SAPPHIRE™

# GovAssure Consultancy Support

# Service Definition

Classification: Confidential

# Document Information

| | |
|---|---|
| **Document title:** | GovAssure Consultancy Support Service Definition |
| **Date** | |
| **Client Reference** | |
| **Sales Contact** | |
| **Technical contact** | |

# Proprietary Notice

# Service Definition
# GovAssure Consultancy Support

## Overview

The GovAssure scheme provides public sector organisations with a better understanding of their security and resilience capabilities in the face of cyber threats. It relays this information to the central government for transparency and alignment with the Government Cyber Security Strategy to strengthen the UK's resilience against cyber-attacks across services.

Services features:

- GovAssure represents a pioneering approach to cybersecurity assurance for government.
- Replaces the cybersecurity component of the Departmental Security Health Check.
- Designed for official systems and does not apply to secret or higher systems.
- Help improve cyber-security posture and the capabilities of government departments.
- The scope is defined by the essential and critical services you provide.
- Assets should be reviewed and critical systems identified.
- Assign a profile from the Government's Cyber Assessment Framework (CAF).
- Undertake a self-assessment from the CAF.
- Measure your organisation against objectives that align with industry-standard frameworks.
- Accredited third-parties are required to independently review your self-assessment.
- Independent review is completed and report generated.

Service benefits:

- Understanding your strategic context, current and evolving cyber-security threat landscapes.
- Five-stage process, scoping, asset review, self assessment, independent review, reporting.
- Managing Security Risk.
- Protecting Against Cyber Attacks.
- Detecting Cyber Security Events.
- Minimising the Impact of Cyber Security Incidents.
- Validate the results of the CAF assessment.
- Develop a targeted improvement plan.

## Functional and non-functional Detail

Sapphire can conduct a GovAssure based gap analysis based on the five key stages:

Organisational Contact and Services

The first stage is a scoping exercise, where you must have and develop a complete understanding of your strategic context, aligning with current and evolving cyber security threat landscapes. This scope is defined by the essential and critical services you provide.

In-Scope Systems and Services

After this, your assets should be reviewed, and critical systems identified – operational and support systems – related to the essential and critical services you provide. These will be assigned to either a Baseline or Enhanced profile from the Government's Cyber Assessment Framework (CAF).

Security Self-Assessment

Next, you will undertake a self-assessment from the CAF, which measures your organisation against four objectives that also closely align with several industry-standard frameworks such as ISO27001.

1. Managing Security Risk
2. Protecting Against Cyber Attacks
3. Detecting Cyber Security Events
4. Minimising the Impact of Cyber Security Incidents

Independent Assurance Review
Accredited third-parties are then required to independently review your self-assessment, assessing the level of attainment, and validating the results of the CAF assessment findings to determine how effective your current security controls are.

Final Assessment and Improvement Plan
The last step involves a final assessment report generated and provided to you after the independent review is completed, with the Cabinet Office's Government Security Group (GSG) working with you to develop a targeted improvement plan.

For each stage we will cover the principles and establish if the GCloud customer have achieved, partially achieved, or not achieved based on a profile from the Government's Cyber Assessment Framework (CAF). The Q&A based session with key staff members and stakeholders will follow the framework. We can help you achieve Gov Assure Compliance by utilising the following services:

**Managing security risk**

Governance
- CISO as a Service
- ISM as a Service
- Compliance to Legislation and Regulation

Risk Management
- CAF Gap Analysis
- Threat Assessments
- Open-Source Threat Intelligence
- Risk Management of IT/OT
- Penetration Testing
- Vulnerability Management
- Breach Attack Simulations

Asset Management
- IT/OT Asset Discovery
- IT/OT Asset Management
- Endpoint Management

Supply Chain
- Business Impact Assessments
- Third-Party Risk Management

**Protecting against cyber attacks**

Policies & Procedures
- Policy Development
- ISMS Development
- Compliance Audits

Identity & Access Control
- IT/OT Consultancy
- Identity & Access Management
- SOC Services

Data & System Security
- Threat Intelligence & Assessments
- Open-Source Intelligence
- Penetration Testing
- Breach Attack Simulations
- Endpoint Management (EDR/XDR)

Resilience Network & Systems
- Business Continuity
- Incident Response

Training & Awareness
- Security Awareness Training

**Detecting cyber security events**

Security Monitoring
- SOC Services
- Threat Intelligence
- SIEM
- EDR/XDR
- IT/OT Discovery

Proactive Security Event Discovery
- Incident Response
- SOC Services

**Minimising impact of cyber security incidents**

Response & Recovery Planning
- Incident Response Readiness
- Incident Response Management
- Business Continuity Planning
- Disaster Recovery Planning

Response & Recovery Planning
- Debrief Sessions
- Improvement and Remediation Planning
- Security Improvement Plannin

## Information Assurance

There are no external regulators within the industry sector that Sapphire 'as a company' has to provide assurance to. Sapphire complies with all legal and statutory requirements as well as client requirements. Individuals are members of professional CHECK schemes. A compliance Matrix which is ISO27001 certified details these areas and can be made available during an onsite audit.

As a 100% Cyber Security company, 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.

All our testers are SC cleared, as part of their CHECK Team Member and CHECK Team Leader status, sponsored by GHCQ.

For standard testing, we deem that we will hold and process information IL2 and below. For IL3 and higher, Sapphire would recommend using our IT Heath Check service outlined separately within Sapphire's Cloud submission.

## Level of Backup/Restore and Disaster Recovery

Sapphire has a Business Continuity and Disaster Recovery plan in place to enable the company to quickly regain its previous performance and standing after any threat to business continuity, showing as little interruption Sapphires employees and our Customers.

Daily tape backups are taken and stored securely off-site on a weekly basis.
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

Depending on the size of the organisation the minimum number of days for a gap analysis is 3 days at £1,100.00 per day.

## 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.

Customer and account management is achieved using Salesforce. This system manages customer information, opportunities and administration (quotes, purchase orders and invoices).

## 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
**Email**: support@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
(Business 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. The client 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. The client 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. |

## Financial Recompense Model

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

## Training

Sapphire can provide general information security awareness training, and internal auditor specific training, drawing on experience of a wide-ranging security practice across technical and systems disciplines. Our training program includes:

- Digital Forensic Readiness Training
- Insider Threat Management Course
- Tailored Cyber Security Training courses
- BCP Desktop Exercises
- Technical Solutions Training
- ISO27001 Awareness Training
- Security Related Training / Skills and Knowledge Transfer
- The National Information Security Conference (NISC)

## 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 GCloud customer. On completion of the project and reports have been submitted and signed off by the customer an invoice will be initiated. 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

Data is backed-up, in order to ensure that, if required, a valid back-up of previous data is available, for purposes of restoration, or in case data becomes corrupt or lost. Sapphire conducts a tape backup restore test and UPS test process on a twice annual basis.

## Consumer Responsibilities

Arranging the relevant Teams sessions for the interviews and provide cyber security related documentation.

- Information Security Policy / Information Security Manual
- Security Incident Response Plans and where possible related policies
- Business Continuity Policy / Disaster recovery policy and any Threat Response Procedures
- Internet, Email and Computer Acceptable Use Policy
- Any IT security based procedures, relevant to the scenarios
- Employee System overview (HR Application or Staff portals etc)
- Telephone/Contact List

- Overview of major assets used for the delivery of services, including Finance and HR systems, Intranet / Extranet, Procurement systems.
- Overview of end point assets, servers (On Prem / Cloud). PCs, Laptops, mobile devices and any encryption technologies in place (Include any 2FA connectivity in use)
- Risk management policies / process and registers if in use

## Technical requirements

Requirements are as detailed in the functional and non-functional detail.

## Trial Service

Not applicable for this service.