G-Cloud

Specialist Services - Cloud support

Catalogue of Services

Service Definitions

15 Colmore Row, Birmingham. B3 2BH - 01215 170057 - www.information-assurance.co.uk
enquiries@information-assurance.co.uk

Contents

Our Service Definitions

Service Name

TOGAF, MODAF, ZACHMANN and SABSA Architecture and Design

Service Description

Effective security is achieved by ‘building in’ appropriate controls during system or service design. All too often, controls are ‘bolted on’ at the end of the development process leading to additional cost and less effective risk mitigation.

We pragmatically apply best practice approaches such as SABSA, MODAF, TOGAF and Zachmann frameworks proportionate to your business. Using these architecture methods to deliver consistent best practice driven security architectures that fully support G-Cloud and generic cloud services.

Service Features

- Pragmatic Architectural Design and Advice
- Evaluation of supplier security architecture design
- Risk Assessment and Mitigation
- Alignment of security architecture with business objectives, priorities and functionality
- Approach is tailored to each organisation
- Clear terms of reference and operational framework
- Best practice driven approach

Service Benefits

- Independent assessment of supplier security architecture providing assurance
- Supports HMG Security Policy Framework compliance and accreditation objectives
- Supports HMG’s 10 Steps to Cyber Security
- Reducing cost through application of security at design and through Agile sprints
- Stakeholder confidence knowing that security design has been verified
- Proportional approach matched to risk appetite and security economics
- Quality of Service assured by professional certifications

Service Name

PCI-DSS

Service Description

Any organisation that handles credit card data is required to meet the Payment Card Industry Data Security Standard (PCI DSS). Failure to address PCI compliance, or lacking an understanding of how the Standard applies to your enterprise, can be costly.

We can assist organisations of all sizes in achieving PCI DSS compliance. Ensuring that the transmission, storage and processing of cardholder data is done so in the most secure and practical way, will not only achieve the required level of compliance but more importantly will minimise the potential of being subjected to a data breach.

Service Features

- PCI DSS Strategy and planning
- PCI DSS Scope review
- PCI DSS Readiness assessment and gap analysis
- Payment Application Best Practices Assessment (PABP)
- PCI DSS Program design
- PCI DSS Implementation
- PCI DSS Remediation validation
- PCI DSS report on compliance

Service Benefits

- Offers unbiased, real-view of PCI compliance posture
- Negates the need to perform internal audits
- Ensures legal compliance where required.
- Enhances organisational awareness of PCI
- Enables and efficient implementation of PCI
- Maintains and manages ongoing PCI DSS business requirements

Service Name

Digital Defence and Regulatory Compliance

Service Description

Our Digital Defence and Regulatory Compliance service resolves complex data assurance and compliance issues by identifying and classifying sensitive data, and protects the data in transit, during processing and at rest. Our service resolves complex data protection, compromise and and compliance challenges.

Features

- Identify, value and classify sensitive information and services.
- Proportionately deploy controls treating risks according to risk business appetite.
- Compliance with PCI, GLBA, HIPAA, Sarbanes-Oxley, PIPEDA
- Compliance with the UK DPA
- Compliance with Safe Harbor, EU Data Protection Directives and Right to be Forgotten

Benefits

- Controls are deployed to treat the risks against digital businesses
- Control and governance suites are monitored to maintain regulatory compliance
- Principles of security economics are followed offering business value
- Valuable assets are protected within the boundaries of regulatory scope
- Avoidance of costly regulatory breaches and associated punitive action

Service Name

Secure Code Review

Service Description

We can conduct code review as an integrated, iterative or stand-alone activity to support digital delivery via web applications utilising open source technologies.

Our approach can identify issues that would be challenging to identify or exploit without access to the code. There are a range of options to balance thoroughness and cost to deliver an appropriate service.

Features

- Automated and manual ‘line-by-line’ code reviews
- Available as a standalone or integrated (iterative) service
- Can be taken as part of a wider security review
- Integrates with Secure Development Lifecycle and Agile methods
- Time optimised services available; prioritising key aspects of the code
- Extensive line-by-line reviews available
- Compatible with in-house, third party and open source code
- SC staff available
- Full SC project management wrap around
- Covering the former IL0, IL1, IL2, IL3, IL4 and IL5 environments

Benefits

- Iterative manual reviews to compliment agile processes
- Assurance over internal testing to focus refactoring activity
- Removes deadline demands to discover vulnerabilities in complex systems
- Fully compliant and conversant with OWASP / CLASP / MS-SSDLC

Service Name

GDPR Consultancy

Service Description

Provision of services that will enable organisations to comply with the General Data Protection Regulation (GDPR).

Our services encompass specialist data protection consultancy, GDPR Awareness workshops, GDPR assessments, GDPR training, Data Protection Impact Assessments (DPIA), data breach management and programme management of GDPR compliance activity.

Service Features

- Impartial and vendor neutral advice
- Expert knowledge of GDPR requirements
- Programme management services for delivering GDPR compliance
- GDPR expertise covering breach, incident management and cyber security service
- Tooling to identify personal data held in the cloud
- GDPR compliance gap analysis and review
- Risk assessment of personal data usage
- Identification and analysis of personal data usage across departments
- Certified GDPR Practitioners
- Define technical and non technical solutions to meet GDPR requirements

Service Benefits

- Know what steps to take if you lose personal data
- Avoid large fines and reputational damage
- Operate your business with confidence
- Create greater trust with your customers and suppliers
- Be compliant with GDPR
- An understanding of your Personal and Sensitive Personal Data processing
- Provision of Certified GDPR Practitioners
- We are experts in regulatory transformation, reducing risk for organisations
- Cost-effective and flexible service delivery model
- Ensure best practice and end user adoption

Service Name

UK Government Security (GSG) - Secure by Design (SbD) Implementation

Service Description

Provision of services that will enable organisations to effectively and efficiently implement UK Government's Mandated Secure by Design Principles. And, where required, the Secure by Design Framework.

Our service covers all 10 SbD principles, and associated activities with each principle, leading to the desired SbD outcomes upon GSG audit.

Service Features

- Create organisational responsibility for cyber security risk
- Source secure technology products
- Adopt a risk-driven approach
- Design usable security controls
- Build in detect and respond security
- Design flexible architectures
- Minimise the attack surface
- Defend in depth
- Make changes securely
- Embed security into all Agile dev processes (inc CICD pipelines)

Service Benefits

- Cyber security is considered, at senior leadership levels in accordance with project and organisational risk appetite
- Informed decisions are made on the trade-off between security, performance, usability and function
- Risks are minimised in accordance with principles of security economics and risk appetite
- A dynamic risk management process that can respond to emerging threats
- Insecure practices are avoided by removing incentives for users to find workarounds
- Fewer weak points where compromises could occur or go undetected
- Faster response is provided to evolving cyber threats
- Reduce opportunities for potential attackers to exploit vulnerabilities in a service
- Keeps the impact of vulnerabilities more contained
- Services are built and maintained with controls required to treat security risks
- Changes are not compromised by changes or updates
- Security is baked-in at all stages of project development, from inception to decommission

Information Assurance, Digital Defence, Information Security and Cyber Security

Knox Cyber Security provide specialist advisory services of cyber security, agile security, information security, secure arcitecture and secure design services. However, as a Cloud support specialist service provider, do not provide this facet of this service. This service is associated within other Lots of G Cloud.

Data Restoration / Backup / Restore and Disaster Recovery

Knox Cyber Security are expert advisors of Business Continuity (including Incident Management and Crisis Management tools and techniques). However, as a Cloud support specialist service provider, do not provide this facet of this service. This service is associated within other Lots of G Cloud.

ISO27001 / Cyber Essentials Certifications

We at Knox Cyber Security hold certification to, and are a Certification Body for the Cyber Essentials schemes. The scope of our certification covers the whole of our business operations. This is in concert with the mandated supplier requirement within the Cabinet Office Procurement Policy Note - Use of Cyber Essentials Scheme Certification - Action Note 09/14 of the 25th September 2014[1].

Our Service Offerings Aligned to the Government Security Classification (GSC) scheme

We at Knox Cyber Security have expertise and substantial experience in the delivery of expert cyber security and accreditation advisory services We offer services to client-partners storing and processing information at all levels of the GSC scheme from **OFFICIAL** to high-threat and military client partners processing **TOP-SECRET** information. However, as a Cloud support specialist service provider, we do not provide client-partner storage or processing facets of this service. Storage and processing elements of this service is associated within other Lots of G Cloud.

On-boarding and off-boarding processes/service migration/scope

We at Knox Cyber Security have expertise and substantial experience in advising cyber security, accreditation, scooping and planning requirements to client-partners migrating to, from and between Cloud Service Providers (on and off boarding). Our services are agnostic of technology or cloud models utilised (as per NIST and Cloud Security Alliance definitions). However, as a Cloud support specialist service provider, we do not provide technical facets of this service. On and off-boarding technical facets of this service is associated within other Lots of G Cloud.

---

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/378247/Cyber_Essentials_Scheme_draft_PPN_28_10.pdf

A Brief Overview of Our Pricing Structure

Knox Cyber Security provides consultancy services for Agile cyber security and accreditation projects on the basis of a fixed daily rate for agreed projects and timescales.

Level	SFIA Definition(s)	Day Rates for All Disciplines*
Senior Consultant	Substantial experience in their specialist field and in a consultancy role. Previous experience in providing specialist technical/subject advice and guidance, and evidence of working on a wide range of high quality and relevant projects. Familiarity of the issues/problems facing public sector organisations.	**720**
Principal Consultant	Substantial experience in their specialist field and in a consultancy role. Sound knowledge of the public sector and current policy and political issues affecting it. Previous experience in providing the specialist technical/subject advice and guidance on at least three major projects preferably in the public sector. Awareness of Government and public sector recognised methodologies	**810**
Managing Consultant	Substantial experience in their specialist field and in a consultancy role. In depth knowledge of the public sector and of current policy and political issues affecting it. Previous experience in providing the specialist technical/subject advice and guidance on at least five major projects, preferably in the public sector. Experience of Government and public sector recognised methodologies.	**1,035**
Director / Partner	Extensive experience in their specialist field, in which they are nationally or internationally renowned as an expert. Extensive experience of leading or directing major, complex and business-critical projects; bringing genuine strategic insight. In depth knowledge of the public sector and of current policy and political issues affecting it.	**1,350**
Discipline Specialisms Include (but are not limited to): CLAS, CISSP, CCP, CEng, CEH, CHFI, CICISO, ITPC, SABSA, ISO27001 Lead Auditor, Certified SCRUM Master (CSM), CSA Cloud Security Auditor.		

Table 1 - Pricing for Specialist Disciplines

Service Management

Knox Cyber Security has a Client-Partner Liaison Officer who is responsible for the overall management of all contracts.

All Knox Cyber Security personnel are self motivated specialists who are used to working with little or no supervision and are capable of liaising with all levels from top management to users within a client organisation. In some circumstances, depending on the size of the contract, Knox Cyber Security may assign an individual Engagement Manager who would be responsible for liaising with the overall Programme

Service Levels

As a Cloud support specialist service provider, we do not supply this service.

Financial recompense Model

Knox Cyber Security , will only invoice upon completion of Client-Partner requirements within agreed parameters. Therefore, no financial recompense mode is applicable.

Training

We at Knox Cyber Security do not undertake formal classroom based training activities. However we do employ skills-transference, coaching and mentoring as part of our using Alistair Cockburn's 'Crystal Clear' osmotic communication methods.

Ordering and Invoicing Process

Orders submitted to Knox Cyber Security for G-Cloud services through the G-Cloud Cloud support Procurement Vehicle will remain open for acceptance by the Client-Partner for thirty days from the date of submission of the specific contract from Knox Cyber Security to the Client-Partner.

Acceptance shall be valid only if made in writing signed by or on behalf of the Client-Partner. Variation of the terms of a Proposal shall be effective only if specified in the written acceptance and countersigned by an authorised representative of Knox Cyber Security .

Knox Cyber Security will invoice the Client-Partner in the amounts and on the basis set out in the proposal with the Client-Partner. Knox Cyber Security is VAT registered, and VAT will be added at the prevailing rate.

Payment terms for all sums payable to Knox Cyber Security by the Client-Partner are thirty days from the date of invoice and shall be paid monthly in arrears.

Termination Terms

If, after acceptance of a Proposal, the Client-Partner shall terminate or be in serious or (after warning) repeated breach of its agreement with Knox Cyber Security or act in such a manner as to render the performance of the agreement by Knox Cyber Security wholly or substantially infeasible, then the obligations of Knox Cyber Security under the agreement shall cease forthwith.

In such a case the Client-Partner shall immediately pay to Knox Cyber Security all fees and expenses (including all the expenses of or caused by or arising out of such termination) and other sums then owing to Knox Cyber Security under the agreement together with a sum equal to the whole of the fees thereafter remaining to be paid under the agreement.

If, after the acceptance of a Proposal, the rights of Knox Cyber Security or of the Client-Partner under the agreement are wholly or substantially diminished or the performance thereof rendered wholly or substantially impossible by reason of force majeure, then the obligations of both parties shall cease forthwith except that the Client-Partner shall pay to Knox Cyber Security all fees and expenses then owing to the company (including all the expenses of or caused by or arising out of such termination) together with a sum equal to whichever is the lesser of the fees remaining to be paid thereafter or a proportion of the total fees equivalent to sixty days' work calculated pro rata against the total time estimated for the project.

Service Constraints and Points of Clarification

Knox Cyber Security provides services through G-Cloud under Cloud support through the deployment of Agile, Digital Defence, Cloud Security and Cyber Security Consultants.

Our consultants and their services are supplied on a 'per-day' undertaking.

The services are such that there is no hardware or software deployed for Client-Partner use or for their ownership. Furthermore, unless specifically requested as a service by the Customer then the following do not apply:

1. Data restoration / business continuity / migration / on or off boarding service (other than associated advisory services);

2. Technical requirements (service dependencies, technical bandwidth / latency);

3. A trial of our consultancy offerings;

About Us - Our Supplier Description

Knox Cyber Security

Knox Cyber Security offers strategic and tactical cyber security advice to high-threat commercial organisations, to UK Government Departments, to the Defence Sector, to healthcare providers, to the education sector and to voluntary organisations. We offer impartial and expert advice to aid our Client Partners in meeting the UK Cyber Security Strategy objectives for risk reduction, opportunity exploitation and capability improvement. Thus assuring their technical activities in a proportionate manner.

Knox Cyber Security offers the following expert consulting professionals:

- Ex-CLAS Consultants
- CCP Consultants
- TSAR Listed Consultants
- Certified Information System Security Professionals (CISSP)
- Certified Secure Development Lifecycle Professionals (CSSLP)
- Certified Cloud Security Professionals (CCSP)
- Information System Security Architecture Professionals (ISSAP)
- Certified Information Security Managers (ISACA)
- Certified Information Systems Auditors (CISA)
- Certified in Risk and Information Systems Control (CRISC)
- SABSA Chartered Security Architects
- TOGAF Certified Consultants
- Certified Chief Information Security Officers
- Certified Ethical Hackers
- Qualified Security Team Members (QSTM - Tiger Scheme)
- GDPR Professionals (CESG)
- SANS Certified Web Application Security Consultants
- ISO27001 Lead Auditors
- Certified SCRUM Masters
- Certified Product Owners
- Prince 2 Practitioners
- Chartered Fellows and Members of the British Computer Society
- Members of the Institute of Information Security Professionals
- Fellows of the Institute of Analysts and Programmers

We have, within HMG professional practice and academic research (at the University of Oxford), incorporated HMG Cyber Security principles with Agile practices and methods during the development of online digital services to UK Government.

We have contributed to national policy as members of CESG's CLAS Policy and Tools Working Group and acted to promote UK Government Policy as part of CESG's CLAS Marketing Group.

Our End-Clients[2]

We have performed cyber security services for the following end-clients:

- Driver and Vehicle Licensing Agency
- Student Loan Company
- Food Standards Agency
- Atomic Weapons Establishment
- Northern Ireland Civil Service
- Department of Justice
- Metropolitan Police
- Cambridge Consultants
- Department of Transport
- General Dynamics
- Ministry of Defence

[2] Contracted via intermediary companies within HMG frameworks.

Contact Us

Please feel free to get in touch with us, you'll find us approachable, receptive and affable. We are always happy to discuss your requirements, assist with enquiries and provide further information on any of our services. You'll be surprised at how much we can help you!


15 Colmore Row, Birmingham. B3 2BH


01215 170057


www.information-assurance.co.uk


enquiries@information-assurance.co.uk