CYBER SECURITY MATURITY ASSESSMENT

CNS at Six Degrees

Fortify your organisation's security posture by evaluating your cyber security maturity against industry benchmarks

The volume, variety and sophistication of cyber security threats have increased significantly, with organisations under constant threat of data loss and disruption from security breaches.

Six Degrees conducts a comprehensive cyber security maturity and benchmarking assessment, delivered and managed in a consultant-led approach that provides you with point-in-time or ongoing visibility into your organisation's security posture.

The Six Degrees Cyber Security Maturity Assessment platform will compile a detailed evaluation of your organisation's cyber security readiness and your ability to address weaknesses, highlighting potential security gaps and making recommendations to reduce vulnerabilities. It draws on recognised standards and approaches including ISO/IEC 27001:2013, Cyber Essentials and NIST 800-53 to deliver a set of questions that cover a range of security domains.

A Comprehensive Assessment of Your Security Infrastructure

Through a predefined consultative engagement, Six Degrees' qualified security consultants will work with you to gather intelligence about your organisation and your current security posture, using the platform to measure and score your organisation's security maturity against 10 key domains:

- Governance
- Physical security
- HR security
- Asset management
- Access controls
- IT security
- Software development
- Supply chain security
- Privacy
- Business continuity and incident management

After the consultations are completed, you will receive a report and a maturity score, along with key areas that you can improve and track progress against.

Cyber Security Maturity Assessment Benefits

- Prioritise future cyber security investment for greater risk reduction.
- Identify and measure the greatest areas of weakness affecting your organisation.
- Highlight the greatest areas of cyber security risk for immediate action.
- Demonstrate the ROI of cyber security spend.
- Assess your suppliers or partners for potential risks and protect your organisation.

A Tailored Report to Prioritise Your Cyber Security Investments

Through our Cyber Security Maturity Assessment, you can access a report that highlights how your organisation's security infrastructure compares against industry and best practice standards. The report maps your security score against the core elements of the security domains and highlights areas of strength and/or weakness.

Within the report, a prioritised action plan shares how you can identify the greatest threats to your organisation, recommends how you can prioritise your cyber security investments, and enables you to better gauge the value and level of return from every cyber security investment, eradicating ineffective spending.

The report provides clear and logical presentation of results, enabling it to be used by both your operational team for improvement road-mapping, and as an executive overview of your security posture for your board members.

For continual assessments, Six Degrees will re-evaluate your security posture annually, bi-annually or quarterly over a one-to-three-year period, or more frequently, if required. Six Degrees will provide access to a real-time dashboard that consolidates your security data reporting and metrics into a single repository, ensuring your organisation has a consistent view of your exposure to cybercrime and potential security gaps, and can help to prioritise security remediation efforts.

Assess and Protect Your Supply Chain

The Cyber Security Maturity Assessment can also be used to assess the cyber security maturity of your current suppliers, and can be used when evaluating and onboarding new suppliers to ensure their security processes and best practices align with your organisation's cyber security policies, protecting your organisation.

Our Credentials

Microsoft Partner | Azure Expert MSP

Member of Microsoft Intelligent Security Association

CREST

CYBER ESSENTIALS PLUS

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR

ISO 27001

CNS at Six Degrees

To learn more about the Six Degrees Cyber Security Maturity Assessment, or to book your assessment, contact your Account Manager or visit https://hub.6dg.co.uk/cyber-security-schedule-call

1. Service Overview

The Cyber Security Maturity Assessment, is a consultant-led approach to understand and rate the Cyber Security Maturity ("CSM") of your organisation or supply chain components. The Service utilises internationally recognised standards and best-practice approaches to provide you insight into your security stance and how that scores against a broad framework of maturity scaled security measurements.

As a standard, we will provide you the following Service features:

(a) Consultant-led assessment;

(b) Contextualised reporting with maturity-based scoring;

(c) Access to our portal to track the assessment and results;

(d) The ability to track your security score and changes to it.

Additionally, we offer the following optional features (subject to an additional Fee):

(a) An assessment of your supply chain to assist you in understanding the security risks associated with your suppliers;

(b) Quarterly or biannual assessments to track CSM progress.

We can deliver the Service as a single, independent point in time assessment (by means of a workshop in first instance) or as part of an ongoing, repeated exercise that measures development and compares your score as you progress on your Cyber Security journey. The Service can focus on individual standards or requirements, such as NIST CSF or NIS Directive, or can be customized to meet your organisation's needs.

We will agree the scope of your Service with you and document details of your Service and the associated Fees in your Order Form and/or SoW.

2. Service Features

2.1 Standards and Approaches

We will assess your cyber security maturity against key elements of recognised standards and approaches that we deemed to be the most appropriate to provide a purposeful and relevant assessment. We use the following standards and approaches:

(a) ISO/IEC 27001:2013;

(b) Cyber Essentials;

(c) NIST 800-53, and;

(d) Best Practice.

2.2 Security Domains

As a standard, we will assess your cyber security maturity against the standards and approaches listed in Section 2.1. The assessment will produce approximately one hundred eighty-five (185) focused security questions that review the following ten (10) different Security Domains:

(a) Governance;

(b) Physical security;

(c) HR security;

(d) Asset management;

(e) Access controls;

(f) IT security;

(g) Software development;

(h) Supply chain security;

(i) Privacy, and;

(j) Business continuity and incident management.

2.3 Optional Customisation

If you require us to assess your cyber security maturity against specific standards or set of requirements not covered in this Service Description, we offer an additional customisation option subject to an additional Fee. Any bespoke requirement will be agreed with you and documented in your Order Form and/or SoW.

2.4 Consultant-led Engagement

The Assessment commences with an initial set of consultative workshops. Our Cyber Security consultants will then process and review the information gathered during the workshop in our benchmarking tool to measure and score your current CSM against the Service's benchmarking questions and domains.

During the workshop(s), our consultants will provide you support in understanding what each question is looking for and will gather information on how your organisation operates in order to reflect this within the CSM tool. Where appropriate, our consultant will require you to provide evidence in order to identify the suitable information to be entered into the tool.

2.5 Security Score Tracking

After completion of the initial set of consultative workshops or, where required, the follow-up workshops, you will be able to track your progress on your CSM journey by accessing the CSM portal. We can perform assessments annually, bi-annually or quarterly over one (1) to three (3) year periods, or more frequently if required. The frequency of assessments and length of contract will be detailed in your Order Form and/or SoW.

2.6 CSM Portal Access

We will setup and configure a personalised portal for you, providing secure access to a dedicated benchmarking tool.

This portal allows you to:

(a) Review the weightings of the key dimensions within the contracted Service benchmarking service option(s) (i.e. best-practice Cybersecurity-related risk standards and/or frameworks);

(b) Revise answers to questions;

(c) Export data for specific regimes;

(d) Create benchmarks over time for comparison;

(e) Review questions and weightings, and;

(f) Create third party benchmarks to assess supply chain.

We will provide you with access to the portal for the length of the Service contract.

2.7 Results and Reporting

Upon completion of the assessment, our consultants will provide you an overview of the findings alongside recommendations. The report maps your security score against the core elements of the security domains used, provides actionable options to improve your security measures and also highlights areas of strength and/or weakness. The recommendations indicate how your security score compares to other organisations and identifies the appropriate actions to improve your overall security posture. Recommendations are rated according to importance - with the most important being item(s) to have the most effect to improve your overall CSM position.

2.8 Supply Chain Assessment

The Service can also be used to assess the CSM of your current suppliers, as well as being used to assist when selecting and onboarding new suppliers.

You can use the Supply Chain Assessment to:

(a) Identify the areas of security weakness of your supplier(s);

(b) Identify the greatest threats to your organisation, from that supplier;

(c) Organise/prioritise Cyber Security remediation to reduce risks related to your supplier(s);

(d) Maintain improvements to CSM;

(e) Demonstrate continuous improvement and the supplier's ability to improve defences;

(f) Demonstrate to your organisation that the supplier can build a successful cybersecurity programme;

(g) Provide evidence to your regulators and customers that you are reviewing your supply chain's security, and;

(h) Show that your organisation is reducing its Cyber Security risk footprint by continually assessing its supply chain.

Once we have assessed and completed all of the relevant information relating to your supply chain's CSM and collated this on the portal, you can request that your supplier makes specific improvements or select and de-select suppliers to align with your organisation's Cyber Security policies.

3. Service Delivery

We will review and agree with you the requirements for the delivery of this Service ahead of the consultancy engagement. We will prepare the CSM platform and schedule the consultant-led assessment at the times agreed with you.

If you are procuring this Service as part of a wider package of security monitoring services, we will include details of such package in your Order Form and/or SoW.

After order acceptance, we will deliver the Service as follows:

Service Delivery	Us	You
We will organise and conduct the initial benchmarking workshop with you.	•	•
You will provide adequate meeting room space and/or assure compatible meeting software (MS Teams, Zoom, *etc.*).		•
You will ensure attendance of your stakeholders.		•
You will provide internet access for our consultant (onsite only).		•
We will build and prepare a dedicated Portal for you.	•	
We will provision a portal in our secured environment.	•	
You will provide a list of user accounts required along with any access restrictions or rights.		•
We will provision accounts as required by you.	•	
We will perform an initial benchmarking of the Service option(s) using COBIT to weight the key dimensions within the contracted Service.	•	
You will provide to us accurate industry and size information for comparison.		•

If applicable, you will request changes to initial weightings.		•
We will share / distribute initial benchmarking activity output with you.	•	
We will organise and conduct an output meeting with you within ten (10) days of the final workshop's completion.	•	
We will make the Assessment output data available to you on the portal.	•	
We will notify your portal users if and when their data is updated.	•	
We will jointly organise and conduct subsequent benchmarking workshops with you.	•	•
You will pre-book dates and stakeholders' time for all scheduled workshops on order placement of this Service.		•
You will repeat initial workshop activities.		•
We will perform ongoing client portal administration.	•	
We will create/delete or perform password resets of users.	•	

3.1 Ready for Service

The Ready for Service Date is the date when we (acting reasonably and properly) notify you that the implementation steps are completed and that the Service is ready for service.

If you consider that the Service is not ready for service on the date notified, you must notify us within two (2) weeks of our notification, after which the Ready for Service date deemed to have occurred and we will proceed with the assessment on the date agreed with you. Any issues of which you may later become aware and notify us about will not change the Ready for Service date and may require additional chargeable services to be resolved.

You can request to postpone the assessment up to eleven (11) Business Days before the agreed assessment date, in which event we will reschedule the assessment and agree a new date with you for no additional charge.

In the event that you are not ready for the assessment on the agreed date and you fail to submit a request to postpone the assessment date with at least eleven (11) Business Days' prior notice, you will be able to cancel the assessment subject to a cancellation fee calculated as follows:

(a) A charge equal to 50% of the Non-Recurring Fee if you submit a cancellation request between eleven (11) and six (6) Business Days before the agreed assessment date; or

(b) A charge equal to 100% of the Non-Recurring Fee if you submit a cancellation request less than (6) Business Days before the agreed assessment date.

For the avoidance of doubt, any assessment that you wish to reschedule after cancellation shall be deemed a new order subject to a separate charge.

4. Billing

The Service will be billed as a Non-Recurring Fee as described in our Billing Guide.

All commercial considerations will be mutually agreed and documented in your Order Form and/or SoW.

We reserve the right to charge additional fees in the following situations:

(a) Implementation or delivery work carried out outside Business Hours;

(b) Any change in your requirements occurring after the implementation of the Service and outside the scope of the contract (as described in the MSA); and

(c) Any increases to the number of assets reporting into the solution, over and above the agreed contractual limit.

5. Dependencies

We will provide the Service subject to the following dependencies:

5.1 Client Obligations

(a) You will coordinate and arrange time for our consultant to work with members of your organisation to carry out the workshop for the CSM assessment (please refer to section 2.4) on the agreed dates;

(b) You will provide honest and accurate answers to the questions, providing documented evidence where appropriate;

(c) You provide an appropriate physical or virtual environment for the workshop. Where workshops are carried out remotely, you will assure that the technology used to conduct the workshop is available and functions within your environment and for the members of your organisation who will be using this technology;

(d) You are responsible for ensuring all questions are answered during the workshops;

(e) Unanswered questions may be completed by you on the system following the workshop, these must be completed in agreed timescales and understanding of the question must be gained during the workshop;

(f) You are responsible for providing us details of your users for accounts to be set up, enabling access to the CSM tool;

(g) You are responsible to notify us of new users and leavers and to adhere to our password policy;

(h) You are responsible for remediation and resolution of identified actions and activity. We can provide assistance for such remediation or resolution upon request as part of a separate professional services or managed service engagement (subject to an additional Fee), and;

(i) If you require any change(s) to the scope of your Service, you must raise your request before the Ready for Service date.

6. Exclusions

Systems, services or requirements outside of those agreed as part of the Service Delivery activities and not defined in this Service Description are excluded from the scope of the Service. You can request the addition of systems, services and requirements at any point during the contracted term, in accordance with the change request terms of your MSA. Please note that this change will require additional professional services and/or managed service(s) engagements, which we will charge separately.

7. Definitions and Acronyms

7.1 Definitions

In this document “we” or “us” refers to the Supplier, and “you” refers to the Client.

The terms listed have the following meanings:

Term	Meaning
Assessment	The information gathering and processing for your organisation during the workshops.
Business Continuity	Measures taken to minimise the impact of external influences on the core operation of the business
Compliance Regime	Conforming to a rule, such as a specification, policy, standard or law.
ISO/IEC 27001:2013	International Standards Organisation (ISO) 27001 is the international standard for information security.
NIS Directive	Networks and Information Systems Directive https://www.ncsc.gov.uk/collection/caf/nis-introduction
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework (CSF) https://www.nist.gov/cyberframework
NIST 800-53	National Institute of Standards and Technology Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organisations.
Security Domains	High level name which encapsulates the focus of the benchmark questions.
Standard Change	A change that can be introduced to maintain smooth running or operation of the system.
Statement of Work	A document which defines project-specific or client-specific activities, deliverables and/or timelines for providing services to that client.
Tier 1 Supplier	Tier 1 supplier is a directly contracted supplier. Tier 1 suppliers are commonly assessed with contracts, initial assessments and/or questionnaires, but following the initial work are then typically forgotten and their Cyber Security posture and maturity is not tracked.

Tier 2 Supplier	Tier 2 – suppliers to the Tier 1 suppliers. Tier 2 suppliers tend not to exist with the parent organisation; therefore, no contracts (demanding a cybersecurity framework) exist or are not considered.
Workshop	The actual session held with your organisation.

7.2 Acronyms

Acronym	Meaning
COBIT	Control Objectives for Information and Related Technologies
CSM	Cyber Security Maturity
HR	Human Resources
ISO	International Organisation for Standardisation
IT	Information Technology
MSA	Master Services Agreement
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
NIST CSF	National Institute of Standards and Technology Cyber Security Framework (CSF)
SoW	Statement of Work