Agilisys

Secure Access Service Edge (SASE) Deployment and Transformation Services

G-Cloud 15 Service Definition

Lot 3 – Cloud Support

Table of Contents

1 Introduction

Agilisys - one of the UK's most innovative cloud and digital transformation specialists, enables organisations to adopt technologies, platforms and processes that promote new ways of working and help organisations transform.

Working for both the public and private sector for over 20 years, we have earned a strong reputation and hold deep domain expertise delivering change and innovation, in particular within local and central government.

Our public sector cloud and IT services have been designed to accelerate cloud adoption and enable our customers to undertake successful, cost-effective transformation.

Our ZTNA services are outcome-driven and designed end to end to enable secure access to applications, data, and services from any location, on any device, while improving resilience, security, user experience, and operational efficiency.

2 Who this Service is For?

This service is designed for UK public sector organisations seeking to modernise network security, remote access, and application connectivity through the adoption of Secure Access Service Edge (SASE) and Zero Trust principles. It is particularly well suited to organisations operating complex, hybrid IT environments that must support a diverse workforce while maintaining high standards of security, resilience, and regulatory compliance.

The service is suitable both for organisations at the early stages of SASE or Zero Trust adoption, as well as those seeking to extend or mature an existing identity or cloud security programme. Engagements can be scoped to support discrete outcomes, such as secure remote access for a specific service area or delivered as part of a broader digital, cloud, or cyber transformation initiative.

We can accommodate varying levels of in-house capability and organisational maturity. Agilisys works collaboratively with internal IT, security, and digital teams to ensure that solutions are appropriate, sustainable, and aligned with existing operating models, governance structures, and statutory responsibilities.

3 SASE Deployment, Migration, & Transformation - an overview

Agilisys provides Secure Access Service Edge (SASE) deployment and transformation services to support UK public sector organisations in modernising network security, remote access, and identity-led access control. Building on extensive experience delivering Zero Trust, Microsoft security, and network modernisation programmes, Agilisys helps organisations replace legacy perimeter-based security models with a modern, cloud native SASE architecture.

Our SASE services are designed to enable secure access to applications, data, and services from any location, on any device, while improving resilience, security, user experience, and operational efficiency. We specialise in deploying Secure Access Service Edge services integrated with Microsoft Entra ID, legacy networks, hybrid cloud environments, and modern workplace platforms.

Our services are modular and scalable, allowing clients to engage us for discrete phases - such as discovery, business case development, or readiness assessments - or for end-to-end

transformation programmes. We combine strategic insight with technical delivery of secure, compliant, cost-effective, SASE adoption, aligned to your organisational goals.

4 Service Description

Agilisys' Secure Access Service Edge (SASE) Deployment and Transformation Services support UK public sector organisations in modernising the way users, devices, and systems securely access applications, data, and services. The service is designed to help organisations transition away from traditional perimeter-based network and security models towards a cloud-delivered, identity-centric architecture aligned with Zero Trust principles and National Cyber Security Centre (NCSC) guidance.

Agilisys delivers a unified approach to secure Internet access, Software as a Service (SaaS) applications, private application connectivity, and identity-driven policy enforcement. The service is particularly well suited to local authorities and other public bodies that operate hybrid estates, support large remote or mobile workforces, and rely on a mix of cloud-hosted, SaaS, and legacy line-of-business applications.

The service recognises that SASE is not solely a technical deployment but a transformation of operating models, access patterns, and security governance, Agilisys provides modular Professional Services that can be consumed independently or combined into an end-to-end SASE transformation programme. As such, the delivery modules encompass strategy, discovery, design, deployment, adoption, and transition to steady-state operations.

4.1 Preparation for SASE

The Preparation for SASE Phase establishes the governance, assurance, and strategic foundations required for the successful adoption of Secure Access Service Edge and Zero Trust capabilities within a public sector operating context. This phase recognises that SASE is not simply a technology deployment, but a shift in how access, trust, and security are governed across an organisation's services, workforce, and digital estate.

Delivery during this phase is intentionally structured to provide confidence to senior stakeholders, ensure alignment with National Cyber Security Centre (NCSC) guidance, the Cyber Assessment Framework (CAF), and reduce risk ahead of technical implementation.

4.1.1 Governance Risk & Compliance

Agilisys' Governance, Risk and Compliance support for SASE adoption builds directly on the principles and assessment approach defined within the NCSC CAF. The service helps public sector organisations understand how the introduction of SASE and Zero Trust controls impacts their ability to protect essential services, manage cyber risk, and demonstrate assurance to regulators, auditors, and senior leadership.

The service begins with a structured assessment of existing governance arrangements, risk management processes, and cyber accountability structures. Particular focus is placed on how access to systems and data is currently governed, how trust decisions are made, and where implicit trust, flat network access, or unmanaged connectivity introduces risk to critical functions. This assessment considers both technical and non-technical factors, recognising that policy, operating models, and decision-making processes are central to effective cyber resilience.

The outcome is a clear, evidence-based view of how SASE and Zero Trust adoption supports improved CAF alignment, alongside a prioritised set of governance and assurance actions that must be addressed ahead of, or alongside, technical deployment.

This service provides:

- A CAF-aligned assessment of governance, risk management, and recovery readiness in the context of SASE and Zero Trust adoption
- Clearly articulated assurance artefacts, including maturity assessments and evidence mapping, suitable for senior leadership and audit audiences
- A prioritised set of governance and policy actions required to safely support SASE implementation and ongoing operation

4.1.2 Zero Trust and SASE Strategy

The Zero Trust and SASE Strategy service translates organisational objectives, cyber risk posture, and CAF findings into a clear and actionable strategic direction for Secure Access Service Edge adoption. This service is designed to ensure that SASE and associated Zero Trust controls are implemented in a way that is proportionate, sustainable, and aligned with public sector service delivery models.

We work collaboratively with your teams to define a target-state Zero Trust architecture that reflects the realities of hybrid estates, legacy applications, and complex user communities commonly found in local government and other public sector bodies. The strategy considers how trust decisions should be made based on identity, device posture, location, and risk, rather than network location, and how these decisions are enforced consistently across internet access, SaaS usage, and private applications.

The resulting strategy provides a clear roadmap for SASE adoption, allowing organisations to sequence delivery in line with risk, readiness, and funding constraints, while maintaining alignment with NCSC Zero Trust principles and broader digital transformation objectives.

This service provides:

- A clearly defined Zero Trust and SASE target architecture
- A phased, risk-aware roadmap for adopting SASE and retiring legacy access models
- Strategic alignment between identity, network security, application access, and wider digital and workforce strategies

4.2 Discovery and Current State Assessment

The Discovery phase provides a structured and evidence-based understanding of the organisation's current cyber security posture as it relates to access, connectivity, and trust. In the context of Secure Access Service Edge and Zero Trust adoption, this phase is designed to ensure that technical and operational decisions are grounded in a clear understanding of existing risks, dependencies, and essential service delivery requirements.

Discovery activities begin with a detailed examination of how users and systems currently access applications and data, including patterns of remote access, third-party connectivity, and inter-system trust. This includes reviewing applications, network architectures, hosting environments, and existing security controls to identify areas of implicit trust, over-privileged access, or flat network designs that increase the potential impact of cyber compromise.

In parallel, we assess your organisation's identity and access management capabilities, with a focus on how effectively access is controlled, monitored, and enforced. Identity platforms, authentication mechanisms, and conditional access controls are reviewed to determine their suitability for supporting Zero Trust and SASE controls. This includes understanding how users, devices, and service accounts are managed, how access decisions are logged, and how deviations from expected behaviour are detected and responded to.

Throughout the Discovery phase, Agilisys works closely with technical teams, security leads, and service owners to validate findings and ensure that evidence collected is accurate, repeatable, and suitable for assurance purposes. Outputs are expressed in a way that directly supports CAF assessment and ongoing governance, rather than purely technical design.

The outcome is a clear and auditable current-state view that underpins subsequent design and implementation phases, reduces delivery risk, and ensures that SASE adoption strengthens, rather than undermines, organisational cyber resilience.

This service provides:

- A CAF-aligned current-state assessment of protection and detection capabilities relevant to SASE and Zero Trust adoption
- A documented view of access patterns, trust relationships, and control effectiveness for services supporting essential functions
- A clear set of evidence-based findings and dependencies to inform secure design, sequencing, and assurance activities

4.3 SASE Architecture and Technical Implementation

Following completion of preparation and discovery activities, Agilisys delivers the SASE deployment through a structured implementation phase. This phase is focused on translating strategic intent, CAF-aligned assurance requirements, and discovery outputs into a working, secure, and operational SASE capability that can be adopted incrementally without disrupting essential services.

Implementation is undertaken in a controlled manner, ensuring that changes to access, connectivity, and security controls are well understood, appropriately governed, and aligned with existing operational processes. The deployment services are modular and can be delivered individually or combined as part of an end-to-end SASE transformation programme.

4.3.1 SASE Architecture and Platform Deployment

Agilisys designs and deploys the core Secure Access Service Edge platform, providing a cloud delivered control plane for secure access to Internet, SaaS, and private applications. The architecture is designed to replace or rationalise legacy perimeter security and network access models while maintaining resilience, performance, and consistency of control across diverse user locations.

The deployment is informed by CAF findings and Zero Trust principles, ensuring that security controls are applied proportionately and in a manner that supports essential services. Platform configuration prioritises resilience, auditability, and visibility, enabling organisations to maintain control and oversight as security enforcement moves from on premises infrastructure to cloud native services. Logging and telemetry are configured to support security monitoring, investigation, and assurance activities from the outset.

Service features include:

- SASE tenant design and baseline configuration
- Secure Web Gateway, DNS protection, and firewall policy implementation
- Centralised logging, reporting, and visibility configuration

4.3.2 SASE Architecture and Platform Deployment

Identity integration is a foundational element of the SASE deployment. Agilisys integrates the SASE platform with Microsoft Entra ID to ensure that access decisions are driven by authenticated identity and contextual signals, rather than implicit network trust. This enables the organisation to consistently enforce access controls across internet access, SaaS platforms, and private applications.

The service focuses on aligning SASE policies with existing identity governance, conditional access, and authentication arrangements. Particular care is taken to ensure compatibility with hybrid identity models, legacy authentication dependencies, and privileged access scenarios common within public sector environments. The approach ensures that Zero Trust access controls are introduced without undermining operational continuity or compliance obligations.

Service features include:

- Entra ID federation and single sign-on integration
- Conditional access and MFA alignment with SASE policies
- Identity-aware access control and session enforcement

4.3.3 Zero Trust Network Access for Line of Business Applications

Agilisys implements Zero Trust Network Access (ZTNA) to replace broad, network-level remote access with application-specific connectivity. This approach ensures that users are granted access only to the applications and services they are authorised to use, significantly reducing attack surface and the potential impact of credential compromise.

Private applications hosted on-premise, in third-party data centres, or in cloud environments are onboarded onto the SASE platform in a phased and controlled manner. Access policies are defined using identity, role, and contextual attributes, and legacy VPN dependencies are progressively reduced or retired. The service is designed to minimise disruption while improving security and user experience.

Service features include:

- Application-level access policy design and enforcement
- Secure connectivity for on-premise and hosted applications
- Controlled reduction or replacement of legacy VPN access

4.3.4 Network Segmentation and Micro-Segmentation

Network segmentation and micro segmentation are implemented to reduce implicit trust and limit lateral movement within the estate. Agilisys uses Zero Trust Network Adapters and policy capabilities to segment access based on application, service, and user context, rather than relying solely on network location or IP addressing.

The service supports the segmentation of critical systems, separation of environments, and controlled third-party access. This is particularly important for local authorities and other public sector bodies that rely on multiple suppliers and shared infrastructure. Segmentation is designed to align with CAF principles by reducing the potential impact of cyber incidents while maintaining operational practicality.

Service features include:

- Application centric segmentation aligned to service criticality
- Isolation of sensitive and essential systems
- Controlled supplier and support access pathways

4.3.5 Secure Internet and SaaS Access Enablement

Agilisys configures the SASE platform to provide secure, policy-driven access to internet and SaaS services for users regardless of location. By moving internet security controls to a cloud-delivered model, organisations can remove reliance on fixed network breakouts and improve both security and performance for remote and hybrid workers.

Policies are designed to reflect public sector usage patterns and data protection requirements, ensuring that access to cloud services is monitored, logged, and controlled appropriately. The service supports gradual adoption across different user groups, enabling organisations to validate controls before wider rollout.

Service features include:

- Cloud-based secure web gateway and DNS filtering
- SaaS access monitoring and policy enforcement
- Location-independent user protection

4.3.6 Modern Workplace Access Enablement

The SASE deployment is designed to support modern workplace delivery by enabling secure access from managed, unmanaged, and bring-your-own devices. Agilisys ensures that access controls reflect device posture, risk, and service sensitivity, allowing organisations to balance flexibility with security.

This service supports a wide range of user scenarios, including home working, mobile staff, elected members, and temporary users. Policies are designed to integrate with existing device management and identity controls, ensuring consistent enforcement without introducing unnecessary complexity.

Service features include:

- Support for managed and unmanaged device access
- Context-aware access controls for remote and mobile users
- Integration with modern workplace and identity platforms

4.4 Service Transition

Service Transition ensures that newly deployed or transformed Secure Access Service Edge capabilities are introduced into live operations in a controlled, secure, and predictable manner. For public sector organisations delivering essential services, this phase is critical to ensuring that changes to access, security enforcement, and network connectivity do not adversely impact service availability, user experience, or cyber resilience.

Agilisys manages the transition from project delivery into business-as-usual operation through a structured and auditable process. This includes validating that the SASE platform components, identity integrations, Zero Trust Network Access policies, and segmentation controls are functioning as designed and can be supported by internal teams or managed service arrangements.

4.4.1 Monitoring, Testing, and Operational Readiness

Agilisys ensures that SASE controls are observable, testable, and operationally supportable prior to full adoption. Monitoring and alerting are validated to ensure that security teams retain visibility and investigative capability as network and access controls move to a cloud-delivered model.

The service includes structured testing of access scenarios, policy enforcement, and failure conditions, ensuring that essential services remain accessible and resilient. Operational documentation and knowledge transfer are provided to support transition into steady-state operations.

Service features include:

- Validation of logging, alerting, and evidence capture
- Access and resilience testing across user scenarios
- Operational documentation and handover activities

4.4.2 Knowledge Transfer, Documentation, and Operational Handover

A core component of Service Transition is ensuring that operational responsibility can be confidently assumed by the receiving support model. Agilisys delivers comprehensive documentation, including architecture diagrams, access models, policy summaries, and operational runbooks, tailored to both technical and non technical stakeholders.

Knowledge transfer is delivered through structured walkthroughs and handover sessions, ensuring that service desk, security, and infrastructure teams understand how SASE services are operated, monitored, and supported. Where required, Agilisys supports a phased transition period, allowing teams to build confidence before full handover, or to transition directly into an agreed managed service.

Service features include:

- Comprehensive operational and support documentation
- Knowledge transfer sessions for IT and security teams
- Defined support and escalation models post transition

4.4.3 Early Life Support and Service Stabilisation

Following transition into live operation, Agilisys provides early life support to ensure service stability and to address any issues arising from real world usage. This period is designed to allow fine tuning of access policies, monitoring thresholds, and user experience controls without undermining security or assurance.

Early life support is delivered by the same personnel involved in design and implementation, ensuring continuity of knowledge and rapid issue resolution. Feedback from users, service owners, and operational teams is incorporated to refine controls and confirm that the service meets agreed success criteria before full handover or steady state operation.

Service features include:

- Post go live early life support and stabilisation
- Rapid resolution of access and policy related issues
- Controlled transition into steady state or managed service support

4.5 Resold SASE Services

Agilisys provides customers with access to Cloudflare One Secure Access Service Edge (SASE) services as part of its managed and professional services portfolio. Agilisys supports the provisioning, configuration, and ongoing operation of the Cloudflare One platform, enabling organisations to securely deliver internet access, Zero Trust application connectivity, and identity-aware security controls without the need to manage complex underlying infrastructure.

Agilisys provides baseline operational support for Cloudflare One, assisting customers with day-to-day service enquiries, configuration guidance, and initial troubleshooting. Where required, Agilisys coordinates escalation to Cloudflare, ensuring that issues are managed efficiently and resolved through the appropriate technical channels. This approach provides customers with a clear and practical route for issue resolution, while maintaining transparency over service responsibilities and support boundaries.

5 Onboarding and Offboarding

Agilisys provides a structured onboarding and offboarding process for programmes and professional services engagements.

5.1 Onboarding Cloud Professional Services Engagements

Onboarding for our professional services engagements begins with a structured mobilisation phase, designed to establish a shared understanding of the project's scope, objectives, and success criteria. This phase includes collaborative discovery workshops with key stakeholders to assess the current IT landscape, business drivers, and organisational readiness for change.

Our team conducts a review of the existing infrastructure, applications, and operating model, identifying interdependencies, risks, and opportunities for optimisation. Where appropriate, we deploy clientless discovery tooling to gather system insights with minimal disruption. This enables us to produce a tailored delivery plan, including a high-level design, migration strategy, and resource model aligned to your priorities.

We work closely with your teams to define governance structures, communication protocols, and decision-making frameworks. As part of mobilisation, we confirm all necessary access requirements, including the verification of staff security clearances (e.g., SC) to ensure compliance with your organisational and regulatory standards.

This approach ensures a secure, efficient, and low risk start to the engagement, enabling rapid progress while maintaining full visibility and control for your organisation.

5.2 Offboarding Cloud Professional Services Engagements

At the conclusion of a professional services engagement, Agilisys ensures a structured and secure transition of responsibilities to the client's internal teams or a nominated third-party provider. Our offboarding process is designed to maintain service continuity, preserve institutional knowledge, and uphold compliance with security and governance standards.

We deliver a comprehensive handover pack, which includes relevant artefacts such as solution designs, configuration documentation, and migration records. Where applicable, we conduct knowledge transfer sessions with technical and operational stakeholders to ensure a clear understanding of the delivered solution, its dependencies, and ongoing management considerations.

Access credentials, administrative rights, and configurations are reviewed and securely transferred to the designated teams. We also confirm the revocation of Agilisys access to client environments and systems, and, where required, provide formal confirmation of data deletion in accordance with our data governance and security policies.

Our offboarding approach is flexible and can be tailored to meet specific client requirements, ensuring a smooth and confident transition to business-as-usual operations or further transformation phases.

6 Support

We offer flexible support options to align with the needs of each engagement, recognising that support requirements vary across the lifecycle of a cloud deployment or migration programme. Our support models are designed to ensure continuity, build in-house capability, and provide assurance during critical transition periods.

6.1 Early Lifecycle Support

Following each deployment milestone or line-of-business system migration, we provide early lifecycle support, typically for a period of two weeks. This is delivered by the same professional services personnel who implemented the solution, ensuring continuity of knowledge and rapid issue resolution. This model is ideal for stabilisation, user onboarding, and addressing any post-deployment refinements.

6.2 Managed Support During Programme Delivery

For clients who require operational support during the delivery phase, Agilisys can provide a managed service that runs in parallel with the professional services engagement. This ensures stability and continuity while new platforms are being deployed or migrated. We also offer a ramped support model, enabling a phased handover to internal teams. This approach allows in-house staff to progressively assume responsibility for managing the cloud environment, with Agilisys providing mentoring, shadowing, and escalation support as capabilities mature.

6.3 Transition to Agilisys Managed Cloud Services

Where ongoing operational support is required beyond the project lifecycle, clients can transition into one of our established Managed Cloud Service tiers:

6.3.1 Standard Cloud Management

Provides core business hours support (08:00–18:00, Monday to Friday), with 24/7 incident response for Priority 1 issues. It includes tenancy management, patching, monitoring, basic cost optimisation reporting, and monthly service performance reviews. This tier is ideal for organisations seeking reliable, foundational cloud management with essential governance and support.

6.3.2 24x7 Cloud Management

Builds on the Standard offering with enhanced capabilities such as proactive security incident response, customised patching cycles, Privileged Identity Management (PIM), and detailed monthly performance reviews led by a dedicated service delivery manager. It also includes proactive execution of optimisation and security recommendations, making it suitable for organisations with complex environments or higher compliance and performance demands.

Each support model is underpinned by our commitment to service quality, security, and knowledge transfer, ensuring that clients receive the right level of assistance at every stage of their cloud journey.

7 Pricing

Pricing is based on the specific service requirements, service levels, scale and scope of services using the rate card provided in the accompanying pricing document for this GCloud service.

We provide UK based onshore, and offshore resources that can be leveraged to meet your specific needs, the prevailing rates are detailed within our Pricing documents.

Please contact info@agilisys.co.uk to obtain a quote for your required services.

8 Compliance and Security

Agilisys embeds robust compliance and security practices across all stages of cloud transformation and management, ensuring public sector organisations meet regulatory obligations while safeguarding critical assets.

Our services are designed in alignment with UK Government and NHS policies, incorporating National Cyber Security Centre (NCSC) guidance and ISO27001, Cyber Essentials Plus, and other relevant certifications.

From initial discovery through to optimisation, we assess and enhance security controls, including identity governance, privileged access management, encryption, and continuous monitoring.

Our managed services provide proactive threat detection and response, patching, and compliance reporting, while our cloud identity and access management solutions ensure Zero Trust principles are applied across hybrid environments. Whether supporting Azure, multi-cloud or hybrid estates, Agilisys ensures that governance frameworks are in place to maintain operational integrity, data protection, and audit readiness throughout the cloud lifecycle.

Agilisys is certified/compliant with the following standards and schemes for Managed and Professional Services and is a proud signatory of the Armed Forces Covenant:

9 Contact and Next Steps

We welcome the opportunity to support your organisation's cloud transformation journey. For further information, to discuss your specific requirements, or to request a tailored proposal, please contact us at info@agilisys.co.uk.