentation
- + Security awareness, training and guidance addressing identified design gaps.
- + Expertise spanning ISO27001, CISM, DCNI, BCI, PCI DSS, and JSP440.

Benefits

- + Independent design authority assuring consistent site security outcomes.
- + Reduced physical and infrastructure security risk across estates.
- + Proportionate, cost-effective security aligned to operational needs.
- + Improved assurance over third-party and supplier site security.
- + Clear remediation plans for identified infrastructure vulnerabilities.
- + Demonstrable compliance with JSP 440 and related standards.
- + Protection of people, facilities, information, and critical assets.
- + Compliance with government, organisational, security and safety accreditation/requirements.
- + Effective knowledge transfer and awareness to internal security/estates teams.
- + Access to SC/DV specialists with extensive SCIDA experience.

Secure by Design Awareness, Behaviour & Culture



i3Secure's Secure by Design Awareness, Behaviour & Culture service helps organisations build a security- and privacy-conscious workforce. We embed Secure by Design awareness and thinking into everyday behaviours, decision-making, and leadership culture, reducing human risk, strengthening GDPR accountability, and ensuring security and data protection become a shared organisational responsibility.

Features

- + Secure by Design awareness programmes tailored to organisational roles.
- + Privacy by Design and GDPR accountability awareness campaigns.
- + Behavioural risk assessment targeting human and process vulnerabilities.
- + Security culture maturity assessment and benchmarking.
- + Leadership and management engagement workshops.
- + Human-centric security and data protection messaging.
- + Integration of security behaviours into policies and ways of working.
- + Targeted awareness for cloud, data handling, and secure design practices.
- + Ongoing reinforcement through communications and micro-learning.
- + Measurement of behavioural change and cultural improvement.

Benefits

- + Embeds Secure by Design thinking and awareness across the organisation.
- + Reduces human-related security and data protection risks.
- + Improves compliance and maturity through accountable behaviours.
- + Strengthens organisational security and privacy culture.
- + Increases leadership ownership of security and data protection.
- + Improves consistency of secure decision-making.
- + Lowers likelihood of data breaches caused by human error.
- + Supports continuous improvement through sustainable, long-term behaviour change.
- + Enhances trust with customers, partners, and regulators.
- + Cost-effective improvement of organisational resilience.

i3Secure's Secure by Design Consultancy service embeds cybersecurity and data protection into systems, processes, and technologies from inception through operation. Our specialist Secure by Design consultants help organisations meet GDPR accountability and data protection by design requirements, reducing risk, strengthening governance, and ensuring privacy, security, and resilience are built in.

Features

- + Secure by Design and Privacy by Design maturity and gap assessments.
- + Secure SDLC and DevSecOps integration.
- + GDPR compliance, accountability, and assurance support.
- + Secure cloud, hybrid, and on-premises architecture design guidance.
- + Privacy risk assessment, DPIA support, and threat modelling.
- + Security, privacy, and data protection policy development.
- + Definition of appropriate technical and organisational measures (TOMs).
- + Recommendation of privacy-enhancing technologies and security controls.
- + Governance across design, build, deployment, and operations.

Benefits

- + Access to trusted Secure by Design, GDPR, and cybersecurity specialists.
- + Reduced GDPR compliance risk and regulatory enforcement exposure.
- + Stronger protection of personal data across cloud, hybrid, and on-premises.
- + Lower likelihood and impact of data breaches and privacy incidents.
- + Practical, scalable compliance aligned to business objectives.
- + Clear visibility of security and privacy risks supporting informed decisions.
- + Improved security, privacy, and data governance maturity.
- + Cost savings through proportionate, risk-based security controls.
- + Enables secure digital transformation and cloud adoption.
- + Demonstrable accountability, effective knowledge transfer, and strengthened stakeholder trust.

i3Secure's Secure by Design Training equips organisations with the skills and knowledge to embed cyber security and risk management into everyday decision-making. Our practical, experience-based Secure by Design training enables teams to embed Secure by Design principles, reduce risk, and deliver secure, compliant systems throughout the lifecycle.

Features

- + Role-based Secure by Design and Privacy by Design training.
- + Targeted awareness for cloud, data handling, and secure design practices.
- + Leadership and management engagement workshops.
- + Human-centric security and data protection messaging.
- + Integration of security behaviours into policies and ways of working.
- + Secure architecture and security-by-default design fundamentals.
- + Practical guidance on technical and organisational measures.
- + Policy, governance, and accountability training for leaders.
- + Real-world case studies, scenarios, and exercises.
- + Tailored delivery for technical, legal, and business audiences.

Benefits

- + Builds in-house Secure by Design and GDPR expertise.
- + Reduces reliance on external consultants over time.
- + Improves data protection and cyber security awareness.
- + Lowers risk of data breaches and compliance failures.
- + Enables consistent, secure design decisions across teams.
- + Supports secure cloud adoption and digital transformation.
- + Strengthens organisational accountability and governance.
- + Improves collaboration between technical, legal, and business teams.
- + Practical skills directly applicable to real projects.
- + Cost-effective upskilling aligned to regulatory expectations.

Security Assurance as a Service



i3Secure's Security Assurance as a Service provides SQEP Security Assurance Coordinators and Security Managers delivering security assurance and accreditation consultancy to MoD Defence Digital, StratCom, DE&S, Royal Navy, Army, and RAF. It embeds Secure by Design and applies NIST 800, ISO27001, HMG Security Standards, NCSC guidance, and MOD JSP 440/604/453.

Features

- + Security Assurance Coordinators and Security Managers leading end-to-end security assurance.
- + Technical security documentation coordination to support CyDR and accreditation bodies.
- + Extensive experience with JSP 440/604/453, working closely with Accreditors/Case Officers.
- + Risk Management and Accreditation Document Set development, assurance and management.
- + Technical Design Reviews, Test Security Instructions and Security Impact Assessments.
- + IT Health Check scoping, coordination, delivery and remedial action planning.
- + Security assurance and management for Data Protection Impact Assessments (DPIA).
- + Development, delivery and assurance of Operational Security Management Plans (OSMP).
- + Security assurance support for audits, operations, incident management and response.
- + NIST 800 Series security implementation, guidance, assurance and testing.

Benefits

- + Access to trusted, certified Security Assurance Coordinators and Security Managers.
- + Security assurance coordination ensuring consistent implementation of informed, risk-based decisions.
- + Delivery of clear, concise, high-quality security artefacts and accreditation documentation.
- + In-depth risk assessments allowing organisations to make informed decisions.
- + Reduced security risk through effectively coordinating assurance activities and assessments.
- + Access to specialist technical skills/resources to support continuous security improvement.
- + Security managers providing informed, risk-based analysis aligned to organisational objectives.
- + SC/DV expertise across all security frameworks including NIST and ISO/IEC 27001.
- + Timely completion of mandatory security documentation to avoid project delays.
- + Strong leadership to integrate assurance activities seamlessly into delivery programmes.

Solution Architecture is one of the high-quality services that i3Secure offers. We provide Solution Architecture practitioners at all levels, from lead to support. Our expertise spans defence, home affairs, central government, infrastructure and local organisations, delivering robust solution designs aligned to organisational strategy, technology standards and business outcomes.

Features

- + Define solution architecture aligned with business goals and constraints
- + Assess technology options ensuring scalability, security and performance
- + Produce end-to-end solution designs across applications, data and infrastructure
- + Validate requirements against architecture principles and delivery feasibility
- + Provide architectural governance ensuring compliance with standards
- + Support technical teams with detailed design and integration guidance
- + Identify risks, dependencies, and mitigation across solution components
- + Engage stakeholders to align expectations and architectural decisions
- + Ensure roadmap alignment with enterprise and cloud strategies
- + Integration of social value, sustainability and low carbon practices

Benefits

- + Clear architectural direction reducing delivery risk and uncertainty
- + Improved alignment between business goals and technical implementation
- + Optimised performance through well-designed, scalable solution architectures
- + Enhanced decision-making supported by structured architectural analysis
- + Better integration across systems through consistent architecture standards
- + Reduced technical debt with future-proof architectural principles
- + Increased delivery confidence via governance and design assurance
- + Faster project mobilisation through well-defined architectural foundations
- + Strengthened organisational resilience through secure architectural patterns
- + Incorporating social value, sustainability and low carbon practices

i3Secure's Supply Chain Assurance service helps organisations manage cyber security and data protection risk across suppliers and partners. Through our Supply Chain Assurance approach, aligned to CSM Model 4 and DCC Defence Cyber Certification, we assess, assure, and strengthen third party security, supporting regulatory compliance, defence requirements, and resilient supply chains.

Features

- + Supply chain cyber security and third-party risk assessments.
- + Assurance aligned to CSM Model 4 and defence sector expectations.
- + Support for DCC Defence Cyber Certification readiness and evidence.
- + Supplier due diligence, onboarding, and security assurance reviews.
- + GDPR and data protection compliance assessments for third parties.
- + Contractual security controls and assurance requirements definition.
- + Supplier risk profiling, criticality analysis, and prioritisation.
- + Continuous monitoring of supplier security posture.
- + Supply chain incident response and breach management support.
- + Governance frameworks and executive assurance reporting.

Benefits

- + Reduced cyber and data protection risk across the supply chain.
- + Improved compliance with CSM Model 4 and defence cyber standards.
- + Stronger readiness for DCC Defence Cyber Certification.
- + Enhanced visibility of supplier security posture and risks.
- + Reduced likelihood and impact of supply chain cyber incidents.
- + Improved regulatory, customer, and defence stakeholder confidence.
- + Risk-based prioritisation of supplier assurance activities.
- + Stronger contractual and governance control over third parties.
- + Cost-effective management of complex supplier ecosystems.
- + Access to specialist defence and supply chain cyber expertise.

Empowering Digital Resilience Since 2021

Who We Are

i3Secure Ltd is a UK-based cyber security and information assurance consultancy protecting the confidentiality, integrity and availability of data across defence, public and private sectors.

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

As a trusted partner to highly regulated clients including the NHS and Ministry of Defence, we deliver clear, fit-for-purpose solutions to manage cyber risk, meet compliance obligations, and safeguard critical assets.

Our services include:

- + **Cyber Security Architecture & Design**
- + **Cloud & DevSecOps**
- + **Cyber Security Strategy & Leadership**
- + **Governance, Risk & Compliance**
- + **ISO Management Systems Consultancy**
- + **Cyber Essentials & Cyber Essentials Plus Consultancy**
- + **Security Assurance & Testing**
- + **Secure by Design Delivery & Training**
- + **Programme, Project & Business Services**
- + **Business Transformation & Programme Delivery (i3Works)**

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

Our Vision

i3Secure is committed to delivering flexible, reliable and competitive cyber security consultancy that protects critical services and enables confident transformation. We strive to work seamlessly alongside our clients to address complex security challenges, providing trusted assurance and long-term value so organisations can operate securely, compliantly and with confidence.

Forward thinking

The cyber threat sector is evolving, and so are we. Our future strategy focuses on:

- + Secure-by-design and resilient architectures to protect critical services
- + Proactive cyber security, risk management and regulatory assurance
- + Cloud, data and AI security to enable safe digital transformation
- + Threat-led insight, testing and assurance to support informed decision-making
- + Building cyber capability, awareness and culture to strengthen organisational resilience

By embracing our priorities, i3Secure 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 i3Secure can help your organisation achieve its strategic goals.

Visit: <https://i3secure.co.uk>

Email: info@i3secure.co.uk

