SAPPHIRE™

Corporate Security Awareness Review

Service Definition

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
Corporate Security Awareness Review (CSAR)

Overview

In today's Information Age, companies understand the importance of information security and the impact it has on their company's ability to trade, make profit, optimise performance and affect their future growth. Information security is based on ensuring the appropriate and commensurate controls as in place to protect the Confidentiality, Integrity and Availability of both corporate and customer Information, in line with the risk appetite of the company. Sapphire incorporate a Risk Management approach towards the physical, procedural, people and technical aspects associated to the key business processes of our client's business. Our Corporate Security Awareness Report provides a comprehensive security improvement plan to ensure key information assets are protected from breaches or disaster, while authorised staff can access corporate information from wherever and whenever the business needs to.

Functional and non-functional Detail

Sapphire's approach to providing our Corporate Security Awareness Report (CSAR) is based on the following steps:

1. Scoping
2. Business Review
3. Gap & Risk Analysis
4. Corporate Security Awareness Report

Business Review

Understanding your business is critical to ensure the security measures are appropriate and commensurate to the business requirements of the company. During this phase Sapphire require to understand the following areas:

- Business Objectives
- Business processes
- Compliance requirements
- Existing security culture

The strategic Business Objectives will be defined during the initial meeting with the Project Sponsor.

The key Business Processes, within the scope of the security review, will be analysed to identify any potential areas of weakness in relation to the confidentially, integrity and availability of the individual activities the business process provides and/or relies upon.

External and internal Compliance requirements will be discussed and any key areas included into the Gap Analysis review phase.

A review of the existing security culture and security maturity will be conducted by Sapphire to understand the level of security controls and good practices that have been successfully adopted and integrated into your company.

Client requirement: This phase would require meetings with staff who are responsible for and understand the key business processes within the scope of this project. Each key process meeting is expected to last about 2 hours per process. However, if the processes are integrated than a workshop would be scheduled for all interested parties to minimise staff involvement.

Gap and Risk Analysis

Gap Analysis

The Gap Analysis is a review of the current security practices within your business in line with recognised International Good Practice Guides, for Information Security (ISO27001), Business Continuity Management (ISO22301) and Supply Chain Management (ISO 27036).

Risk Assessments

Sapphire will carry out an Information Security Risk Assessment, which identifies the appropriateness of your existing security controls in relation to the value of the information asset/process it is protecting. Sapphire's Risk Assessment Methodology offers a prioritised list of Risks to your company assets.

The outcome of the Gap Analysis and Risk Assessment provides an 'as-is' picture of where your company is today, in relation to the adoption of good security practices that are appropriate to the business objectives of the company.

Client Involvement: During this phase sapphire require to analyse what security controls including the Physical, Process, People and technical aspects of the systems with scope. It is expected that these would be approx. 45 Minute minutes with HR, Facilities, Legal, and Procurement. The meeting with IT to discuss technical controls is expected to last about half a day.

It should be noted that there may be follow up meetings with key staff to verify our findings and/or to discuss some area in more depth.

Corporate Security Awareness Report (CSAR)

Once we understand the 'as-is' position of the information security aspects of your company, we work with you to develop your Security Improvement Plan that identifies a clear plan of action for the implementation of security controls to allow you to meet your business objectives and implement good practice.

Your Corporate Security Awareness Report provides you with full details of our findings and a clear prioritised roadmap and action plan on how to achieve your goals ('to-be' plan) in relation to incorporating good information security practices within your business processes.

The Corporate Security Awareness Report is a security review of your company and consists of:

- An Executive Summary
- Business Overview
- Gap Analysis (with Statement of Applicability - where relevant)
- Risk Assessment
- Risk Treatment Plan
- Analysis of findings ('as-is')
- Security Improvement Plan ('to-be')

Information Assurance

There is 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 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 CESG CHECK scheme; developed to enhance the availability and quality of IT health check services provided to government in line with HMG policy.

Sapphire has carried out the Cyber Essentials self-assessment and was awarded its certification by IASME Information Security Standard on 8th June 2015 (Certificate Number: IASME-A-00234). Since then, Sapphire has become a Certification Body and our senior business consultant has conducted Cyber Essentials and Cyber Essentials Plus audits.

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 Managing Director 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 £950.00 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.

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
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.

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
- GDPR Awareness Sessions
- BCP Desktop Exercises
- Technical Solutions Training (including but not limited to UAG)
- ISO27001 Awareness Training
- IRCA ISO27001 Lead Auditor
- 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 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

Both critical data and sensitive data are held on various secure servers within Sapphire, both for internal use and for use by Sapphire customers. Such data is backed-up, in order to ensure that, if required, a valid back-up of previous data is available, for purposes of restoration, 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

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.

As part of a CLAS or Cyber project you will be assigned an Accreditor and this individual will need to be introduced to Sapphire. Sapphire will work with the Accreditor throughput the project to ensure all documentation is submitted for his approval.

In a nutshell we need time and people.

A CLAS or Cyber project is all about time, management and providing Sapphire the relevant information to allow us to write the relevant policies, plans and procedures. We simply need you to demonstrate what you have in regard to the system security.

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

Technical requirements

Typically a CSAR 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 a typical CSAR project is 3 -5 days dependent on the size of the organisation.

Trial Service

No trial service is available for our CSAR service 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.