G-CLOUD 14

Service Definitions

4Secure Ltd

May 2024

CONTENTS

INTRODUCTION

1. 4Secure prides itself on its agile and responsive operating model, delivering consistent, timely and high quality Cloud Support Services in the following areas:

- Strategic Information Assurance
- Risk Management & Accreditation
- Technical Security & Architecture
- Information Assurance Compliance and Assessment
- Cyber Security Expertise
- Digital Forensics
- Cross Domain Transfer Services

2. Our team of IA & Cyber Security professionals possess a wealth of knowledge and experience within HMG, and are fully conversant with prevailing HMG Security policies, Information Assurance standards and the latest National Cyber Security Centre (NCSC), National Protective Security Authority (NPSA) guidance and Industry best practice.

3. Our team of highly skilled and experienced IA and Cyber Security professionals are members of various professional bodies including the Institute of Information Security Specialists (IISP), British Computing Society (BCS), ISACA, ISC^2 and possess some form of professional qualification/certification including Certified Information Systems Security Professionals (CISSP), Certified Cyber Professional (CCP) and CREST Testers with many other specialist qualifications in other areas.

Contact Details

4. For more information on our Cloud Support Services, please contact:

The Digital Marketplace - Searching for 4Secure, or:

4Secure Ltd
80 Main Road
Earls Barton
Northamptonshire
NN6 0HJ

Tel No: 0800 043 0101

Fax No: 0845 053 7101

Email: enquiries@4-secure.com

Website: www.4-secure.com

SERVICE DESCRIPTION

Strategic Information Assurance

5. 4Secure recognise the importance effective IA governance plays within an organisation, both in terms of demonstrating board level commitment to IA and promoting robust and effective security cultures and behaviours throughout the business.

6. 4Secure have extensive experience setting, creating and delivering effective and successful IA programmes, strategies and policies within the public and private sector. Our consultants will confidently engage and collaborate with key stakeholders across the organisation, drawing on years of experience working with, and supporting, board level security representative (in particular Departmental Security Officers and Senior Information Risk Owners) in order to successfully deliver business driven IA and Risk Management activities throughout your organisation.

7. As part of this service provision, 4Secure are able to:

- Define and implement a business-driven IA Governance model and compliance regime, that integrates robust and effective information risk management activities into the heart of the organisations operating model.
- Consult, engage and influence senior stakeholders on business driven information risk management strategies, policies and practices.
- Initiate the development of new IA controls and/or policies.
- Develop organisation wide information risk assessment and management techniques, reporting frameworks and/or processes.
- Undertake audit and compliance activities against applicable security and IA standards/policies, analysing shortfalls and/or capability gaps and advising on proportionate and effective risk management activities.
- Collaboratively work with Senior Information Risk Owners (SIROs) and Information Asset Owners (IAOs) to develop risk appetite and tolerance statements in support of business lead priorities and objectives.
- Enable informed decision making across the business making, through strategic level threat and risk modelling and the development of enterprise wide risk and threat landscapes/registers.
- Support the delivery of strategic and tactical information risk reporting requirements against organisational security principles and outcomes (Security Risk Management Overview, Annual IT Health Checks, Departmental Security Officer Reporting etc).
- Assessing supply chain threats and advising on proportionate and effective IA activities within the context of the organisations risk appetite. Where necessary 4Secure can also manage the completion of Cyber Essentials, Defence Cyber Protection Partnership (DCPP) and NCSC Supplier Assurance submissions.

Risk Management & Accreditation

8. At 4Secure, our team of IA and Cyber Security professionals not only possess extensive knowledge and experience of public sector risk management and accreditation policy and procedures (Inc. the Security Policy Framework and JSP440), they also have a proven track record successfully supporting the secure delivery of some of the most complex and novel ICT systems within HMG.

9. The increasing reliance on ICT systems and continued demand for a fully connected digital world, coupled with the evolving cyber threat has only emphasised the need for agile, effective, and fully embedded through life risk management and accreditation activities within the business. Our risk management and accreditation service can be tailored to meet the needs of the business, ensuring proportionate and effective risk assessment and management activities are conducted within the context of the business requirement and fully aligned to the organisations risk appetite/tolerance levels.

10. As part of this service provision, 4Secure are able to:

- Undertake a full business impact assessment in consultation with internal/external stakeholders (in particular IAOs), against the organisation's information assets, identifying the business impact levels for the Confidentiality, Integrity, and Availability (considering the impact of Aggregation).
- Undertake an assessment of potential threats, vulnerabilities and identify, categorise and prioritise appropriate controls to reduce risks to a level deemed acceptable to the business. Throughout this process our consultants will take full account of relevant statutory obligations and protections, including the Data Protection Act, Freedom of Information Act, the Official Secrets Act etc.
- Consult and engage with relevant stakeholders (delivery teams, accreditor etc.) to scope accreditation and assurance strategies. Develop and agree associated accreditation management plans (including the production of the complete risk management and accreditation body of evidence) aligning deliverables with key project/programme milestones.
- Conduct a comprehensive technical risk assessment in accordance with the agreed risk assessment methodology and provide technical advice to determine proportionate and effective security controls to mitigate the identified risks within agreed risk appetites/tolerances.
- Develop the required policies, procedures, and processes (Inc. Security Operating Procedures, Risk Registers etc.) agreed as part of the risk management and accreditation body of evidence.
- Identify and document through life information assurance processes, in order to ensure security controls, remain effective and commensurate to the evolving threat landscape.
- Undertake an independent assessment that the information system meets its information assurance requirements and that any identified residual risks, are being managed within organisational risk appetite and tolerance levels.

Technical Security & Architecture

11. As part of our technical security services, our highly qualified team of security architects and engineers are experienced in the design and implementation of secure ICT architectures within the public and private sector.

12. As part of this service provision, 4Secure are able to:

- Scope, review and design architectures against HMG and Industry best practice guidance, that mitigate identified information risks posed by new technologies and business practices.

- Identify information risks that arise from potential architectural solutions, advising on alternative design solutions to mitigate identified risks.

Information Assurance Compliance and Assessment

13. At 4Secure, we recognise the increasing challenges organisations face in the digital world. With the rapid development of new ICT systems and the evolving nature of today's cyber threat, maintaining the security and resilience of business critical systems can be a challenge. Our IA Compliance and Assessment services offer a range of strategic and tactical activities, tailored to your organisations needs to tackle this challenge head on.

14. As part of this service provision, 4Secure are able to:

- Conduct a range of targeted technical vulnerability testing activities (inclusive of IT Health Checks and Penetration Testing), including the categorisation and prioritising of system vulnerabilities to support remediation plans.
- Scope and provide specialist input on targeted system and product assurance schemes.
- Provide impartial assessment and reports on security investigations, information risk management and investment decisions to improve an organisation's information risk management
- Provide an independent assessment on whether IA control objectives are being met within the organisation, identifying systemic trends and weaknesses in security, and recommending proportionate and effective responses to findings.
- Undertake a thorough review of the configuration of organisational ICT (inclusive of end user devices, servers and boundary protection devices) against HMG guidance and Industry best practice, optimising security enforcing features/settings to enhance system security and resilience.
- Review and assess business critical ICT systems, processes and procedures against the organisations business continuity and disaster recovery strategies/plans, ensuring 'response' activities support the continuous operation of core business services during critical events and/or incidents.
- Provide a discreet and professional incident response capability to support the preparation, detection, analysis, containment, eradication and recovery (Inc. post incident and lessons learnt reporting) of an incident in accordance with HMG and Industry best practice policies, standards and guidelines.

Cyber Security Expertise

15. At 4Secure our team of information security professionals possess a wealth of knowledge and experience delivering highly effective subject matter expertise within the public and private sectors.

16. The entire team is fully conversant with prevailing national and international security standards, policies and legislation, and have years of practical experience setting, creating and delivering effective and successful information security strategies, concepts and regimes tailored to the individual needs of an organisation.

17. As an organisation we remain committed to the strategic intent of the UK Cyber Security Strategy and continue to support the successful delivery of its core objective across government departments and other private sector organisations.

Digital Forensics

18. 4Secure's digital forensic capabilities offer a complete catalogue of digital forensic services, from simple data recovery to full digital investigations of corporate systems. Our analysts will examine your digital media with the aim of identifying, preserving, recovering, analysing and presenting facts and opinions in a report format. Throughout this process our experts can recover data and/or admissible evidence to support legal or disciplinary proceedings.

19. As part of this service provision, 4Secure are able to:

- Provide a complete digital media forensic investigation capability; including full data recovery and evidence capture activities in accordance with HMG and Industry best practice.
- Provide forensic readiness consultancy in accordance with HMG and Industry best practice.

SERVICE MANAGEMENT

Ordering and Invoicing

20. Customers are encouraged to contact 4Secure in the first instance, in order to discuss the nature, scope and scale of the requirement prior to placing an order. Further information on ordering and invoicing can be found in our Standard Terms and Conditions.

Payment and Performance

21. Information on payment and performance can be found in our Standard Terms and Conditions.

Termination Terms

22. Our standard Terms and Conditions set out the specific termination terms against the contract or its schedules.

Service Constraints

23. Under the Cloud Support (Lot 3) G-Cloud provision, 4Secure is providing IA and Cyber Security specialists on a per day basis for services supplied, and on a per delegate/day basis for training services unless otherwise indicated. There may be circumstances (long term contract, multiple resources, group bookings) where rates can be negotiated and/or fixed price arrangements agreed.

Customer Responsibilities

24. Throughout the course of our engagements, the Customer is expected to make available all information (documentation), information facilities (specialist/sensitive ICT provisions) and personnel required in order to fulfil the statement of work. These shall be made available in a timely manner in order to avoid any delay to the agreed work schedule/deliverables.

25. Where the engagement requires the production and/or exchange of information, the format and delivery mechanism will be agreed with the customer, with due consideration to any sensitivities (Security Classification etc.) of the information.

Considerations

26. The following elements are not applicable to this service provision, unless specifically requested by the customer:

- Backup/restore and disaster recovery.
- On-boarding and Off-boarding.
- Data restoration / service migration.
- Technical requirements (e.g. client-side requirements, bandwidth/latency requirements etc.), and
- Trial service.