Service Definition Document

SOC Analyst

We Are **i3Secure,** Your Trusted Cyber Security Partner.

i3Secure is a trusted supplier to the Ministry of Defence and the wider Defence Supply Chain, along with the National Health Service (NHS) and local government. We have extensive industry knowledge in Cyber Security, Information Assurance and Data Protection, generated from supporting a diverse customer base.

We have maintained a proven track record in serving the comprehensive needs of our clients, whilst providing value for money.

Our approach to delivery is centred on reliability, flexibility, and leading expertise. We use only the best people, highly personable, qualified, and experienced, enabling us to exceed customer expectations, time and time again.

Understanding our clients needs and expectations is very important to us. We recognise that our clients have unique challenges, and therefore generic and inflexible approaches do not suffice.

Jason McAdam,
Co-Founder and Director

CYBER ESSENTIALS CERTIFIED PLUS

HM Government G-Cloud Supplier

NET ZERO 2030

nqa ISO 27001 INFORMATION SECURITY MANAGEMENT UKAS MANAGEMENT SYSTEMS 0015

Chartered Institute of Information Security

info@i3secure.co.uk

Contents

Service Description

SOC Analyst

Our SOC analysts monitor, detect, investigate, and respond to cybersecurity threats and incidents. They expertly manage security tools, stay updated on threats, and contribute to improving the organisation's security posture.

Features

- Technical Expertise: Proficiency in using security tools and technologies such as SIEM, IDS/IPS, firewalls, and endpoint security solutions.
- Analytical Skills: Ability to analyse large volumes of data to identify patterns, anomalies, and potential security threats.
- Problem-Solving Abilities: Aptitude for investigating security incidents, troubleshooting issues, and devising effective solutions.
- Attention to Detail: Thoroughness in monitoring and analysing security alerts to ensure nothing is overlooked.
- Communication Skills: Capability to convey technical information clearly and concisely, both orally and in writing, to various stakeholders.
- Adaptability: Flexibility to adapt to evolving threats, technologies, and organisational needs.

Benefits

- Enhanced Security Posture: SOC analysts help in proactively monitoring, detecting, and responding to cybersecurity threats.
- Improved Incident Response: With dedicated SOC analysts, organisations can respond to security incidents more efficiently and effectively, minimizing the impact and potential damage caused by cyberattacks.
- Reduced Downtime: Timely detection and response to security incidents can help reduce downtime caused by system outages or data breaches, ensuring business continuity and minimizing financial losses.
- Compliance Adherence: SOC analysts help organizations meet regulatory compliance requirements by implementing security controls, monitoring systems for compliance violations, and generating audit reports.
- escalate into major incidents, reducing the likelihood of data breaches or other security incidents.

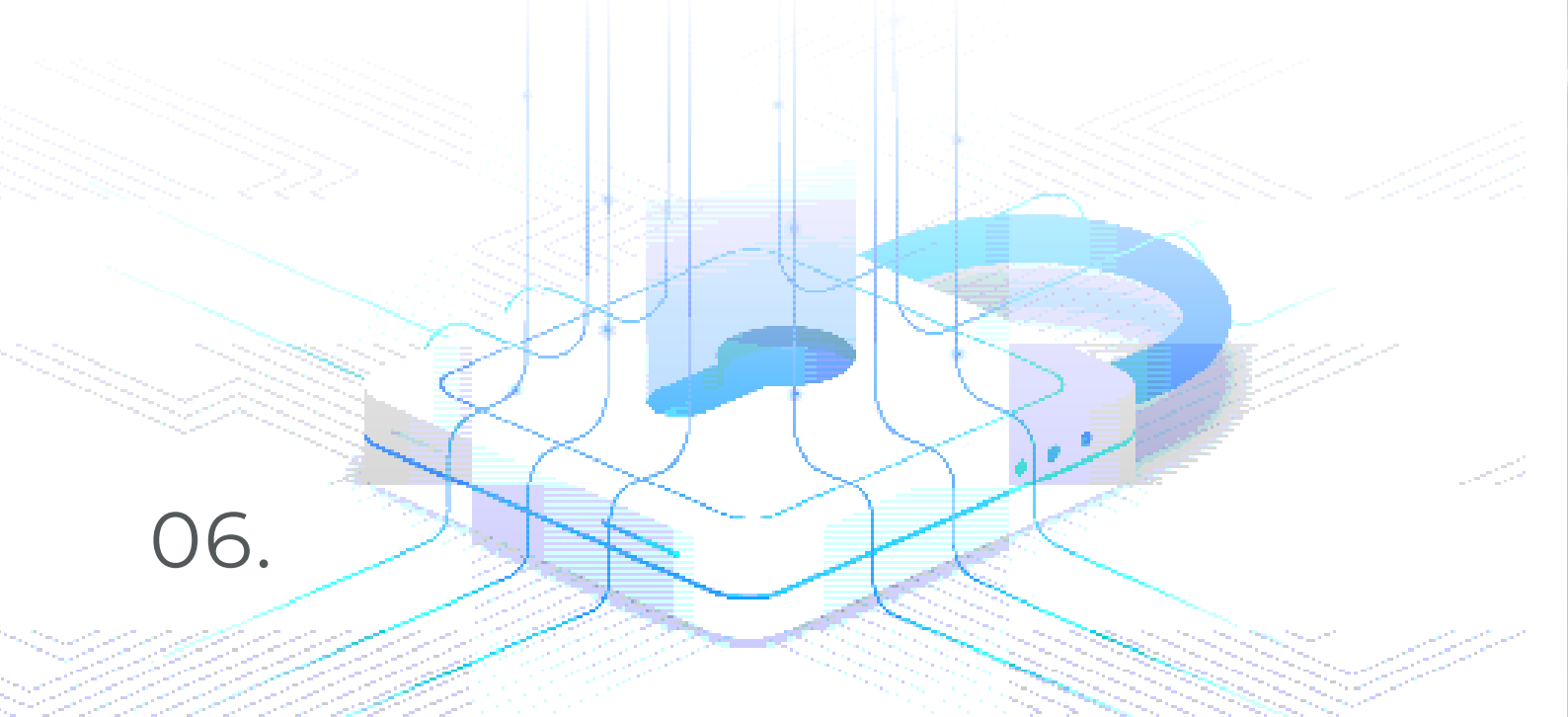
Other Services on G-Cloud

Services

- Information Assurance
- Accrediattion
- Security Architecture
- Cyber Security
- JSP 604 JSP 440
- Pen Testing
- Data Protection
- ISO 27001
- ISO 27701
- ISO 22301
- Incident Management
- Business Continuity
- Risk Management
- Cloud Security
- Physical Security
- Cyber Resilience
- Project Management
- Project Support

Rate Card

	Strategy & Architecture	Change & Transformation	Development & Implementation	Delivery and Operation	People & Skills	Relationships & Engagement
Follow	£460	£440	£440	£440	£440	£440
Assist	£630	£600	£600	£600	£600	£600
Apply	£800	£770	£770	£770	£770	£770
Enable	£900	£875	£875	£875	£875	£875
Ensure / Advise	£1000	£975	£975	£975	£975	£975
Initiate / Influence	£1250	£1200	£1200	£1200	£1200	£1200
Set Strategy / Inpsire/ Mobilise	£1350	£1300	£1300	£1300	£1300	£1300



Standards for Consultancy Day Rate Cards

Consultant's Working Day
8 hours exclusive of travel and lunch.

Working Week
Monday to Friday excluding national holidays.

Office Hours
09:00 h – 17:00 h Monday to Friday.

Travel and Subsistence
Payable at department's standard T&S rates.

Mileage
Payable at department's standard T&S rates.

Professional Indemnity Insurance

Included in day rate.

Volume Discounts

Volume Discounts
Considered on an engagement by engagement basis

Note: Rates are exclusive of VAT which will be charged at the prevailing rate.

Our Client Portfolio

"The i3Secure consultant responsible for delivering our CISO as a Service has been exemplary. He has completely focused on the Trust's needs rather than any third-party commercial drivers. His integrity, knowledge, ability and flexibility to go above and beyond have been second to none. I am thoroughly satisfied with the solution provided and would not hesitate in recommending it."

University Hospital North Midlands

info@i3secure.co.uk

Our Client Portfolio

We're trusted by a number of highly regulated and complex organisations: in the public, private and defence sectors.

Ministry of Defence

POST OFFICE

NHS London Ambulance Service NHS Trust

TRANSPORT FOR LONDON EVERY JOURNEY MATTERS

HADEAN

South Somerset District Council

Humberside Police

GB Railfreight

iFORCE

Ramsay Health Care

NHS Buckinghamshire Healthcare NHS Trust

GIACOM™

"i3secure were fundamental to gaining our ISO 27001 certification on a very aggressive timeline. They were an effective guide through every stage - from initial scoping through to audit. They worked as both an extension of our team to take on the implementation effort and as a driver holding us to account for the necessary business change. We would highly recommend them.

Hadean

Our Experience

Case Study

Client
iForce Ltd

Service
ISO 27001 Implementation and Ongoing ISMS Management

“i3Secure have helped us overcome a number of information security and data privacy obstacles, they have provided innovative solutions and have always reacted in a timely manner. It is an honour to have i3Secure support our team and we look forward to continuing our working relationship with i3Secure.“

Senior Test Analyst, iForce Group

info@i3secure.co.uk

Case Study

iForce Ltd - ISO 27001 Implementation and Ongoing ISMS Management

Situation

i3Secure was selected as a new supplier to iForce Ltd in early 2020. This was during a period of resource challenge for the company. The senior management team were looking for a reliable consultancy to implement an ISO 27001 Information Security Management System to provide assurance to their customers.

i3Secure was selected as the preferred Cyber Security supplier because of our commitment to providing reliable consultants, for being a flexible company to work with and for having deep rooted values – integrity, innovation, and ingenuity. Work began implementing ISO 27001 for iForce in summer 2020.

Action

Our highly qualified and experienced consultant began work by conducting a Gap Analysis against the ISO 27001 Standard to better inform the implementation plan. This involved working with iForce employees and members of the senior leadership team to understand the security posture of the company before any implementation work started. Our Lead Implementer then created an outline plan for the project and once this had gained appropriate sign off, began implementing the Standard. In preparing the company for Stage 1 and Stage 2 audits with a UKAS accredited Certification Body we took a hands-on approach to creating Policies, Standards and Procedures to meet mandatory requirements. This involved conducting internal audits, management reviews, continuous improvement activities and working with software developers to create “Secure Development Processes”. The i3Secure approach to implementation of ISO 27001 is unique. We aim to provide the most efficient, cost-effective way of gaining certification for our clients.

Task

The task was to ensure the iForce Software as a Service (SaaS) offering – Route Genie was incorporated into an ISO 27001 certified ISMS to ensure future growth of the service and to meet contractual requirements from customers. We were able to deploy an experienced, CISSP level qualified ISO 27001 Lead Implementer at short notice (just 3 weeks) to begin the project.

Result

Passing Stage 1 and Stage 2 audits was a fantastic result for iForce. It was the culmination of hard work and commitment between us and the client. During the implementation of ISO 27001, our consultant had quickly become the go-to person in the company for all Cyber Security and Data Privacy matters, and even some which weren’t strictly cyber security related! The icing on the cake for i3Secure was the request from the customers senior management that we provide ongoing ISMS support and maintenance for a further 12 months. This relationship has continued to work extremely well, evident by contract extensions in 2022, 2023 and 2024 for the support and maintenance of for their ISMS and additional contracts for UK GDPR Assurance projects and Cyber Security training.

Our Experience

Case Study

Client
Ministry of Defence

Service
Security Assurance &
Secure By Design

“i3Secure’s consultant worked tirelessly to plan and communicate our programme’s approach to security assurance, developing a strategic methodology to adopt and transition to Secure by Design“

Programme Delivery Manager, Defence Digital

Ministry of Defence

Case study

Defence Digital - Security Assurance & Secure by Design

Situation

Our Security Assurance Coordinator (SAC) was selected to be part of the design and build team for an innovative data platform programme for the Ministry of Defence in Defence Digital. The team was formed of Civil Servants and consultants from a range of commercial companies, government laboratories and His Majesty's Armed Forces. Having such a diverse team required our consultant to already have a strong understanding of MOD policies and directives along with national and international cyber security standards and methodologies such as NIST.

The role required the formulation of all papers and plans to support the cyber security elements of the project throughout the Concept, Assessment, Demonstration, Manufacture, In-Service and Disposal (CADMID) lifecycle.

Action

Our consultant quickly gained the confidence of all collaborative partners and built effective professional relationships with all elements of the project. To ensure timely progress, our consultant produced a Risk Assessment in line with NIST 800-30, a Risk Treatment Plan and Risk Register, Baseline Control Set, System Security Categorisation (FIPS…), Risk Management Accreditation Document Set, Plan of Action and Milestones, a NIST 800-37 Document Tree, Security Working Group (SWG) documents and presentations and chaired the bi-weekly SWG. The document set fulfilled the requirements defined in JSP 440 and JSP 604.

Task

Appointed during the CONCEPT phase, the SAC was fully immersed in the project from the early design stages. The SAC was tasked to advise and direct on the relevant MOD policies and how they should be applied in conjunction with the National Institute of Science and Technology (NIST) Risk Management Framework process and select appropriate controls.

Result

Our consultant's experience meant they had full understanding of the processes involved which consequently allowed the project to deliver within tight timeframes even despite significant changing requirements. of the programme. Collaborative working, striving for excellence and high professional competence produced an outstanding product.

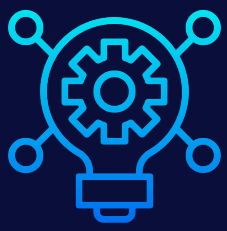
The professional ability of our consultant coupled with the nature of the interactions with all stakeholders involved with the project, resulted in the our consultant being requested to join the team once again during the next evolution of the system.

What You Can Expect From Our Service Team

Quality of Service is at the heart of everything we do

Clients are our number one priority. Without their trust and respect, i3Secure wouldn't be the success it is today. We will make a conscious effort to deeply understand client needs and expectations. This understanding, combined with our specialist knowledge of Cyber security , Information Assurance and Data Protection consulting, enables us to help cleints acheieve their desired outcomes.

Unrivalled cyber security solutions



Our proprietary solutions can analyse your existing exposures and deliver effective solutions that integrate seamlessly into your business activities. We use our expert knowledge of technology, governance, and regulations to help you overcome business challenges and cost drivers, while enabling you to drive further growth.

Highly experienced specialists

Our consultants have been serving clients for over 40 years. We have worked with similar organisations both domestically and globally, delivering solutions that enable our clients to meet their security needs during tight timescales and extreme commercial pressures.

Delivering credible cyber security professionals

i3Secure deliver a dynamic team that will bring an innovative approach to your Cyber security.
Most of our services can be provided remotely, ensuring a smooth and fast deployment, when it matters most.

Alligning ourselves with your vision

Our methodology is designed to understand your long-term aspirations and provide solutions that empower you to achieve them. While we understand that ambitions do evolve over time, we are flexible enough to adapt quickly and ensure your services remain appropriate and best in class.

i3Secure Ltd
i3secure.co.uk
info@i3secure.co.uk