SAPPHIRE™

Cyber Security Consultancy

Service Definition

Classification: Internal use Only

Document Information

Document title:	Cyber Security Consultancy Service Definition
Date	
Client Reference	
Sales Contact	
Technical contact	

Proprietary Notice

Service Definition
Cyber Security Consultancy

Overview

Sapphire provides a complete range of cyber security consultancy services in relation to strategies, policies, architecture, products and cyber training and awareness to our clients who are considering and engaging into the cloud environment.

These services include but not limited to the follow areas:

Strategic Services

- CISO as a Service
- Security Culture
- Security Strategy
- Change Management
- Business Continuity
- Governance
- Threat Assessment
- Behavioural Insider Threat Analysis

Tactical Services

- Risk Management
- ISO27001:2013
- Forensic Readiness
- Supply Chain/Third Party Assessments
- Cyber Essentials (PLUS) Security Architecture
- Behavioural and Social Engineering
- GDPR Security Improvement Planning

Operational Services

- Penetration Testing
- Vulnerability Assessments
- Cyber Forensics
- eDiscovery

Sapphire Academy Training and Awareness Courses

Through the Sapphire Academy we offer training and awareness on cyber security in the cloud and much more. Clients can select from our Public Courses or have courses tailored specifically for their needs, which can include branding and organisational specific topics and content.

Examples of our course include:

- Executive Guide to security in the Cloud
- Risk Management in the Cloud
- Business Continuity
- ISO27001 Awareness
- Forensic Readiness
- Internal Auditors
- End User Security Awareness
- Technical Training on Security Products.
- Behavioural Analysis and Insider Threat
- Getting ready for GDPR

Sapphire is a dedicated, independent and trusted security company who for over 20 years have provided comprehensive solutions designed to protect our customer's corporate and client information by ensuring the appropriate and commensurate security controls are in place to protect the organisational information assets from the latest cyber threats.

As a Trusted Security Integrator, our credibility is built not only on our long-standing reputation amongst our clients for successful testing and auditing services but is also demonstrated by our certifications. Sapphire was one of the first organisations in the UK to achieve certification to ISO 27001, the international information security standard. Sapphire have developed our standards and practices over the years based on industry good practice. We are proud to be members of schemes such as NCSC Check and CREST and that all our staff are all highly trained and qualified in their disciplines.

Functional and non-functional Detail

Sapphire can assist you with cyber security consultancy services to ensure the following areas are address in line with UK Government and Industry Good Practice for adoption of cloud-based solutions:

- Policy & Standards
- Risk Management
- Security Architecture
- IA Methodologies
- Third Party & Supply Chain Management
- Incident Management
- Audit & Review
- Training and Awareness

Policy & Standards

Policy and Standards are the core of an organisations information security culture as they define the security requirements in line with the business objectives. All businesses that use IT or online services should have cyber security policies.

Cyber security standards are applicable to all organisations regardless of your size or the industry and sector in which you operate.

Sapphire will provide assistance in the development and implementation of appropriate policies and standards in line with your business needs and based on UK Government and International good practice (e.g. ISO27001, ISO22301)

Risk Management

Sapphire's Risk Management Methodology has been developed over many years in line with industry best practice. Our methodology includes:

- Risk Policy Management
  Review of existing risk management policies and practices and develop, enhance and implement changes as required.

- Gap Analysis & Risk Assessment
  Assess current security practices and controls against standards and legislative requirements that are appropriate to the client's business. These may be UK Government, International (ISO), Industry Sector specific or even internal practices.

- Risk Treatment Plan(s)
  Following a Gap Analysis and Risk Assessment process, Sapphire will produce a prioritised Risk Treatment Plan in line with the client's timeline and business requirements.

- Risk Escalation processes
  In general, companies tend to manage risks at strategic and tactical levels. The strategic risks are usually managed at Corporate Board level, where the tactical risks are often delegated to Head of Departments. If required, Sapphire will assist organisation implement streamlined processes that ensures risks can be effectively escalated from tactical to strategic to ensure the organisations can manage/monitor the risk accordingly.

- Audit process
  The sustainability of a good security culture relies on organisations having appropriate audit processes in place to ensure good security practices are being applied accordingly. Sapphire can assist clients with either carrying out audits on their behalf or by developing an information security audit process for internal staff to adopt and implement. Sapphire can also offer training to internal auditors on information security audit practices.

- Governance & Compliance
  Sapphire assist many of our clients by facilitating Governance and Compliance meetings on a regular basis to ensure all information security requirements for new and existing projects are being implemented in line with expected practices. As part of this process, Sapphire produce a regular positional report for the client's key stakeholder on the progress and issues relating to information security practices

Security Architecture

Sapphire's security consultants have a long-proven track record of understanding business, its challenges, the threat landscape and delivering meaningful security strategies that aligns both the business processes and the technical enablers. Our consultants can review or design secure infrastructure topologies in line with UK Government architectural patterns and also recognised industry best practice. Sapphire has a wealth of knowledge and experience:

- Mobile Security
- Identity Control
- Network Security
- Data Security
- Endpoint Security
- Security Intelligence
- Content Security

IA Methodologies

Our security consultants develop strategies and apply standards for verifying the measures taken to mitigate cyber risks.

Sapphire enhances the business capability of our clients through implementing Information Assurance methodologies to help them enhance their service offerings to their customers and partners.

Incident Management

Sapphire will assist the customers to establish, document, and implement procedures and a management structure to respond to a disruptive incident.

This will include helping to:

a) Identify impact thresholds that justify initiation of formal response,
b) Assess the nature and extent of a disruptive incident and its potential impact,
c) Activate an appropriate business continuity response,
d) Have processes, and procedures for the activation, operation, coordination and communication of the response,
e) Have resources available to support the processes and procedures to manage a disruptive incident in order to minimise impact,
f) Communicate with interested parties and authorities, as well as the media.

Audit & Review

Sapphire has a wealth of audit experience in the areas of gap analysis, internal audit, ISO 27001 system compliance audits. Sapphire offers a range of specific security services against the international standard for best practice information security ISO 27001, as well as general security audits, financial sector audits, internal audits, pandemic flu gap analysis audits, and full system mock compliance audits.

Information Assurance

Sapphire are Accredited to both ISO27001:2013 and Cyber Essentials Plus, which we deem as good practice. Sapphire complies with all legal and statutory requirements as well as client requirements.

As a Trusted Security Integrator, our credibility is built not only on our long-standing reputation amongst our clients for successful testing and auditing services but is also demonstrated by our certifications. Sapphire was one of the first organisations in the UK to achieve certification to ISO 27001, the international information security standard. The organisation is also a member of the NCSC CHECK scheme; developed to enhance the availability and quality of IT health check services provided to government in line with HMG policy.

Sapphire is a Certification Body for Cyber Essentials and Cyber Essentials Plus.

Level of Backup/Restore and Disaster Recovery

Sapphire has a Business Continuity and Disaster Recovery plan in place to mitigate the risk of potential disruption from an incident occurring. Sapphire carries out regular business continuity exercises to test our Business Continuity Plan.

Sapphire has a secure backup strategy and practices, which involves daily backups and regular off-site storage.

Information security is critical to Sapphire, and that of its customers. It is the goal of Sapphire to ensure that:

- Information is protected and controlled against unauthorised access or misuse.
- Confidentiality of information is assured.
- Integrity of information is maintained.
- Business continuity planning processes will be maintained.
- Regulatory, contractual, and legal requirements will be complied with.
- Information security training will be provided to all personnel.
- Security statements will be issued and signed by all personnel.
- Assets are classified and protected as required.
- Physical, logical, environmental and communications security is maintained.
- Operational procedures and responsibilities are maintained.
- All identified information security incidents (breaches, threats, weaknesses, or malfunctions) are reported to the CEO, and investigated through the appropriate management channel.
- Infringement of this Policy may result in immediate disciplinary action or criminal prosecution.
- Business requirements for the availability of information and information systems will be met.

On-boarding and Off-boarding Processes

For all consultancy services, Sapphire will provide a project cost which will include scoping, phased delivery, reporting and associated deliverables and presentations to senior management.

The project cost will be identified following the scoping call/meeting.

Service Pricing

All Sapphire services are £900.00 per day and an overall project cost will be submitted following a scoping meeting/call.

Service Management

Sapphire's uses project management techniques as a methodical approach to planning and guiding a project from start to finish. Using best practice methods, we adopt key processes which direct our customers through five stages: presales, scoping, executing, controlling, and after care support. Project management is applied to all Sapphire's service range and is widely used to control the complex processes of IT security project and solutions.

Sapphire’s Customer Relationship Management System allows us to maintain our client information in such a manner to maximise the services offered through our Helpdesk and Maintenance Support, Managed Services or Contract Management function.

Service Constraints

None, as the service will be defined during the project scope.

Service Levels

Sapphire is the first line support for all our customers and all calls should be raised through our Helpdesk. Support will be provided between 08:30 and 17:00, Monday to Friday. Calls should be directed to the Sapphire Helpdesk by telephone, fax, or e-mail.

Tel: 0845 58 27999
Fax: 0845 58 27005
Email: helpdesk@sapphire.net

The requester must provide at least the following information.

Company and position
Contact telephone number
E-mail address
Brief description of fault

Other support numbers:

Lisa Ingham 07976 057156
lisa.ingham@sapphire.net
(Consultancy Services Manager, Sapphire)

Alan Moffat 07535 666210
alan.moffat@sapphire.net
(Business Services Director, Sapphire)

Response to Helpdesk calls will be within 4 hours. From the initial call the requester will automatically be informed by e-mail of the log number for future reference. The response to the call will be from an Engineer via, telephone, fax, or e-mail.

On completion of a call an automatic e-mail completion will be sent to the requester together with an incident report.

The Customer is entitled to escalate faults at any time, for example if there is a need to highlight the critical nature or impact of a service outage. The following escalation path should be used:

Level	Contact	Description
Level 1	Sapphire Helpdesk	The first point of escalation should always be the Sapphire Helpdesk and escalation must be separate from the initial call to log the fault. MIB must obtain a case reference number for the fault.
Level 2	Sapphire Professional Service Manager	This is the second point of escalation in the event of the Helpdesk being uncontactable or an increase in call priority being required. MIB should quote the case reference number provided.

Level 3	Sapphire Sales Director	This is the third point of escalation in the event of the Manager being uncontactable or a further increase in call priority being required.

Sapphire also offer 365x7x24 hour support for clients. This information is available on request.

Financial Recompense Model

Sapphire does not offer any additional recompense beyond what is covered by our Professional Indemnity Insurance.

Training

Through the Sapphire Academy we offer training and awareness on cyber security in the cloud and much more. Clients can select from our Public Courses or have courses tailored specifically for their needs, which can include branding and organisational specific topics and content.

Examples of our course include:

- Executive Guide to security in the Cloud
- Risk Management in the Cloud
- Business Continuity
- ISO27001 Awareness
- Forensic Readiness
- Internal Auditors
- End User Security Awareness
- Technical Training on Security Products.
- Behavioural Analysis and Insider Threat
- Getting ready for GDPR

Ordering and Invoicing Process

Following receipt of a purchase order, a credit account application will need to be completed for all new customers to Sapphire. Once approved, a job will be created, and a project team will be assigned to the Penetration Test. On completion of the test and reports have been submitted and signed off by the customer an invoice will be initiated. Hard copies of all invoices are posted to the provided Customer address and contact of the finance department. All invoices are to be paid within a 14-30 day agreed notice period.

Termination and Cancellation Terms

The Professional Services Agreement (PSA) Terms and Conditions may be terminated by either party on giving at least 30 days' notice to the other. If we give notice, you shall be liable to pay all charges up to the expiry of the notice. If you give notice, you shall be liable to pay all charges until 30 days after the date we receive the notice or until expiry of the notice, whichever is the latter. Your service of notice does not avoid any other liability for Service already provided. You shall be entitled to any data or work in progress created in relation to the Service up to the date of termination unless notice is served as a result of a breach of this Agreement by you in which case all rights to such data or work in progress remain with us.

Sapphire reserve the right to invoice in full any job cancelled or deferred within 9 working days of the scheduled delivery/start date*. Jobs cancelled/deferred between 10 and 21 working days of the scheduled delivery/start date will be subject to an invoice of 50% of the total job value**.

Please note: Any time used/spent on will be invoiced (plus associated expenses including travel and accommodation). This time will be deducted from the overall time allocated to the project and may necessitate a further purchase order being raised to cover the projected shortfall in allocated days.

*The invoice for cancelled/deferred jobs within 9 working days of the start date will be equal to the whole value of the purchase order or alternatively 5 days consultancy – whichever is the smaller.

**The invoice for cancelled/deferred jobs within 10 – 21 working days of the start date will be equal to the 50% of the value of the purchase order or alternatively 5 days consultancy – whichever is the smaller.

Data Restoration / Service Migration

All business critical and sensitive data are held on appropriately secured infrastructure. All data is backed-up as defined early in this document.

Sapphire conduct Disaster Recovery tests, data restore tests and UPS tests on a regular basis and being no less than twice within any twelve-month period.

Consumer Responsibilities

Government has very specific requirements towards the governance of computer systems. This is called "accreditation" and requires an individual, called "an Accreditor", to make a balanced decision that all the risks to an information system are appropriately mitigated.

If the project requires UK Government Accreditation, you will be assigned a named Accreditor from the accrediting body. Sapphire will work with this Accreditor throughout the project to ensure all documentation is submitted to their standards for approval.

A security project will require a client's time and management to provide Sapphire with the relevant information to complete the project. This may include writing policies, plans and procedures. This would normally involve in meetings with key staff responsible for business processes and security aspects in your organisation.

Our Cyber Security Consultants will take you through all the system controls and meet with key personnel throughout your organisation.

Technical requirements

Typically, a Cyber project can cover all category areas or on an individual basis dependent on the customer requirements. The timeframes will be dictated during a scoping meeting however the following guidelines have been provided.

- Policy & Standards – 1 day per policy
- Risk Assessment – 2 - 3 days dependent on size of organisation
- Risk Management – 2 - 3 days dependent on size of organisation
- Security Architecture – 3 - 5 day assessment
- IA Methodologies – 3 - 5 day strategy assessment
- Incident Management – 5 – 10 days dependent on size of organisation

- Audit & Review – 2 days

Trial Service

No trial service is available for our Cyber Security Consultancy Services. However, we can meet with your organisation and complete a Gap Analysis.

The Gap Analysis is a 1 day on site assessment (1-day off-site reporting) based on recognised best practices for information security. The analysis will take criteria from the recognised standard ISO 27001 and will cover the following areas:

- Information Security - Organisation and Responsibility
- Risks Relating to External Party's
- Information Classification and Handling
- Internet and Email Acceptable usage policy
- Mobile Device and Asset management
- Incident Reporting and Management policy
- Access Control (network and Application) & Password Management Policy
- Human Resources Security
- Compliance

During the day we will complete a worksheet which will assist with our findings report and initial recommendations for gaining accreditation.