Agilisys

Strategic Information Security Leadership, Governance, Risk & Compliance

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?

This service is designed for UK public sector organisations responsible for delivering essential services and seeking to strengthen their cyber resilience.

It is particularly suited for councils, NHS bodies, and government agencies that need to comprehensively safeguard their organisation's digital and physical information, whilst integrating governance, operational security practices, and advanced technologies, which in turn will mitigate risks, ensure compliance, and support business continuity.

3 About this Service

This Strategic Information Security Leadership, Governance, Risk & Compliance service is designed to align with internationally recognised standards such as ISO 27001:2022, NIST Cybersecurity Framework, Cyber Essentials Plus, and the NCSC's Cyber Assessment Framework (CAF), offering scalable, proactive, and adaptable solutions tailored to your organisation's needs.

Key Objectives

- Protect Confidentiality, Integrity, and Availability (CIA) of information.
- Ensure compliance with relevant regulatory frameworks (e.g., UK GDPR, PSN CoCo, PCI DSS, NHS DSPT etc.).
- Strengthen resilience to cyber threats through ongoing monitoring, response, and improvement.
- Foster a security-first culture through training, policies, and awareness.

4 Service Description

Governance, Risk, and Compliance (GRC)

Policy Development and Implementation - create tailored security policies, including access control, data classification, and incident management, that align with both your organisation and operational needs whilst maintaining compliance with good practice frameworks such as ISO 27001:2022. Then implement those policies and controls in a way that keeps operational friction as low as possible whilst driving material and demonstrable good practice security outcomes such as those described in NIST CSF and/or NCSC's CAF. All of this enabled by an overarching end to end security management plan, designed and maintained throughout the service lifecycle, ensuring a clear roadmap to security success.

For informed decision-making, structured tools such as 5x5 risk matrices and Data Protection Impact Assessments (DPIAs) are deployed. Data, system and process discovery exercises are also undertaken contributing to a series of gap analysis'. The service's continuous assessment of compliance with UK GDPR, Cyber Essentials Plus (CE+), PCI DSS, and Public Services Network (PSN) requirements. We implement Audit Management, which facilitates internal and external audits, proactively identifying and addressing gaps.

Technical estate compliance

The Agilisys security compliance blends the policy and procedural compliance with the technical, ensuring paperwork doesn't just align to good practice but the technical estate is constructed in such a way as to enable the long term security goals of the organisation without blocking operational requirements or blowing technical budgets.
This can include:

- Validation/gap analysis of Zero Trust Architecture.
- Network zoning review.
- Identity and Access Management reviews, Gap analysis and re-design.
- Discovery of NCSC Architecture Anti-Patterns and risk assessment.
- Gap analysis and risk assessment of layered defence in depth and cyber incident resillienceincludesresilience utilising a blend of threat intelligence sources and frameworks such as MITRE.
- Reviews of security tech stack/licensing and utilisation vs potential utilisation.
- Reviews of security monitoring capabilities and scope, gap analysis and risk assessment of critical blind spots
- Maturity improvement plan for security monitoring, including reducing false positive detections and data ingestion costs where possible
- Design of thorough test plans for SOC and security monitoring to materially validate detection capabilities
- Design of relevant and incident response and crisis management exercises, tailored to audience, ranging from technical deep dives with engineers and incident responders to high level leadership orchestration of crisis management
- Orchestration of external tests and audits such as Pen tests and IT Health Checks etc.

Incident Response and Recovery

We define workflows for handling incidents such as ransomware attacks, phishing campaigns, or insider threats. Backup Management includes the implementation of NCSC good practice guidance (Such as the 3-2-1 rule) backup strategies to safeguard critical data against loss or corruption. This service also includes technical resilience Planning and Post-Incident Reviews: Detailed root cause analysis and documentation of lessons learned to improve future response capabilities.

Proactive Security Practices

Phishing Simulations and education deployment, Penetration Testing, Horizon Scanning implementation, and Security Control Validation, implementation of security governance committees and security champions groups practices all collectively enhance user and organisational awareness and reduce the likelihood of human error, in addition to identifying and mitigating risks and vulnerabilities before they can be exploited.

Reporting and Analytics

Custom Dashboards, Executive Reports Compliance Audit Trails enable data-driven decision-making. KPIs and Metrics demonstrate accountability and compliance to internal and external stakeholders. Ensure you can materially demonstrate the security ROI to organisational leadership.

Regulatory Compliance Mapping

Identifies and aligns organisational processes with applicable standards such as GDPR, ISO 27001, Cyber Essentials Plus, and NCSC CAF and ensures clarity on regulatory requirements and provides a tailored compliance roadmap to reduce non-compliance risk.

Gap Analysis and Risk Assessment

Conducts detailed assessments to identify compliance and security practices gaps and prioritises corrective actions and mitigates risks by addressing vulnerabilities and non-conformities.

Policy and Procedure Development

Creates, updates, and reviews policies and procedures to align with compliance standards, which establish clear guidelines for secure and compliant operations, reducing ambiguity and ensuring consistency.

Audit Preparation and Support

Provides guidance and assistance during internal and external audits, including evidence collection and readiness reviews which improves audit success rates and minimises disruptions by ensuring thorough preparation.

Continuous Monitoring and Reporting

Implements tools and processes to monitor compliance status and generate regular reports and enables proactive identification of issues and informed decision-making through actionable insights.

Third-Party Compliance Oversight

Assesses and monitors third-party vendors for compliance with security and data protection requirements, whilst mitigating risks associated with external parties, ensuring contractual and regulatory obligations are met.

Customised Compliance Tools Integration

Deploys and configures tools for compliance monitoring, policy management, and risk tracking, thereby enhaing efficiency and accuracy in managing compliance activities through automation.

Proactive Governance Reviews

Facilitates regular governance meetings to review compliance performance and adapt strategies, supporting continuous improvement and alignment with evolving regulatory landscapes.

5 Onboarding and Offboarding

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

5.1 Onboarding

Onboarding 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 business drivers, and organisational readiness for change.

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

At the conclusion, Agilisys ensures a structured and secure transition of responsibilities to your internal teams

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 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, 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.