Agilisys

Microsoft Security 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.

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 skills, experience and capacity needed to make the right cloud decisions and transform public services.

2 Who this Service is For?

Our Microsoft Security Transformation services are designed for UK public sector organisations — including local authorities, NHS bodies, emergency services, and other public institutions — seeking to strengthen their security posture and modernise their digital infrastructure, regardless of project scale or complexity, such as implementing a Zero Trust architecture, deploying advanced Microsoft security tools, integrating identity and access management, or delivering a full security transformation roadmap, our services are tailored to meet each organisation's unique needs.

Our services are ideal for organisations with legacy estates, hybrid environments, or cloud strategies, and are designed to ensure secure, compliant, and cost-effective adoption of Microsoft security capabilities that support operational continuity and long-term resilience.

3 Microsoft Security Transformation Services - an overview

Agilisys' Microsoft Security Transformation Services provide a comprehensive approach to strengthening security posture and enabling resilient, compliant operations across cloud, hybrid, and on-premises environments. These services are designed for UK public sector organisations seeking to modernise security capabilities and align with recognised frameworks such as the NCSC Cyber Assessment Framework (CAF), NIST Cybersecurity Framework Tier 4, and UK Government Cloud Security Principles.

The focus is on building and deploying advanced security architectures and controls using Microsoft technologies, including Entra ID, Microsoft Defender, Microsoft Sentinel, and Intune. Each service is delivered as a structured engagement, ensuring organisations gain a fully implemented solution across the following areas**:**

- Security Strategy & Roadmap – Establishes a clear, phased plan for security transformation, including governance, compliance alignment, and prioritised actions.
- Zero Trust Architecture – Designs and deploys a security model based on least privilege, continuous verification, and integrated Microsoft security capabilities.

- Threat Detection and Response – Implements advanced detection and response solutions using Microsoft Sentinel and Defender XDR, with automated playbooks and orchestration.

Each engagement delivers detailed documentation, operational guides, and handover packs, enabling organisations to maintain and evolve their security posture independently. The outcome is a robust, future-ready security foundation that supports operational continuity and long-term resilience.

4 Service Description

We deliver end-to-end Microsoft Security Transformation services for UK public sector organisations, enabling secure, compliant, and resilient digital environments. Our services combine Zero Trust principles, advanced threat protection, and governance aligned to NCSC Cyber Assessment Framework (CAF) and NIST Cybersecurity Framework Tier 4 maturity. Leveraging Microsoft's E5 security stack, Azure security benchmarks, and automation, we help clients achieve robust security posture and continuous improvement.

Our range of services are described below, customers are able to call-off these services individually, or in any combination in order to customise the call-off to meet their specific requirements. Please contact us at info@agilisys.co.uk to discuss your needs further and we will be delighted to help.

4.1 Security Strategy & Roadmap

The Security Strategy & Roadmap service establishes a clear, structured approach to achieving a resilient and compliant security posture across cloud, hybrid, and on-premises environments. It begins with a comprehensive assessment of the current security landscape, examining controls, policies, and technologies against recognised frameworks such as the NCSC Cyber Assessment Framework (CAF), and ISO27001. From this baseline, the service defines a strategic direction for security transformation. It sets out a phased roadmap that prioritises actions, allocates resources, and aligns with organisational objectives.

Governance and regulatory alignment form a core part of the service, ensuring adherence to Cloud Security Principles, GDPR, and sector-specific requirements. The roadmap also embeds continuous improvement measures, enabling organisations to adapt to evolving threats through automation, AI-driven insights, and proactive risk management. The outputs can be tailored to your specific requirements and include:

- Baseline Security Assessment Report: Detailed analysis of current security posture against CAF and ISO27001 standards.
- Gap Analysis & Risk Register: Identification of vulnerabilities, compliance gaps, and prioritised risks.
- Strategic Security Roadmap Document: A phased plan outlining actions, timelines, dependencies, and resource requirements.
- Zero Trust Architecture Blueprint: Design documentation for identity, access, and network segmentation aligned with Microsoft security capabilities.
- Governance & Compliance Framework: Policies and controls mapped to Cloud Security Principles, GDPR, and sector-specific regulations.
- Continuous Improvement Plan: Recommendations for automation, AI-driven threat detection, and ongoing posture enhancement.

- Executive Summary & Presentation Pack: High-level overview for senior stakeholders, including key findings and strategic priorities.

4.2 Zero Trust Architecture

The Zero Trust Architecture service delivers a security model that assumes no implicit trust within or outside the network, enforcing strict identity verification and continuous validation of every user, device, and application. This service establishes a layered security approach built on Microsoft technologies, integrating identity and access management, device compliance, application security, and data protection.

The architecture is designed to secure hybrid and cloud environments by applying least-privilege principles, conditional access policies, and real-time threat detection. It incorporates Microsoft Entra ID for identity governance, Microsoft Intune for device compliance, and Microsoft Defender for endpoint and cloud protection. Network segmentation and micro-perimeters are implemented to reduce lateral movement, while data classification and encryption safeguard sensitive information.

Continuous monitoring and automated response capabilities are embedded through Microsoft Sentinel and integrated workflows, ensuring rapid detection and remediation of threats. The outcome is a resilient, adaptive security framework that aligns with UK Government Cloud Security Principles, CAF Enhanced Profile, and NIST Tier 4 maturity standards. Key outputs include:

- Zero Trust Architecture Blueprint: Design document outlining identity, device, application, and data security layers.
- Identity & Access Control Policies: Conditional access rules, MFA configurations, and least-privilege role assignments.
- Device Compliance Configuration: Intune-based policies for endpoint security and posture enforcement.
- Application Security Integration: Single Sign-On (SSO) and Microsoft Defender for Cloud Apps configuration.
- Data Protection Framework: Information classification, encryption standards, and DLP policies.
- Network Segmentation Plan: Design and segmentation strategy for hybrid environments.
- Monitoring & Response Playbooks: Automated workflows for threat detection and incident response using Microsoft Sentinel.
- Compliance Mapping Report: Documentation aligning architecture with CAF, ISO27001, and UK Government security principles.

4.3 Threat Detection and Response

The Threat Detection and Response service delivers a fully deployed security capability designed to identify, analyse, and respond to threats across cloud, hybrid, and on-premises environments. This service focuses on the design and implementation of an integrated detection and response solution using Microsoft security technologies, ensuring organisations have a strong foundation for proactive threat management.

Deployment includes Microsoft Sentinel as the central Security Information and Event Management (SIEM) platform, configured to ingest logs from critical systems and apply advanced correlation rules for real-time alerting. Microsoft Defender XDR is implemented to extend detection and response across endpoints, identities, applications, and workloads, creating a unified security layer. Custom detection policies and behavioural analytics are developed to address organisation-specific risks, while automated playbooks are deployed to accelerate containment and remediation through orchestration tools such as Azure Logic Apps.

The architecture incorporates threat intelligence feeds and compliance-aligned reporting frameworks, providing visibility into emerging risks and ensuring adherence to UK Government Cloud Security Principles, the Cyber Assessment Framework (CAF) Enhanced Profile, and NIST Tier 4 maturity standards. Dashboards and operational documentation are delivered as part of the deployment, enabling security teams to monitor, investigate, and respond effectively from day one. Key outputs include:

- Microsoft Sentinel SIEM Deployment: Configured platform with log ingestion, correlation rules, and alerting policies.
- Defender XDR Integration: Unified detection and response across endpoints, identities, and applications.
- Custom Detection Rules and Analytics: Tailored policies and behavioural analytics for advanced threat identification.
- Automated Response Playbooks: Orchestrated workflows for rapid containment and remediation using Logic Apps.
- Deployment Documentation and Handover Pack: Detailed configuration records, operational guides, and knowledge transfer materials.

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.

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.