Service Definition Document

James Martin MSc CISM
Lead SOC-CMM assessor for Maple and Oak Consulting Ltd
www.mapleoakconsulting.co.uk

Introduction

Service Overview

Why Maple and Oak Consulting Ltd?

- Boutique consultancy concentrating on Cyber Operations Assessments
- Extensive experience in the UK and RoW building, maturing and assessing Cyber Security Operation Centers
- Provide SME remediation capability to support CSOC on their maturity journey
- The team have developed a repeatable process using the SOC-CMM methodology to produce your report and presentation in six weeks from the start of the assessment
- Service Features:
  - Maturity Assessment aligned to NIST
  - Maturity and capability score for each Domain
  - Results are scored across 26 function areas
  - The final report contains clear remediation actions
  - Remediation resource is offered on a T&M basis
  - Process should take no more than 6 weeks from approval

SOC Maturity Model Assessment

- Maple and Oak Consulting Ltd use the Open-Source SOC-CMM tool to carry out all assessments.
- James Martin is an accredited SOC-CMM assessor.
- Elisha Quaye is an accredited SOC-CMM assessor.
- The model was initially created as a scientific research project to determine characteristics and features of SOCs, such as specific technologies or processes. From that research project, the SOC-CMM has evolved to become the standard for measuring capability maturity in Security Operations Centres. At the core of the assessment tool lies the SOC-CMM model.
- This model consists of 5 domains and 26 aspects, that are each evaluated using a number of questions. The domains 'Business', 'People' and 'Process' are evaluated for maturity only, the domains 'Technology' and 'Services' are evaluated for both maturity and capability.
- The model can be found here SOC-CMM
- The SOC-CMM assessment tool is free software, released under the CC SA-BY licence.

SOC-CMM Advanced Assessment

The aim of the assessment is to gain insights into the strengths and weaknesses of the CSOC under assessment. The SOC is assessed by its Maturity Level and its Capability Level.

The 6 levels of SOC-CMM Maturity Score	
0	Non-existent
1	Initial
2	Managed
3	Defined
4	Quantitatively managed
5	Optimising

The 4 levels of SOC-CMM Capability Score	
0	Incomplete
1	Performed
2	Managed
3	Defined

SOC-CMM Advanced Assessment - Result by Domain

Domains

Business Drivers

- Is the SOC aligned with what the business assets in needs to protect

People

- Does the SOC have a training programme and a defined talent process in place

Process

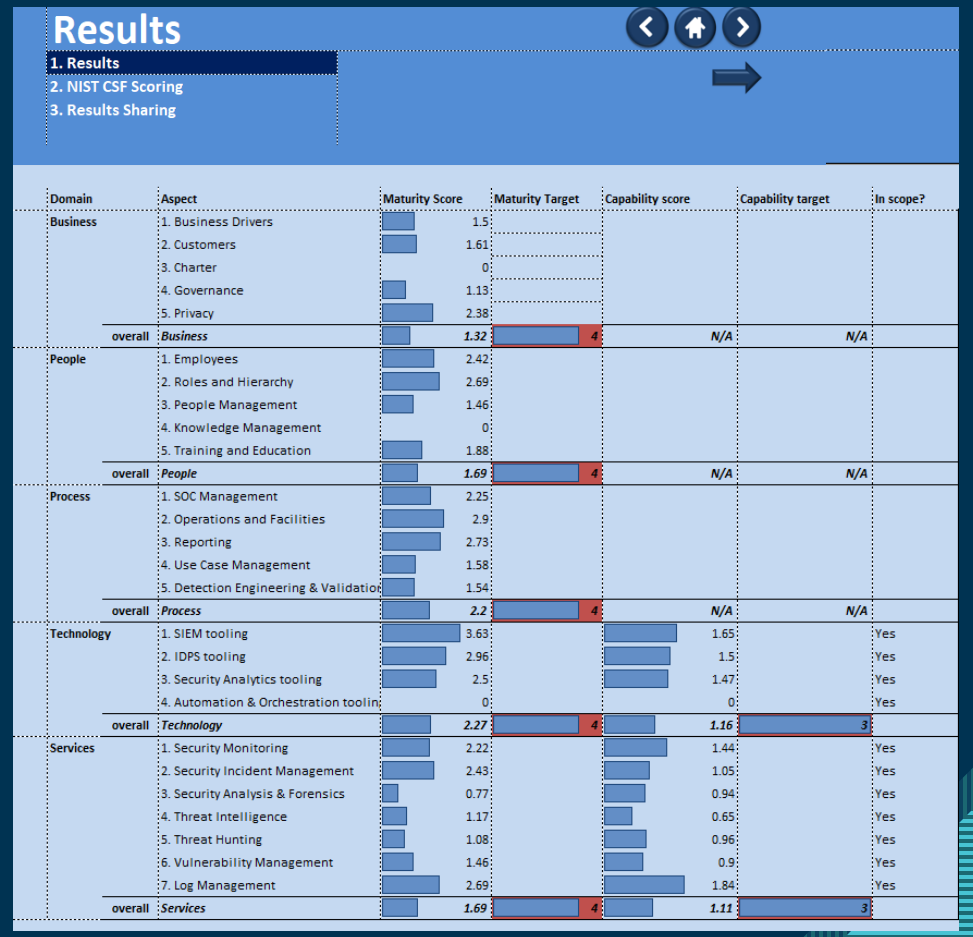
- Are SOC management process in place, are SOC services supported with documented processes

Technology

- Are Security tools configured and alerts triaged in a timely manner

SOC Services

- Is a description in place for each service and indicators to measure performance and quality.

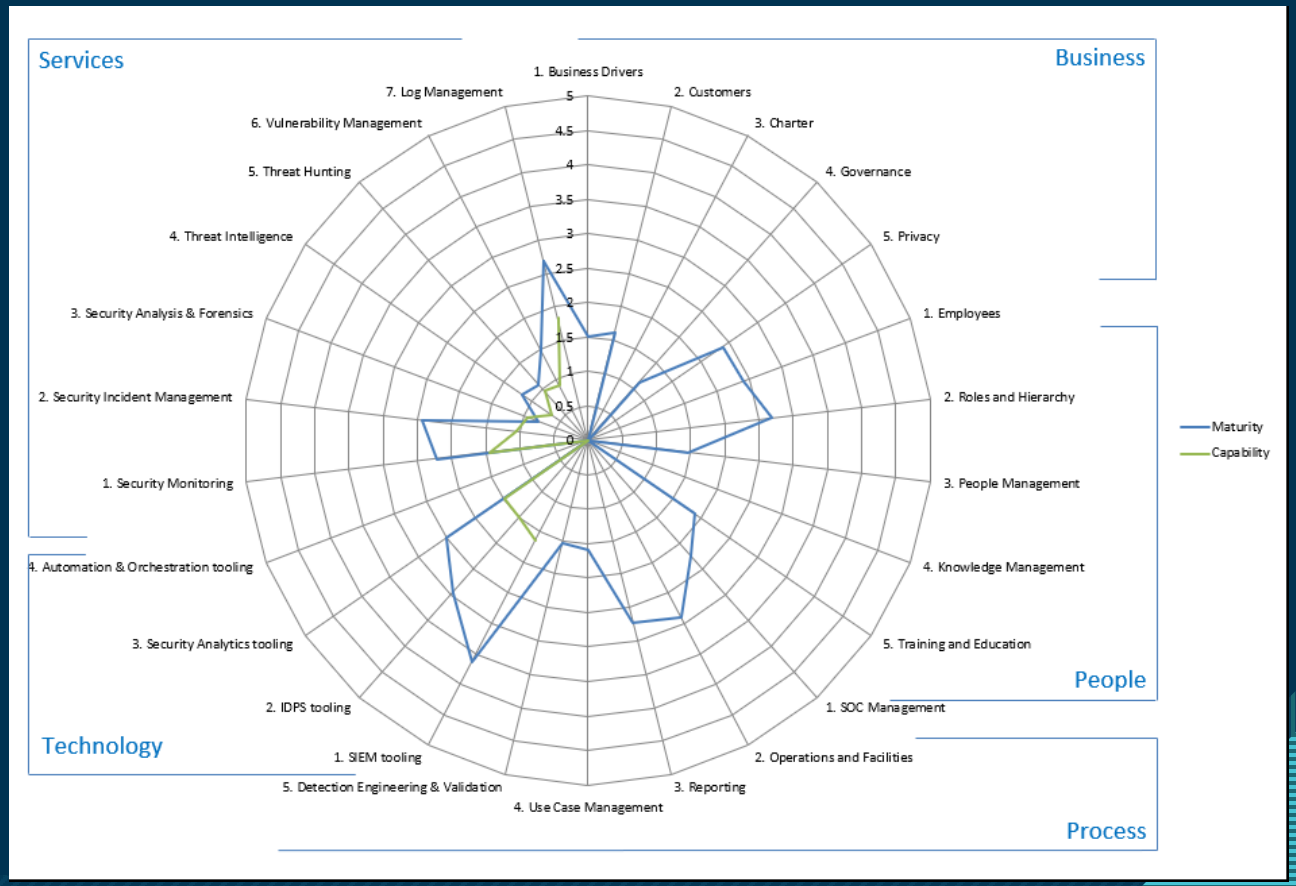


Domain	Aspect	Maturity Score	Maturity Target	Capability score	Capability target	In scope?
Business	1. Business Drivers	1.5				
	2. Customers	1.61				
	3. Charter	0				
	4. Governance	1.13				
	5. Privacy	2.38				
overall	*Business*	*1.32*	*4*	*N/A*	*N/A*	
People	1. Employees	2.42				
	2. Roles and Hierarchy	2.69				
	3. People Management	1.46				
	4. Knowledge Management	0				
	5. Training and Education	1.88				
overall	*People*	*1.69*	*4*	*N/A*	*N/A*	
Process	1. SOC Management	2.25				
	2. Operations and Facilities	2.9				
	3. Reporting	2.73				
	4. Use Case Management	1.58				
	5. Detection Engineering & Validatio	1.54				
overall	*Process*	*2.2*	*4*	*N/A*	*N/A*	
Technology	1. SIEM tooling	3.63		1.65		Yes
	2. IDPS tooling	2.96		1.5		Yes
	3. Security Analytics tooling	2.5		1.47		Yes
	4. Automation & Orchestration toolin	0		0		Yes
overall	*Technology*	*2.27*	*4*	*1.16*	*3*	
Services	1. Security Monitoring	2.22		1.44		Yes
	2. Security Incident Management	2.43		1.05		Yes
	3. Security Analysis & Forensics	0.77		0.94		Yes
	4. Threat Intelligence	1.17		0.65		Yes
	5. Threat Hunting	1.08		0.96		Yes
	6. Vulnerability Management	1.46		0.9		Yes
	7. Log Management	2.69		1.84		Yes
overall	*Services*	*1.69*	*4*	*1.11*	*3*	

SOC-CMM Advanced Assessment - Domain Visualisation

A visualisation is created for the 26 aspects of the assessment

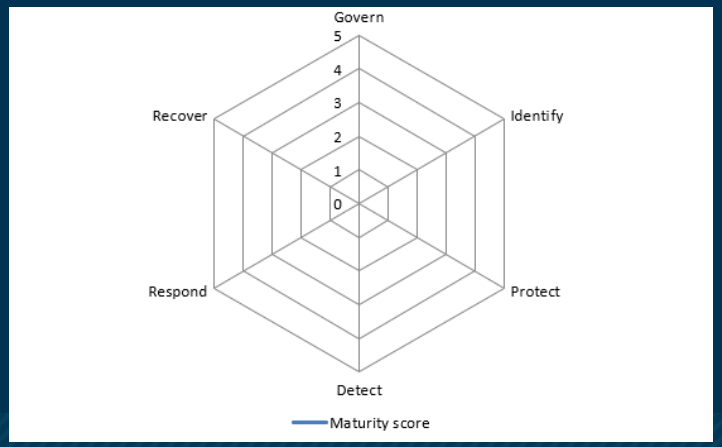
- Maple and Oak Consulting Ltd suggest a maturity level of 4 should be the aim.
- The example depicts each aspect and the relevant score.
- The final report will suggest remediation work to improve each aspect to reach the maturity level of 4 or above



SOC-CMM Advanced Assessment - Results by NIST

The majority of Government departments rely on the NIST framework to assess their cyber readiness

- Organisations that have undertaken a Cyber Maturity assessment using the NIST CSF framework for example reviewing top five key services can now use the same framework to align their protective monitoring capability.
- The model has been updated to use the CSF 2.0 framework as seen below



Results

1. Results
2. NIST CSF Scoring
3. Results Sharing

NIST CSF 2.0
NIST CSF 1.1

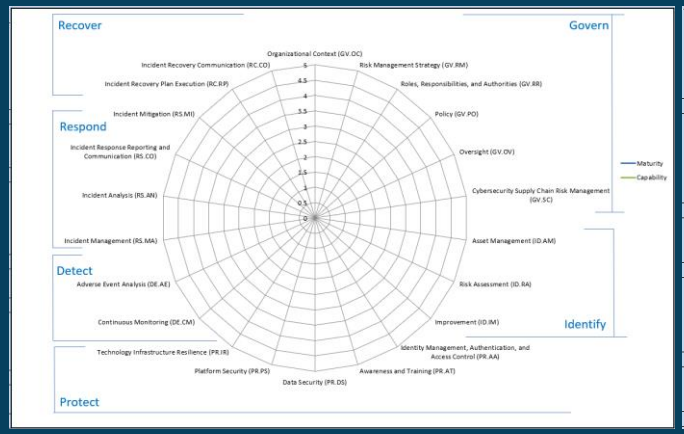
Domain		Aspect	Maturity Score	Capability score
Identify		Asset Management (ID.AM)	2.31	N/A
		Business Environment (ID.BE)	1.03	N/A
		Governance (ID.GV)	1.94	1
		Risk Assessment (ID.RA)	2.3	0.73
		Risk Management Strategy (ID.RM)	2.5	N/A
		Supply Chain Risk Management (ID.SC)	N/A	0.75
	overall	*Identify*	*2.02*	*0.83*
Protect		Access Control (PR.AC)	2.88	0.94
		Awareness and Training (PR.AT)	2.34	0
		Data Security (PR.DS)	2.02	0.94
		Information Protection Processes and Procedures (PR.I	1.95	0.6
		Maintenance (PR.MA)	2.33	0
		Protective Technology (PR.PT)	2.5	0.75
	overall	*Protect*	*2.34*	*0.54*
Detect		Anomalies and Events (DE.AE)	3.75	1.35
		Security Continuous Monitoring (DE.CM)	5	1.38
		Detection Processes (DE.DP)	2.23	1.67
	overall	*Detect*	*3.66*	*1.47*
Respond		Response Planning (RS.RP)	0	0
		Communications (RS.CO)	4	1.44
		Analysis (RS.AN)	0.63	0.61
		Mitigation (RS.MI)	0	1.5
		Improvements (RS.IM)	1.25	0.38
	overall	*Respond*	*1.18*	*0.79*
Recover		Recovery Planning (RC.RP)	N/A	N/A
		Improvements (RC.IM)	N/A	N/A
		Communications (RC.CO)	N/A	N/A
	overall	*Recover*	*N/A*	*N/A*

SOC-CMM Advanced Assessment – NIST Visualisations

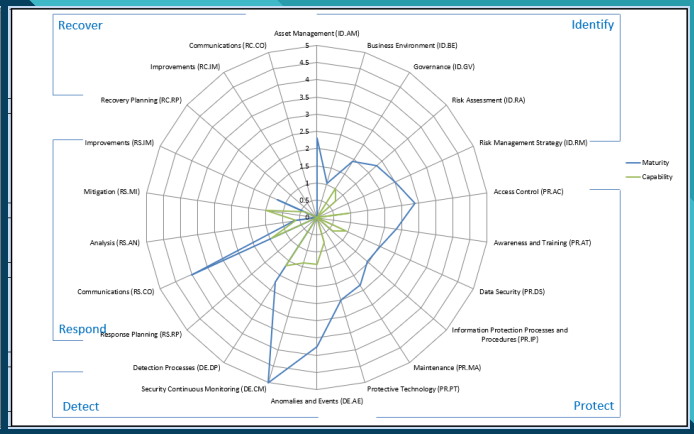
A visualisation is created for the NIST Functions

- A visualisation maps the scoring for both the maturity level of the CSOC and the Capability of its technology and services.
- This representation allows the reader to quickly assess issues and perform a gap analysis

NIST CSF 2.0



NIST CSF 1.1

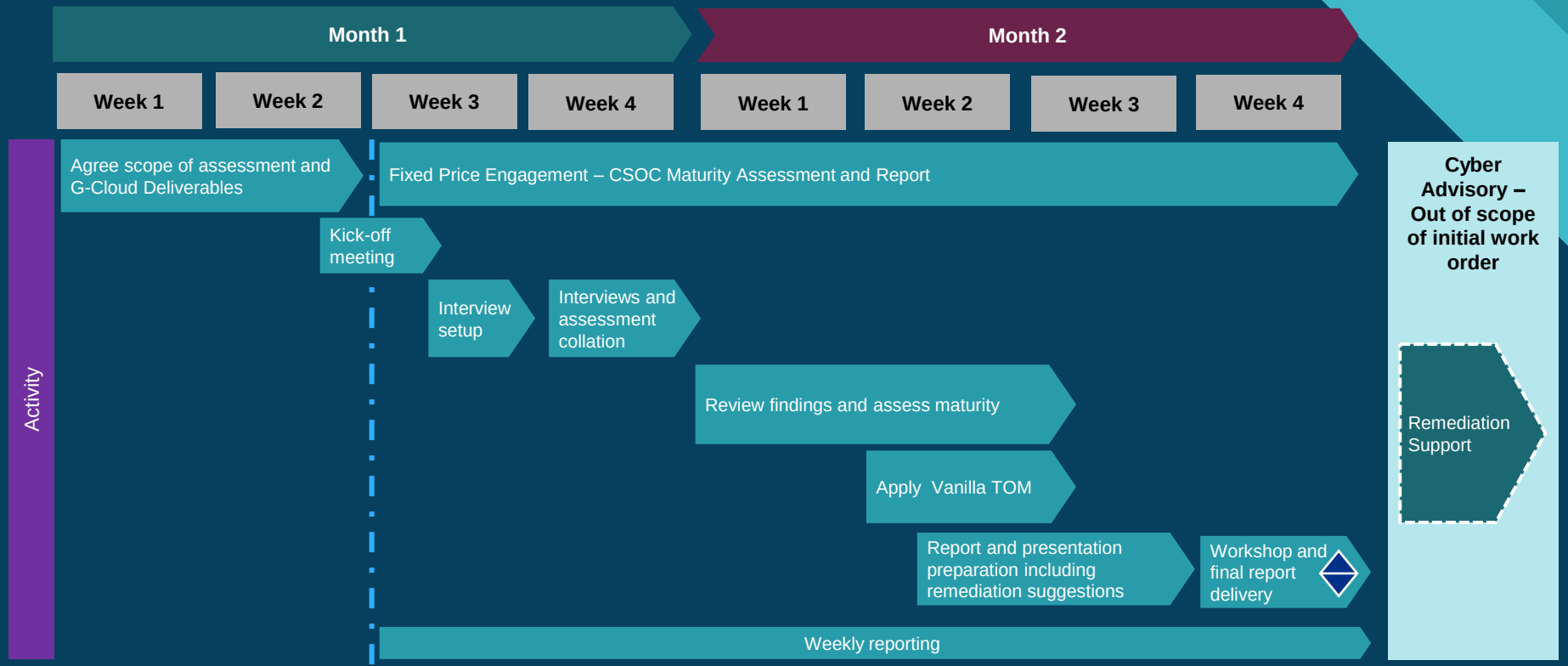


SOC-CMM Advanced Assessment – Final Report

Final report includes a verbal brief and next steps discussion as part of the fixed price assessment

- Final Report Structure will be discussed with the client before completion, a standard report includes:
  - Breakdown by domain of findings and remediation actions
  - A target operation model graphically showing areas that could be improved broken down as quick wins, medium and long-term activity
- A presentation and half day workshop allowing the CSOC to agree next steps. Actions from this session will be added as an annex to the final report.

Generic Project Plan



Key Deliverables

1) Planning and Mobilisation	2) Customer Engagement	3) Assessment	4) Report and workshop
1.1 Agree scope and allocate sufficient resources **1.2** Agree stakeholder groups to be interviewed	**2.1** Conduct stakeholder interviews to understand current maturity. This may lead to secondary interviews	**3.1** Apply Maturity model to findings and assess scores **3.2** Create visualisation of TOM **3.3** Develop recommendations	**4.1** Report write up, outline findings and subsequent recommendations **4.2** Chair workshop

Key:
Project Activities
Project Phases
Workshop

Maple and Oak Consulting – Cyber Operations Advisory

The Team

Assessment timeline

James Martin - MSc CISM. Lead Assessor, Cyber Advisory

James, a part-time Associate at one of the “Big Four” consultancies and a retired British Army officer, has over 20 years’ experience in cyber operational transformation leadership roles, in and out of the military. He brings experiences in cyber security transformation, CSOC maturity assessment, cyber risks assessment, security incident management, cyber projects and programmes governance. He also has comprehensive experience in building and running Cyber Security Operations Centres (CSOC) in both the public and private sector across the globe.

Academic and Professional Highlights

- MSc Design of Information Systems
- BSc (Hons) Software Systems
- Certified Information Security Manager (CISM)
- Managing Successful Programmes Practitioner
- Management of Risk Practitioner
- ISO27001 Foundation
- AZ900 Azure Foundation
- SC900 Identity and Access Management
- Open Group - Architecture Foundation (TOGAF)
- Open Group - Risk and Security
- Clearance level DV

Dept Environment Food and Rural Affairs: Cyber Security Operations Centre Development Manager

Led on cyber security strategy definition and procurement and implementation of a new Security Platform

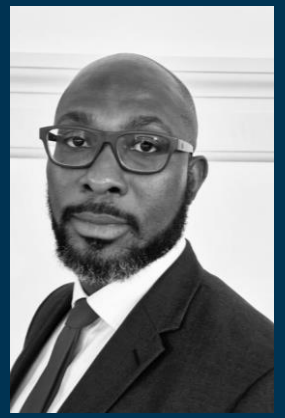
Home Office, Live Services: Cyber Security Operations Centre Manager

Led the implementation and maturity of HO CSOC, from SOC strategy definition, tooling and building relationship with other government agencies and third-party suppliers.

Saudi Arabia: SOC Operations Associate Director

Cyber capability development (TOM, Security Uses case, Security tooling) with SOC-CMM assessments model

Elisha Quaye - MSc. Business Systems Analysis & Design. Assessor, Cyber Advisory



Elisha, an experienced IT consultant with over 13 years' experience in both the private and public sectors. He has been part of a team delivering multiple IT transformation programmes and projects on security systems and tooling implementation, cyber maturity assessment, security incident management, as a lead business analyst and CSOC consultant in both private and public sector. His professional approach, diligence and unfailing positive mindset have helped in the delivery outcome to clients such as UK Home Office, NCA, National Highways, EQ Financial Services and AIG Group.

Academic and Professional Highlights

- MSc. Business Systems Analysis & Design
- BSc (Hons) Business Enterprise
- ITIL Foundation Certificated (V.3)
- Certificate in Cybersecurity - CC (ISC2)
- Security Plus
- TOGOF 9.2
- PRINCE2® Foundation and Practitioner
- Open Group - Risk and Security

National Highways – Lead Security Business Analyst

Performing SOC maturity assessment against NIST framework to identify gaps and level of security maturity. Support the definition of SOC services and implementation of tooling for effect security monitoring. Defining requirements all tooling implementation.

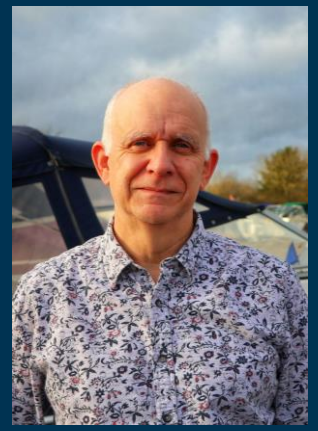
Home Office – Lead Security Business Analyst

Support definition, analysis and delivery of protective security monitoring solution for HO technology platforms. Project aimed at providing proactive security monitoring solution across the HO estate.

EQ Financial Services – Lead Business Analyst

Establishing process centre of excellence (PCoE) to ensure regulatory compliance with UK FCA requirements.

Geoff Young - BSc (Hons) Microsoft SME Supporting Remediation Work



With a first-class heritage in the information technology industry spanning more than forty years, Geoff offer a unique set of integrated digital skills combining technical analysis, solution architecture, project management, multi-disciplined technical consultancy.

In his most recent role he was part of the NHS England National CSOC working closely with the team since formation to provide expertise in Microsoft cyber security technologies.

Academic and Professional Highlights

- BSc (Hons) Chemistry
- Azure Hybrid Cloud Foundation
- Microsoft Certified Systems Engineer
- Windows XP Instructor

NHS England – Microsoft Defender XDR specialist

Acknowledged Microsoft Defender XDR expert working at NHS England to deliver deep technical skills into NHS Trusts, Integrated Care Boards and various arms lengths bodies. Working closely with Microsoft Product Engineering teams as a design partner, testing new capabilities, providing detailed feedback and de-risking adoption.

Microsoft UK – Senior Engagement Manager

Managing a portfolio of consultancy services engagements to UK Central Government customers, including Defence and Police Services. Highly customer facing role working with very demanding stakeholders/execs. Leading and managing exceptional specialists in small teams to deliver outstanding results.

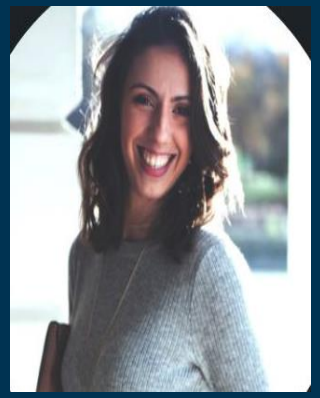
Fujitsu Services – Senior Project Manager

Freelance professional managing several disparate work streams for a Technology Refresh Programme at UK Central Government Directorates.

National Westminster Bank – Various roles

Microsoft Windows Platform and Infrastructure specialist, Database specialist, SAP R/3 development and support, 370 Assembler Programmer

Anna-Maria Stavrakellis, Project Manager



Anna-Maria, has over 10 years' experience in the project/programme manager space. She bring a wealth of industry knowledge in both the private and public section, ensuring effective use of various project/programme management methodologies to support effective governance on all projects. She deployed these skills and experience in providing the required governance to successful deliver CSOC maturity assessment for clients.

Academic and Professional Highlights

Home Office - Project Manager

Project managing CSCO maturity assessment phase and asset discovery and onboarding of system into the Cyber Security Operations Centre (CSOC) for protective monitoring

BEIS – Product Owner

Running the Project Management function in a Product Owner role ensuring industry standards are met and projects are moving forward in a timely manner.

Document Control

This proposal is made under the terms of G-Cloud 14 by Maple and Oak Consulting Ltd, a UK limited liability company, a private English company limited by guarantee. The service offering set out in this document do not constitute an offer capable of acceptance until Maple and Oak Consulting Ltd have carried out an evaluation of the client including size and complexity of IT estate. Once complete a specific engagement letter or contract will be sent to the buyer for approval.

Version: 1.0 For Release

Author: J Martin

Date: 1 May 2024

Thank you