Agilisys

Agilisys CloudAegis

G-Cloud 15 Service Definition

Lot 3 – Cloud Support

Table of Contents

1 Introduction 2

2 Who this Service is For? 2

3 CloudAegis - an overview 3

4 Service Description 4

4.1 CloudAegis Protect 4

4.2 CloudAegis Sentinel 4

4.3 CloudAegis Identity 4

4.4 CloudAegis Govern 5

4.5 CloudAegis Resilience 5

4.6 CloudAegis AzureOps 5

4.7 CloudAegis Edge 6

4.8 Resold Azure and Fabric Services (Direct CSP) 6

5 Onboarding and Offboarding 6

5.1 Onboarding Agilisys CloudAegis 6

5.2 Offboarding from Agilisys CloudAegis 7

6 Support 7

6.1 Baseline CSP Support for Resold Azure and Fabric Services 7

6.2 Standard Support 7

6.3 24x7 Support 8

7 Pricing 8

8 Compliance and Security 8

9 Contact and Next Steps 9

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 compelling 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.

We combine technology, tested methodologies and skills that unleash the power of cloud and minimise the complexity that can sometimes come with migration. We put strategy before technology and deliver the capabilities, experience and capacity needed to make the right cloud decisions and transform public services.

2 Who this Service is For

CloudAegis is purpose-built for UK public sector organisations that operate in increasingly complex digital environments and face mounting pressures around security, compliance, and operational resilience. This includes local authorities, central government departments, NHS bodies, emergency services, and other regulated entities that handle sensitive data and deliver critical citizen services.

These organisations often manage hybrid or multi-cloud infrastructures, legacy systems, and diverse user bases, all while adhering to stringent regulatory frameworks such as the NCSC Cyber Assessment Framework (CAF), DSPT, and ISO27001. CloudAegis is designed for those who need to:

- **Strengthen cyber resilience** against evolving threats such as ransomware, phishing, and insider risk.
- **Adopt Zero Trust principles** to secure identities, devices, and workloads across distributed environments.
- **Ensure compliance and governance** through automated policy enforcement and audit-ready reporting.
- **Optimise cloud operations** while maintaining cost control and operational efficiency.
- **Enable continuity and disaster recovery** without compromising performance or scalability.

Whether you are at the start of your cloud security journey or seeking to mature your existing posture with advanced automation and predictive analytics, CloudAegis provides a structured, scalable pathway to achieve these goals.

3 CloudAegis - an overview

At its core, CloudAegis combines Zero Trust architecture, identity governance, Microsoft Defender and Sentinel operations, and Azure security optimisation into a unified solution. It provides a structured approach to safeguarding cloud environments, enabling organisations to:

- Protect critical assets through advanced threat detection and response.
- Govern identities and entitlements with automated compliance controls.
- Optimise cloud operations for resilience and cost efficiency.
- Embed assurance and continuity through disaster recovery and ransomware protection.

CloudAegis operates within a modular ecosystem of complementary services—such as Managed Cloud Services, Modern Workplace, and Intelligent Automation—to deliver a holistic transformation journey. This means clients can start with foundational security capabilities and progressively mature their posture with advanced automation, predictive analytics, and integrated governance.

CloudAegis is not a standalone offering; it is part of a broader framework of services designed to support clients' modern platforms at scale. This integrated framework delivers security, assurance, operational efficiency, and long-term value, ensuring that organisations can confidently adopt and manage cloud technologies while meeting regulatory and performance requirements.

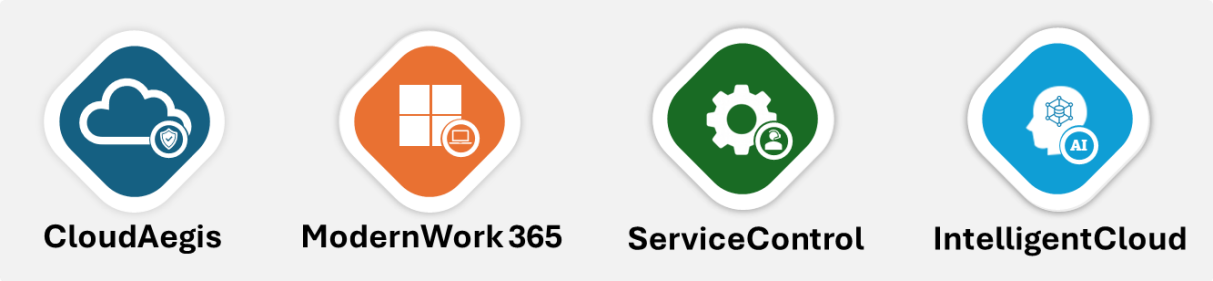

Figure 1 - Agilisys Cloud Assurance and Management Framework

4 Service Description

CloudAegis provides a **high-level, integrated security and governance service** designed to protect modern cloud platforms at scale. It combines Zero Trust principles, identity management, and advanced threat detection with compliance automation and operational resilience. The service is modular, enabling organisations to select individual components or adopt the full suite for comprehensive protection.

Service Offers:

- **CloudAegis Protect** – Delivers advanced threat protection and vulnerability management to secure endpoints, email, and web traffic.
- **CloudAegis Sentinel** – Provides managed detection and response with automated incident handling through Security Orchestration Automation and Response (SOAR) playbooks.
- **CloudAegis Identity** – Implements robust identity governance with Entra ID, MFA, and Privileged Identity Management.
- **CloudAegis Govern** – Automates compliance and policy enforcement aligned to CAF, DSPT, and ISO standards.
- **CloudAegis Resilience** – Ensures business continuity with backup, DRaaS, and ransomware recovery solutions.
- **CloudAegis AzureOps** – Optimises cloud operations through secure landing zones, patching, and cost governance.
- **CloudAegis Edge** – Secure Access Service Edge (SASE) for unified network and cloud security, enabling secure connectivity for remote and hybrid workforces.

4.1 CloudAegis Protect

CloudAegis Protect focuses on safeguarding your organisation's digital perimeter. It deploys Microsoft Defender XDR for comprehensive endpoint protection, implements vulnerability management to reduce attack surfaces, and enforces email and web security controls. This proactive approach mitigates risks before they escalate, ensuring a secure foundation for cloud operations.

- Deploy Microsoft Defender XDR for comprehensive endpoint protection.
- Implement vulnerability management to reduce attack surfaces.
- Enforce email and web security controls for proactive threat mitigation.

4.2 CloudAegis Sentinel

Delivers advanced security operations through Microsoft Sentinel. It enables real-time threat detection, incident response, and automated remediation using SOAR playbooks. By integrating log analytics and incident workflows, CloudAegis Sentinel reduces response times and enhances operational resilience, ensuring threats are neutralised quickly and effectively.

- Enable real-time threat detection and incident response using Microsoft Sentinel.
- Automate remediation workflows through SOAR playbooks.
- Integrate log analytics for faster resolution and improved resilience.

4.3 CloudAegis Identity

Identity is the new security perimeter, and CloudAegis Identity enforces Zero Trust principles across your environment. It leverages Entra ID for secure authentication, applies Conditional

Access policies, and implements MFA and Privileged Identity Management to protect sensitive accounts. This ensures only authorised users access critical resources, reducing insider and external risks.

- Apply Zero Trust principles across all user access points.
- Use Entra ID for secure authentication and lifecycle governance.
- Implement MFA and Privileged Identity Management to protect sensitive accounts.

4.4 CloudAegis Govern

Governance and compliance are central to public sector operations. CloudAegis Govern automates policy enforcement and entitlement reviews, mapping controls to CAF, DSPT, and ISO frameworks. It provides audit-ready reporting and continuous compliance monitoring, helping organisations maintain regulatory alignment while reducing manual overhead.

- Automate policy enforcement and entitlement reviews.
- Align governance with CAF, DSPT, and ISO frameworks.
- Provide audit-ready reporting and continuous compliance monitoring.

4.5 CloudAegis Resilience

Business continuity is critical in today's threat landscape. CloudAegis Resilience delivers robust backup and Disaster Recovery as a Service (DRaaS) using Veeam and Azure technologies. It includes ransomware recovery capabilities and structured testing to validate recovery plans, ensuring services remain available even during major disruptions.

- Deliver robust backup and Disaster Recovery as a Service (DRaaS).
- Include ransomware recovery capabilities for critical systems.
- Validate recovery plans through structured testing and assurance.

4.6 CloudAegis AzureOps

Optimising cloud operations is essential for cost control and security. CloudAegis AzureOps establishes secure landing zones, enforces Azure policies, and applies patching and configuration baselines. It also integrates FinOps practices to manage cloud spend effectively, enabling organisations to maintain performance while reducing unnecessary costs.

- Establish secure landing zones for cloud deployments.
- Enforce Azure policies and maintain patching baselines.
- Integrate FinOps practices for cost optimisation and governance.

4.7 CloudAegis Edge

CloudAegis Edge delivers Secure Access Service Edge (SASE) capabilities to unify network and cloud security for modern, distributed environments. It integrates secure web gateways, cloud access security brokers (CASB), Zero Trust Network Access (ZTNA), and firewall-as-a-service into a single, cloud-native architecture. This ensures secure, policy-driven access for users, devices, and applications—regardless of location—while maintaining compliance and performance.

- Provide secure, encrypted access to cloud applications and data from any location.
- Enforce Zero Trust policies with integrated CASB and ZTNA for granular control.
- Simplify network security through a unified, cloud-native architecture that scales with demand.

4.8 Resold Azure and Fabric Services (Direct CSP)

Agilisys provides customers with access to Microsoft Azure services as a Cloud Solution Provider (CSP). As a Direct CSP, Agilisys provisions Azure subscriptions and invoices monthly in arrears based on actual consumption. Agilisys also offers baseline support, assisting customers with day-to-day queries and initial troubleshooting, and coordinating escalation to Microsoft where appropriate. This ensures customers receive practical guidance and a clear route for issue resolution without overstating the support dependency.

Agilisys maintains Premier Support for Partners (PSfP). This provides enhanced escalation capabilities, faster response SLAs, and access to Microsoft engineering experts, enabling Agilisys to manage escalations on behalf of our clients efficiently, and draw on specialist guidance when needed.

5 Onboarding and Offboarding

Agilisys provides a structured onboarding and offboarding process for clients seeking to transition services into or away from our CloudAegis Services.

5.1 Onboarding Agilisys CloudAegis

Onboarding begins with a collaborative discovery phase to understand the current architecture, operational practices, and service dependencies. We assess the environment's health, security posture, and governance controls, and establish a baseline for service delivery.

Our team works with client stakeholders to align service levels, access protocols, and reporting requirements, ensuring continuity and minimal disruption. Where appropriate, we integrate with existing subscriptions and tooling, adopting client-specific configurations and documentation into our management framework. This approach enables rapid service mobilisation while maintaining full visibility and control for the client.

5.1.1 Resold Azure and Fabric Services

For the onboarding of Resold Azure and Fabric Services, we are required by Microsoft to confirm Customer acceptance of the Microsoft Customer Agreement, (name, email, timestamp) prior to any subscription provisioning.

5.2 Offboarding from Agilisys CloudAegis

When transitioning from our CloudAegis service, Agilisys ensures a secure and orderly handover to the client's internal teams or a nominated successor provider.

We transfer ownership of the cloud subscription, along with all client-specific designs, operational documentation, and configuration records. Environment credentials and access details are securely handed over, and any client data retained within Agilisys systems—such as monitoring logs or support records - is securely deleted in accordance with our data governance policies.

Upon request, we provide formal confirmation of data destruction. Our offboarding process is designed to preserve service integrity, maintain compliance, and support a smooth transition with minimal operational impact.

5.2.1 Resold Azure and Fabric Services

For the offboarding of Resold Azure and Fabric Services, we will assist with:

- Subscription Transfer/Termination: at customer request, Agilisys will assist with transferring the CSP relationship to another provider or terminating the subscription(s); customer must give notice in line with Microsoft terms for any auto renewed services.
- Final Billing & Consumption: final invoice will reflect usage up to the effective transfer/termination date; charges may continue until resources are deprovisioned by the customer. Consumption remains the customer's responsibility.
- Data & Records: provide subscription configuration snapshots and service records; delete Agilisys held operational data per our data governance policies and issue destruction confirmation on request.

6 Support

Our flexible service tiers offer scalable support, proactive monitoring, cost optimisation, and 24/7 incident response, empowering public sector organisations to focus on service delivery while we maintain the health, compliance, and efficiency of their cloud ecosystems.

Agilisys offers baseline support for Resold Azure and Fabric Services, with two primary service tiers for its managed cloud services:

6.1 Baseline CSP Support for Resold Azure and Fabric Services

Baseline CSP support is not a managed service; it is limited to first-line break/fix and subscription/billing assistance (intake and triage of tickets, troubleshooting tenant/configuration issues, and escalating undocumented service defects/outages to Microsoft) and therefore does not include proactive monitoring, solution architecture/design, day-to-day operations (e.g., backups, patching, incident response), cost governance/FinOps, or 24×7 managed SLAs that are typically delivered under a managed Azure service.

6.2 Standard Support

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 24x7 Support

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.

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.