SAPPHIRE™

# Cyber Essentials and Cyber Essentials Plus Service Definition

Classification: Internal use Only

# Document Information

**Document title:** Service Definition

**Date Created**: 23 February 2024

# Document History

| Status | Version | Author | Date | Changes |
|---|---|---|---|---|
| Approved | 1.0 | Kate Oldershaw | 23/02/24 | Rebranded existing approved version |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Proprietary Notice

# Service Definition
# Cyber Essentials and Cyber Essentials Plus

## Overview

Cyber Essentials, a Government-backed, industry supported scheme was set up to help organisations protect themselves against common cyber-attacks. The scheme has five security controls:

1. Secure Configuration
2. Boundary Firewalls and Internet Gateways
3. Access Control and Privilege Management
4. Patch Management
5. Malware Protection

We've been delivering the very best cybersecurity services and solutions for over 22 years. Our expertise covers all aspects of cybersecurity; people, policies and technical controls. We are one of only a small number of organisations in the UK who are qualified to assess and certify businesses against both Cyber Essentials and Cyber Essentials Plus schemes.

Our experienced consultants have a wealth of knowledge and are best placed to review and prepare your business for security audits, as well as offering practical and pragmatic advice and guidance to steer your cybersecurity planning along the right path.

Sapphire is a Certification body for Cyber Essentials and Cyber Essentials Plus against the IASME scheme.

## Functional and non-functional Detail

### Cyber Essentials Basic

Cyber Essentials can help your organisation in many ways:

- Reassure customers that you take cyber security seriously.
- Be listed on our Directory of organisations awarded Cyber Essentials.
- Attract new business with the assurance that you have cyber security measures in place.

Cyber Essentials basic is a self-assessment that is completed online via the IASME portal. Sapphire can provide you a spreadsheet of the questions or a PDF questions booklet can also be found here: https://iasme.co.uk/cyberessentials/basic-level-cyber-essentials/free-download-of-self-assessment-questions/

Once the spreadsheet is complete, you can submit at: https://www.iasme.co.uk/apply-for-self-assessment/. Ian you will need to copy out the answers and into the portal. It is £300.00 for the standard Cyber Essentials basic assessment. There is also an opportunity to complete the Governance questions, which you will get an additional certificate for however be an additional £100.00.

We can help with the self-assessment in two ways, you can complete the spreadsheet in the first instance and send it to Sapphire for one of my Cyber Essentials assessors to review and provide recommendations. At this stage we can guide you around answers and suggest any changes. The spreadsheet now also covers a GDPR module, and it is worthwhile doing the governance questions

too. This will be 0.5 day for remote assistance on this, alternatively we can come on-site for a day and do a gap analysis against the spreadsheet.

### Cyber Essentials Plus

The Cyber Essentials Plus assessment is a more comprehensive detailed security audit which can result in a PASS or FAIL. Anything that is not internet facing can be excluded from scope. Think vulnerability assessment meets audit without a formal penetration test.

The 5 areas we cover as part of a Cyber Essentials Plus:

1. Boundary firewalls and Internet Services;
2. Secure Configuration;
3. User Access Control;
4. Malware Protection; and
5. Patch Management.

To deliver the Cyber Essentials Plus assessment we need to concentrate on the following areas:

**External testing**
Test whether an Internet-based opportunist attacker can hack into the Applicant's system with typical low-skill methods.

**Internal testing**
These tests assess defence against attacks which originate externally but involve some form of internal user action, or which are difficult to test directly from the Internet.

**Authenticated vulnerability scan of devices**
Identify missing patches and security updates that leave vulnerabilities that threats within the scope of the scheme could easily exploit.

**Check malware protection on EUDs**
To check that all of the EUDs in scope benefit from at least a basic level of malware protection.

**Check effectiveness of EUD defences against malware delivered by email**
To test whether or not EUDs are protected against malware that is delivered via email attachments.

**Check EUD defences against malware delivered through a website**
To test whether or not EUDs have protection from malware delivered through a website.
The scope is key and is based on verification of your answers from the basic self-assessment.

## 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

The scope is key and is based on verification of your answers from the basic self-assessment. When it comes to Cyber Essentials Plus we would need to know the following:

- How many internet facing IPs do they have? (this excludes non IAAS cloud services).
- Details of your internal IP address scheme and # approx hosts (within scope of the Cyber Essentials) to be scanned internally (servers/PCs etc etc).
- How many different builds (Operating Systems) do you currently run for you end user devices?
- Do you issue company mobile devices (phones, tablets etc). If so does the figure of your internal assets above include company issued mobile devices?

Typically, a Cyber Essentials Plus audit takes between 3 and 5 days (including audit report).

For Cyber Essentials Basic it is £300.00, plus £100.00 for the Governance module. This is paid by the customer as it is a self-assessment. Sapphire can help with the questionnaire based on a 0.5- or 1-day consultancy services.

## Trial Service

No trial service is available for our Cyber Essentials Consultancy Services. However, we can meet with your organisation and conduct a gap analysis against Cyber Essentials or a technical pre-assessment against Cyber Essentials Plus.