

ACME

SASE Navigator Statement of Works

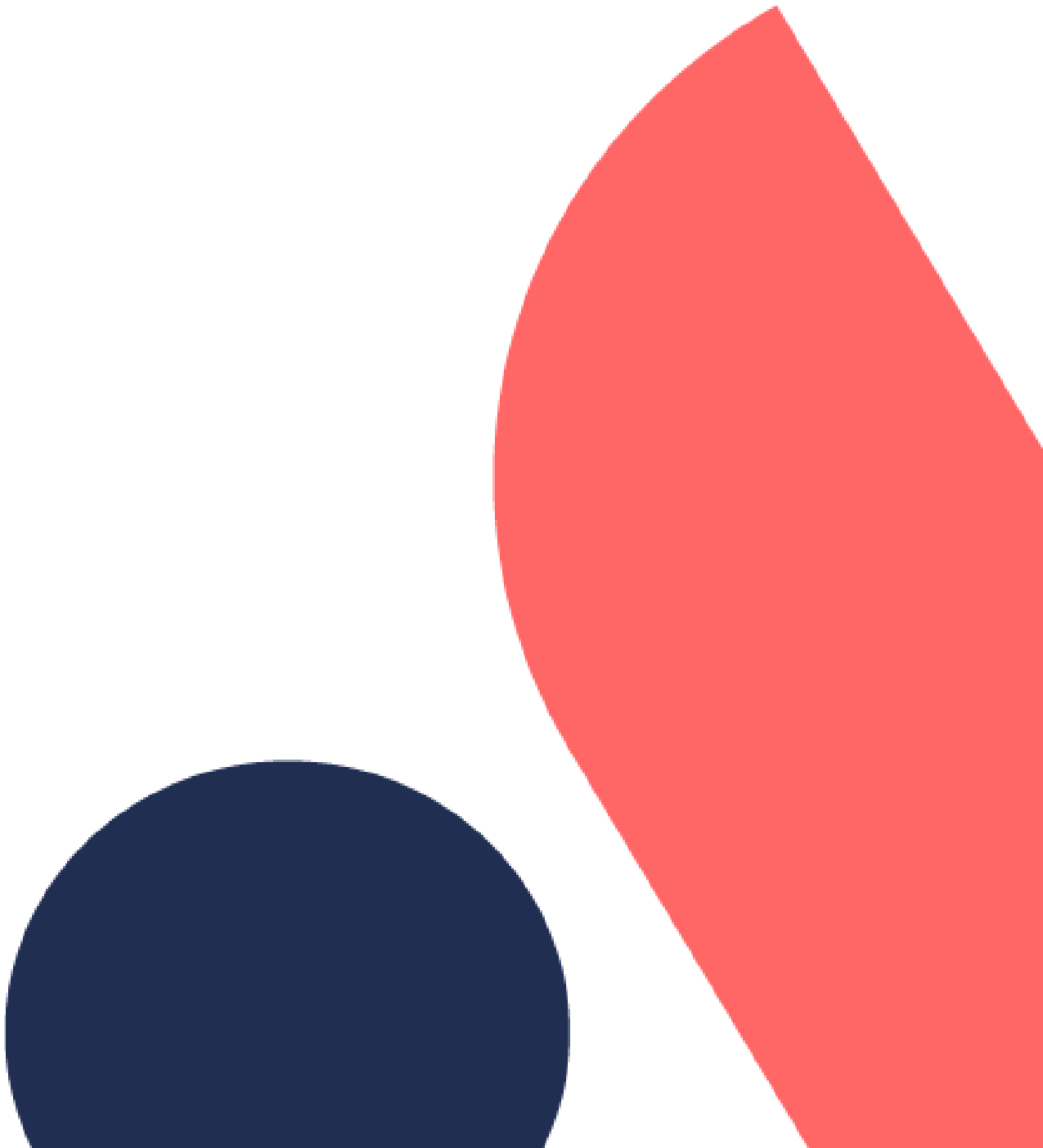




Table of Contents

1.	ISO Document Control	2
2.	Overview	3
3.	Navigator Scope	5
3.1.	SASE Products Assessment	5
3.1.1.	Connectivity – SDWAN	5
3.1.2.	Connectivity – Secure Web Gateway	6
3.1.3.	Connectivity – Firewall as a Service	6
3.1.4.	Connectivity – Cloud Access Security Broker	6
3.1.5.	Zero Trust Network Access	7
3.2.	Gap Analysis	7
3.3.	Navigator Deliver Process	8
3.3.1.	Pre-Requisites	8
3.3.2.	Workshop 1 – Security and Connectivity Strategy and Foundations	8
3.3.3.	Workshop 2 – Target Architecture	9
3.3.4.	Workshop 3 – Business Case Presentation and Case for Change	9
3.3.5.	Expected Output	10
3.4.	SASE Maturity Model	11
3.5.	Operational assessment	11
3.6.	Migration and adoption	11
3.7.	Cost Analysis and Business Case	11
3.8.	Operating Model	13
3.8.1.	Existing Operating Model	13
3.8.2.	Desired Operating Model	13
4.	Solution Architect Stage Plan	14
5.	Service Descriptions and Prerequisites	16
6.	Assumptions & Exclusions	18
7.	Customer Information	18
7.1.	Address / Site details	18
8.	SoW Acceptance	19



One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676



1. ISO Document Control

Document Control

Document Name	ACME – SASE Navigator Statement of Works
Date Originated	20/04/2024
Status	00.1
Document Owner	
Approved By	Ian Warburton
Next Planned Review Date	TBC

Version Control

Date	Version
20/04/2024	First Draft – 00.1

Document Team

Name	Role	Email
------	------	-------

Distribution List

Name	Role	Email
------	------	-------



One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676



2. Overview

Secure Access Service Edge (SASE) combines advanced networking, client connectivity, security, and observability capabilities, delivering secure access to any application, over any network, anywhere users work.

SASE is about connecting both the on-prem and off-prem users to applications more efficiently, by consolidating security and connectivity services and bringing them closer to the user. Connectivity is a key component of the framework to reduce hop count, reducing latency, which ultimately allows our customers to improve their user's experience. SASE integrates Software Defined networking, security and application visibility with advanced interconnection solution that enables seamless, on-demand and direct access to multiple clouds, across multiple networks, to multiple resources, across the globe. It enables access to any application, over any network, anywhere users work, elevating their cloud experience in respect to latency, security, and performance.

ACME have engaged with ANS to carry out a SASE Navigator assessment to help them understand where they are in the SASE maturity Framework and how they can adopt and migrate to a SASE based approach to implementing converged connectivity and security across the business. ANS will perform a comprehensive assessment on ACME's current connectivity and security posture across all technologies and solutions that are defined in the SASE architecture framework. The ANS managed SASE framework for cloud delivered security and connectivity is illustrated below:



ANS will review ACME's existing security and connectivity capabilities and align these to a SASE adoption strategy that can be implemented at ACME 's own pace. ANS will assess the technology currently deployed by ACME and gain an understanding of the operational model currently in use. Each [pillar of the SASE architecture framework will be assessed in detail and will result in an architecture framework roadmap that will clearly detail ANS' recommended approach to SASE adoption and migration. ANS will assess the technology and operational efficiency currently deployed by ACME across the following areas:



One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676



- Connectivity – Software Defined Networking
- Cloud Access Security Broker
- Remote Access
- Application Firewalling and Firewall as a Service
- Secure Web Gateway (forward proxy)
- Secure application access

ANS will assess the current management model deployed by ACME for each area and will review their cloud strategy. ANS will review ACME's readiness for adopting cloud delivered security and gain an understanding of the current security policies in place.

ANS will work with ACME to understand their business and technical objectives and to gain a clear understanding of their strategic connectivity and security roadmap, how applications will be consumed in the future, where these will be hosted and how users remotely access these. ANS will assess the working practises of ACME in terms of where users access applications from, the locations from which they usually work and what the current levels of user experience are. ANS will also review the connectivity and security technology currently in place and assess the levels of integration that are currently in place. This will include access to SaaS and 3rd party application providers or connectivity to partners and suppliers.

The objective of this assessment is to provide ACME with a high-level view of the following themes consistent with connectivity, security, cloud and digital:

- Efficiency
- Target Architecture and SASE adoption framework
- Security and Risk
- Target Operating Model

These themes will provide the best high-level approach to provide ACME with the necessary information to make a decision on the suitability of adopting some or all the SASE technologies across the organisation and will detail how to make best use of the integrated management capabilities to deploy security and connectivity policies centrally across the network for all users.

ANS will align the output of the Navigator for converged cloud and security architectures to support the business objectives and outcomes to consume business applications and services residing in the cloud, whether that be legacy on-premises, IaaS, PaaS and SaaS.



One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676



3. Navigator Scope

ANS have developed the Navigator process to include a comprehensive scope for assessing ACME's connectivity and security environment so they can build a technical and operational roadmap that can be adopted at a pace to suit the business. ANS will build a Target Architecture that ACME can use for adoption. The Target Architecture will build any technology that is currently in place or has been recently invested in and deliver a clear and concise maturity model that will help ACME adopt and gain value from building a strategy based on this integrated framework.

ANS' Connectivity Solutions Architect will follow a structured methodology reviewing each SASE technology area under the pillars of:

- Efficiency
- Architecture
- Application Access
- User access (including identity and endpoint security)
- Security Posture – Application, user, cloud etc.
- Operating model
- Case for change/adoption.

The following sections highlight details covered in the assessment under the key SASE technology areas:

3.1. SASE Products Assessment

3.1.1. Connectivity – SDWAN

SD-WAN provides secure, optimized, deterministic, reliable connectivity among offices, and data centres via multiple PoPs with central management. SD-WAN services are becoming smarter. They no longer have basic features related to MPLS replacement but also provide user & application-aware routing/QoS, SaaS acceleration via intelligent routing, WAN optimization & caching for low latency access to redundant data, and even basic security services such as NAT, Firewall and VPN.

ANS will discuss LMU's business objectives and strategy. These will be aligned to the Connectivity Navigator, to ensure that all activities are consistent in delivering on the required outcomes.

As part of the SASE Navigator assessment, ANS will review the following key areas:

- Review of existing WAN implementation
- Hardware/Software lifecycle review
- Current strategic vendor alliance across network – WAN/Campus and cloud
- Existing Connectivity to site branches
- Existing Connectivity to cloud (private or public)
- Review of network traffic path flows
- Review of critical application connectivity – SaaS and Private
- Existing cost analysis
- Remote Access connectivity for hybrid/remote workers



One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676



The output of the connectivity section will include SASE integration review highlighting how the current network could be integrated or replaced with a SASE based solution. All sites will be reviewed for available connectivity and ANS will present a connectivity report detailing the availability of connectivity across our Tier One carriers. In addition, ANS will develop a integrated secure Connectivity Target Architecture that will align to ACME's business and technical objectives. This will be integrated with the SASE output that will be presented back to ACME.

3.1.2. Connectivity – Secure Web Gateway

SWG functionality protects Enterprise client assets while accessing Internet. It stops users from visiting bad sites that host malware and social engineering sites that steal passwords. It also stops users from downloading or uploading malware content. SWG does this by including URL malware filtering and Anti-malware functions. SWG also offers identity-based URL filtering feature to provide differentiated access to Internet services based on user group/role.

As part of the SASE Navigator assessment, ANS will review the following key areas:

- Existing proxy services in use
- How hybrid and corporate users are protected when accessing the internet
- Security policy management and deployment
- Review traffic inspection points.
- Access to private applications hosted in cloud – public or private.
- Policies and management of existing proxy services
- Cost analysis

3.1.3. Connectivity – Firewall as a Service

Firewall as a Service (FWaaS) is the cloud-based delivery of firewall functionality to protect non-web Internet traffic. In addition to layer 3-4 filtering, FWaaS typically includes features for intrusion prevention and application-level visibility and control. FWaaS provides cloud delivered firewall services without the need to deploy, maintain, and upgrade physical or virtual appliances at a site

As part of the SASE Navigator assessment, ANS will review the following key areas:

- Existing perimeter firewall architecture design
- Cloud security
- Firewall scaling (public or private)
- Current firewall updates and patching process
- Review of existing of regulatory compliance
- Process for adapting security for new attack vectors.
- Cloud hosted application security

3.1.4. Connectivity – Cloud Access Security Broker

CASB functionality protects Enterprise data in SaaS Services by ensuring that genuine users are accessing the allowed resources. More importantly, it provides visibility on users and resources being accessed. CASBs also help in stopping access to unsanctioned SaaS sites. Since CASBs are coming in the way of traffic, they also can identify any shadow IT accesses and identify if there are any data leaks between corporate accounts and personal accounts. Some SaaS vendors don't recommend inline security. To address security requirements of Enterprises for these SaaS services, API- level CASBs are expected to be present in the SASE solution. API-



One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676



level CASBs work with SaaS provider APIs to automate privileges and to scan content for any malware and data (sensitive, PII) leaks.

As part of the SASE Navigator assessment, ANS will review the following key areas:

- Review of current SaaS applications used by ACME
- Review of security of SaaS applications
- Review Data Loss Prevention strategy.
- Review of shadow IT policies and security.
-

3.1.5. Zero Trust Network Access

ZTNA functionality protects Enterprise applications and associated data. SD-WAN services have basic ZTNA functionality via VPN & stateful inspection firewall. That is not sufficient to call it ZTNA in SASE architecture. ZTNA functionality includes identity-aware application access, user role-based granular access to applications to address "least privilege access" principle, traffic Engineering to multiple instances of the application across clouds & data centres, privileged access management to critical services, and more. Differentiated ZTNA frameworks are augmented with WAF (Web Application Firewall), API security, DLP (Data Loss Prevention) and Anti-Malware functionality for both threat protection.

As part of the SASE Navigator assessment, ANS will review the following key areas:

- Application access by corporate office
- Application access by hybrid/remote corporate users
- Application access by 3rd party or BYOD users
- Identity provider currently used and current policies defined
- Secure network access for endpoints and users
- Review of encryption in place and Policy Enforcement points

3.2. Gap Analysis

ANS will perform a Gap Analysis on the existing security and security environment against a potential SASE architecture framework. The Gap Analysis will assess where ACME is today and will consider where ACME needs to be from a technical and business perspective. The GAP Analysis will detail where the gaps lie in reaching the target architecture state.

As part of the SASE Navigator assessment, ANS will review the following key areas:

- Current SDWAN or connectivity state
- Current application security posture
- Current user and endpoint security
- Identity
- Firewall security installed in the network and in the cloud
- Existing management platforms
- Policy deployment



One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676



3.3. Navigator Deliver Process

As part of the SecOps Navigator, the ANS Security Solution Architect will perform series of workshops and assessments for ACME to gain an understanding of their current security landscape. We will review the existing security architecture and its capability to support a transition to cloud and digital in line with ACME business, technical & security strategy. ANS will work with ACME to understand their business objectives and to gain a clear understanding of ACME's strategic IT roadmap, in particular how applications, services, end users, data and infrastructure will be secured, protected and compliant in the future.

3.3.1. Pre-Requisites

ANS require the following baseline pre-requisite information in order to complete the Navigator and streamline the process:

- WAN sites and address details
- Check Connectivity pre -reqs.....

ANS will create an external Teams channel for the Navigator and this will enable communications and provide a documentation repository.

3.3.2. Workshop 1 – Security and Connectivity Strategy and Foundations

The objective of this workshop is to provide ACME with a high-level view of the following agenda items:

Security Architecture Analysis & Target State Strategy

- Pre-requisite information gathering.
- Workshop 1 - Security Infrastructure Foundation Review & Discussion.
- Understand how security is mapped to your environment.
- Iterate and follow up.

These items will provide the best high-level approach to provide ACME with the necessary information to decide on the suitability of their security architecture and security operations and it's alignment to the business and technical objectives and protects business applications and services residing in the cloud, whether that be legacy on-premises, IaaS, PaaS, and SaaS.

3.3.2.1. ANS Deliverables

The purpose and scope of the Workshop 1 is to review and understand <Customer>'s security strategy and infrastructure suitability for cloud (Private/Public) and digital services. ANS' Security Solutions Architect will follow a structured methodology reviewing areas such as identity, access, zero trust architecture, security infrastructure design and associated costs, resources, risk, compliance and regulatory requirements. There will be a requirement to review the current security operating model.

The information discussed, reviewed and documented in this workshop, will form the basis of the Workshop 2 engagement and will be concluded and appraised in the business case document.



One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676



3.3.3. Workshop 2 – Target Architecture

The objective of this workshop is to provide ACME with a high-level view of the following agenda items:

Security Architecture Definition & Target Architecture

- Pre-requisite information gathering from Workshop 1.
- Workshop 2 - Review Modern security architecture to support security objectives & Strategy.
- Workshop 2 - Define target architecture.
- Iterate and follow up.

These Workshop 2 deliverables will provide the most suitable security architecture and target architecture to provide ACME with the necessary information to decide on the suitability of their security architecture foundation to support ACME's business objectives and for a modern security operations environment.

3.3.3.1. ANS Deliverables

The purpose and scope of the Workshop 2 is to review and understand <Customer>'s defined security requirements and produce a security architecture foundation and a target architecture to support a modern approach to security operations. The areas covered in the second workshop include the following domains:

- SDWAN
- Secure Web Gateway
- Cloud Access Security Broker
- Zero Trust Network Access
- Next Generation Firewalling (FWaaS)

3.3.4. Workshop 3 – Business Case Presentation and Case for Change

The final workshop, and the next stage of the SASE Navigator, outlines the Case of Change based on the findings and recommendations of the assessment workshops. This workstream will use ACME's business, technical and security goals and objectives documented during the workshops to deliver a Target Architecture to fulfil these technical and commercial objectives.

During the Case For Change stage of the SecOps Navigator the ANS Security Solutions Architect will produce a Target Architecture based on the outcomes documented during the Assessment Workshops phase and based on the technical objectives defined by ACME. The Target Architecture will also be based on the commercial review and subsequent assessment of the overall security costs outlined by ACME outlined by ACME during the assessment phase. The ANS Security Solutions architect will produce a comprehensive commercial case for any changes proposed based on our assessment of the market and on a pricing review best practice cloud security reference architecture. This will form a comprehensive business case for that will allow ACME's technical and executive level representatives to present the case for changes to the board of directors or Senior Leadership Teams. The business case presented to ACME will include the following elements:

- Comprehensive Business case illustrating cost savings and overall Total Cost of Ownership (TCO).
- Identification of short term and high impact initiatives that <Customer> can take advantage of.
- Innovative Target Architecture with documented technical and business benefits.



One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676



- Bill of Materials to fulfil the target architecture.
- Managed Service proposal based on the operating model selection.
- Finance options and funding availability.
- Statement of Works to transition to the agreed target architecture.

3.3.5. Expected Output

Once all the information has been gathered from ACME the ANS Solutions Architect and Account Manager will conduct a Case for Change assessment and produce outputs that will be delivered during the assessment workshop meeting review. The expected output from the workshops include the following:

- Present business case to senior stakeholders and executives outlining the Case for Change.
- Present the target Architecture and associated benefits.
- Produce business case output document.
- Deliver a draft Statement of Works that defines the deliverables associated with implementing the proposed solution design.



One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676



3.4. SASE Maturity Model

As part of the SASE Navigator, ACME ANS will develop a SASE maturity model and present it back to ACME against which they can build an adoption roadmap. The maturity model will take into account any existing elements of SASE already in place or any investment made in specific vendors or technology. The maturity model will be based on the following criteria:

- How users connect to critical applications
- Where users are located
- Remote site connectivity and security
- Management tooling to manage and maintain existing network.
- Application security and reporting
- SaaS security and reporting
- Application and network visibility
- User experience monitoring
- The level of application traffic optimisation
-

3.5. Operational assessment

As part of the SASE Navigator assessment, ANS will review the following key areas:

SOC/SIEM

SOAR

EDR/XDR

3.6. Migration and adoption

As part of the SASE Navigator assessment, ANS will review the following key areas:

3.7. Cost Analysis and Business Case

As part of the SASE Navigator assessment, ANS will review the following key areas:

ANS will complete a cost analysis against the current market and vendor technologies using the Single Vendor or Universal SASE models. The following networking architectures will form the basis of the analysis:

- WAN
- Cloud Connectivity
- Cloud Networking and Security Services



One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676



ACME's existing Connectivity operating costs will be assessed against the market rates ANS have access to through our Tier 1 UK and international carrier relationships. ACME's existing security, connectivity and operating costs will be assessed, and a business case produced demonstrating a clear Total Cost of Ownership and, if costs savings are identified, the return that can be expected on any investment made to implement the target architecture.



One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676



3.8. Operating Model

3.8.1. Existing Operating Model

ANS will discuss the following points with view of understanding how the existing network and security functions are supported:

- Organisation/departmental structure
- Network management tooling currently in place for on-premise and cloud environments
- Fault escalation process internally and with 3rd part providers
- Existing Network operations capabilities
- Existing Security operations capabilities
- Existing SIEM in place
- Policy management – Network, users, and endpoints
- What roles and responsibilities are deployed to support the WAN and cloud connectivity environments?
- Current skillsets
- What could be improved and what is done well?

3.8.2. Desired Operating Model

ANS would like to understand the desired SASE operating model once all technologies have been deployed and in the interim whilst migrations are taking place. Through the Navigator process, ANS will discuss the impact, if any, on the existing operating model:

- Is there a desired operating model and what is it?
- Develop and Expand
- The new skills required to provide SASE operations.
- Period of cover for network and security products
- Outsourced managed service.
- Co-Managed service
- What are the desired changes and level of access for co-managed services?
- Are there any timescales to moving to the desired operating model?
- What reporting and service management would be desired – Role based visibility for example



One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676



4. Solution Architect Stage Plan

- **Pre-Stage – Pre-requisites :**
 - Set up external project MS Team.
- **Stage 1 – Meet and Greet :**
 - Define members of the ANS SecOps Navigator team.
 - Define members of ACME's engagement team.
 - Navigator kick-off Meeting (external or virtual Teams).
 - Outline process in detail and explain deliverables.
- **Stage 2 – Assessment Workshop 1 :**
 - Workshop 1 will be held on-site at a convenient location or virtually on Microsoft teams. The following points will be covered:
 - Pre-requisite customer documentation review.
 - Pre-qualification questionnaire run through.
 - Existing hardware, software & license inventory evaluation.
 - Capture strategic business and technical objectives.
 - Create RAG status report on existing challenges and hardware/software/licensing Lifecycle.
 - Review existing security design and topology.
 - Outline guiding principles.
- **Stage 3 – Assessment Workshop 2:**
 - Workshop 2 will be held on-site at a convenient location or virtually on Microsoft teams. The following points will be covered:
 - Present findings on information documented during Workshop 1.
 - Review RAG report.
 - Outline challenges and findings on current security architecture through RAG report.
 - Document business requirements with senior stakeholders.
 - Present draft Target Architecture supporting the business and risk requirements.
 - Present initial technical roadmap recommendations.
- **Stage 4 – Assessment Workshop 3:**
 - Workshop 3 will be held on-site at a convenient location or virtually on Microsoft teams. The following points will be covered:
 - Discuss the outcomes from Workshop 2.
 - Review the security operations reference architecture from the target architecture.





- Review the skillsets required and align to the target architecture.
- Discuss and agree the appropriate security operating model.
- Present commercial review and proposed costs compared to existing TCO.
- Solution Statement of Works.
- **Stage5 – Case for Change:**
 - The Case for Change phase will involve the ANS Navigator team aligned to ACME working on a clear and concise business case that will be delivered to ACME's key Stakeholders and the executive board. The following points will be covered:
 - Review of current overall TCO.
 - Review of any 3rd party management or hardware/software contracts.
 - Presentation of solution design costs based on the Target Architecture.
 - Outline of any specific solution costs savings.
 - Presentation of high-level migration plan.
 - Present commercial and technical benefits associated with Target Architecture.
 - Explain how Target Architecture aligns to key strategic business goals and objectives.
- **Stage 6 – Refine and Transform:**
 - The Refine and Transform phase will involve the ANS Navigator team aligned to ACME making the final amendments required to the solution design in order that it can be signed off by ACME's key Stakeholders and the executive board. The following points will be covered:
 - Present any amendments made during the Case For Change phase.
 - Document how proposed Target Architecture will address specific use cases.
 - Agree key milestones and set timescales.
 - Present Navigator output document.
 - Present final finance options and funding availability.
- **Stage 7 – Sign Off:**
 - The final phase is to agree the actions required for final sign off and handover the outputs from the SecOps Navigator to ACME's project team.





5. Service Descriptions and Prerequisites

The following is an outline of what is and is not provided within this Statement of Work:

- ANS Group requires remote access to the necessary network devices as required for the duration of the project.
 - Usernames
 - Passwords
 - IP Addresses
- LMU to provide their business and technical objectives with regards to the cloud and digital
- LMU to provide full site lists with full postal addresses including postcodes, circuit details (type/bearer/committed data rate) sites to include HQ/Head Office, Datacentres, branches, remote users, Cloud (Azure/AWS/Google)
- LMU to provide the latest up to date WAN schematics or diagrams including information on existing data centres and internet access.
- LMU to provide accurate commercial pricing for existing WAN and Cloud connectivity.
- LMU to provide a full inventory of equipment deployed in the WAN and security infrastructure (Manufacturer/Models/Role).
- LMU to provide an overview on the support and maintenance on the above.
- LMU to provide their Service Provider Reports of current WAN and cloud connectivity – if available
- LMU to provide the latest security report.
- LMU to provide existing design documentation for the:
 - WAN
 - Cloud Connectivity
 - Security Perimeter and Remote Access
- LMU to provide a recent summary of availability and faults for the WAN, security and cloud services deployed for the following time periods:
 - Recent (Last Report)
 - Last 12 Months

LMU to provide access to knowledgeable personnel remotely to discuss findings to further define the output.

What is included within Connectivity Navigator scope?

- Commercial Analysis – WAN/Cloud Environments
- Lifecycle Services Review – Hardware and Software
- High Level Architecture Review
- Security Assessment Review
- Operating Model Review
- Remediation Opportunities
- Connectivity Navigator – Summary Presentation



One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676



Outputs from the Connectivity Navigator include:

- Connectivity Navigator Presentation
- Target Architecture
- Migration Storyboard
- Commercial review – High Level
- Written proposal – If required
- Business Case – if required
- Statement of Works – if applicable



One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676



6. Assumptions & Exclusions

This Statement of Work is delivered as a free of charged engagement by ANS' pre-sales solutions architects. As such, ANS can terminate the engagement at any time subject to LMU not meeting the requirements outlined in this Statement of Work, including aligning to the project plan.

This is delivered free of charge on the assumption that ANS are allowed to share the assessment output to Microsoft as an approved delivery partner for their Integration assessment process.

- All work to be carried out remotely via Microsoft Teams unless agreed otherwise.
- All teams' workshops are required to be recorded.
- All work is to be carried out during normal working hours, Monday to Friday, 9.00am to 5.30pm.
- All required access and permissions to any existing environments are in place.
- It is assumed all network design documentation is available and up to date.
- The Service Definition document agreed between ANS and LMU may be updated following "Stage 2 – Connectivity Navigator Workstream" with any necessary details that are clarified during the planning and design work. LMU will then be required to sign an updated version of the Service Definition document that reflects these changes.
- All pricing is current and complete.
- Any quotation and any subsequent order are based on the scope of work. ANS Group will be pleased to cost any alterations and amendments and submit a new Statement of Works.
- Any vendor discount will be registered against the name of London Metropolitan University
-

7. Customer Information

7.1. Address / Site details

The project will be delivered remotely.

Any visits required will be agreed between the parties.



One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676



8. SoW Acceptance

Accepted on behalf of London Metropolitan University

By signing this Contract, you confirm you accept the Supplier Terms and Conditions located at <http://www.ans.co.uk/site-info/terms-conditions>

Project Title: LMU - Connectivity Navigator Statement of Works

Project Status & Version: First Draft v1

Name: {{_es_:signer2:fullname}} Signed: {{_es_:signer2:signature}}

Purchase Order Number: {{*PONUMBER _es_:signer2}} Date: {{_es_:signer2:date}}

Pre-Sales Confirmation Signature

Signature	{{_es_:signer1:signature}}
Name	{{_es_:signer1:fullname}}
Date	{{_es_:signer1:date}}



One Archway
Birley Fields
Manchester, M15 5QJ

0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk

Co. Reg No. 3176761
VAT No. 245684676