

Renaissance Computer Services Ltd

Service Definition Document (SDD)

Managed IT Service Plans – G-Cloud Lot 3 (Cloud Support)

Supplier: Renaissance Computer Services Ltd

Service: Managed IT Service Plans

Lot: G-Cloud 15 – Lot 3 (Cloud Support)

Version: 1.0

Last Updated: 29/01/2026

Document Owner: Director of Sales & Account Management

Contents

1. Service Overview
2. Service Description
3. Intended Users
4. Service Scope and Responsibilities
5. Service Features
6. Benefits
7. Tooling and Reselling Arrangements
8. Implementation and Onboarding
9. Service Management and Support
10. Monitoring, Reporting and Analytics
11. Security and Data Protection
12. Availability and Resilience
13. Exit and Offboarding
14. Assumptions and Constraints
15. Document Control

1. Service Overview

Managed IT Service Plans are a cloud support service delivered by Renaissance Computer Services Ltd ("Renaissance"). The service provides structured, ongoing IT support designed to maintain reliable day-to-day IT operations for users and supported business systems.

The service combines service desk support, proactive monitoring, secure remote access, backup, and security monitoring, amongst other productivity, compliance, and security services, to support organisations operating cloud-based and hybrid IT environments.

2. Service Description

Renaissance delivers Managed IT Service Plans as an ongoing support service aligned to G-Cloud Lot 3. The service includes remote 1st, 2nd and 3rd line support, proactive monitoring using Remote Monitoring and Management (RMM) tooling, secure remote access, backup services, security monitoring, and other productivity, compliance, and security services dependent on the chosen Service Plan level.

Renaissance manages incidents, service requests, endpoint tooling, and user support activities to minimise disruption and maintain service continuity. The service is delivered primarily remotely, with onsite support available where required at additional cost.

3. Intended Users

The service is suitable for:

- Central government departments and agencies
- Local authorities
- Education providers
- NHS and healthcare organisations
- Arm's length bodies and other public sector organisations

The service is appropriate for organisations seeking ongoing IT operational support rather than cloud design, migration, or transformation services.

4. Service Scope and Responsibilities

4.1 Included in the Service

Renaissance provides:

- Remote service desk support (1st–3rd line)
- Incident and service request management
- Proactive monitoring and alerting
- Secure remote access for support activities
- Backup monitoring and support
- Endpoint tooling management
- User support and coordination of end-user training
- Reporting on incidents, trends, and service activity

4.2 Buyer Responsibilities

The Buyer is responsible for:

- Providing supported endpoints and stable internet connectivity
- Granting administrative access required to onboard monitoring and security tooling
- Maintaining internal policies for device usage and data protection
- Requesting changes and support via agreed channels

5. Service Features

- Remote Monitoring and Management (RMM)
- Antivirus Management (AV)
- Endpoint Detection & Response (EDR)
- 24x7 Security Operations Centre (SOC) Secure, VPN-less remote access
- 24/7 security monitoring alerts
- Backup solutions and monitoring
- Password management tooling
- Phishing simulations and security awareness training
- Managed email signature services

6. Benefits

- Consistent and reliable IT support
- Faster identification and resolution of issues
- Reduced unplanned downtime
- Improved operational stability
- Enhanced security awareness and posture

7. Tooling and Reselling Arrangements

Renaissance uses third-party tooling to deliver elements of the Managed IT Service Plans. Where applicable, Remote Monitoring and Management and associated security and backup tooling are provided using the **Kaseya and Microsoft** platforms.

Renaissance acts as a reseller providing additional support and managed service capabilities beyond the underlying tooling.

8. Implementation and Onboarding

Onboarding activities are agreed at call-off and typically include:

1. Initial discovery and service setup
2. Deployment of monitoring, security, and backup agents
3. Configuration of alerting and reporting
4. Service desk onboarding and escalation setup
5. Transition to steady-state support

Implementation timescales depend on the number of endpoints, complexity of the environment, and buyer readiness.

9. Service Management and Support

9.1 Support Channels

- Email support
- Online ticketing
- Telephone support

9.2 Support Hours

- Core support hours: Monday to Friday, 09:00–17:00 UK (excluding public holidays)

9.3 Support Levels

- **Standard (included):** Remote 1st/2nd/3rd line support, incident and service request handling, monitoring alert triage, and reporting during core hours
- **Onsite (additional cost):** Onsite support for installations, changes, and fault resolution, charged on a time and materials or fixed-price basis
- **Account Management:** A Technical Account Manager may be provided for certain plans or added at call-off

9.4 Incident Handling

Incidents and requests are triaged on receipt and prioritised by impact and urgency. Response targets are agreed at call-off and documented within the Service Level Agreement (SLA).

10. Monitoring, Reporting and Analytics

- Continuous monitoring with 24/7 alerting
- Incident and trend reporting
- Proactive results analysis to identify recurring issues

11. Security and Data Protection

Renaissance operates security controls proportionate to the service risk profile, including:

- Role-based access controls and least-privilege principles
- Secure remote access for support activities
- Monitoring and alerting for security-related events
- Staff screening and BPSS clearance availability where required

Personal data is processed in accordance with applicable UK data protection legislation.

12. Availability and Resilience

The service is designed to support operational continuity through proactive monitoring, alerting, and responsive incident handling. Where third-party tooling or infrastructure is used, resilience is dependent on those providers.

13. Exit and Offboarding

At contract end, the service may be terminated, extended, or transitioned by agreement. Renaissance will support offboarding activities in line with the call-off contract and agreed exit procedures. Onsite or extended offboarding support may incur additional charges.

14. Assumptions and Constraints

The service requires supported endpoints, stable internet connectivity, and administrative access to onboard monitoring, backup, and security tooling. Onsite support is not included and is chargeable where required.

15. Document Control

Item	Value
Document title	Service Definition Document – Managed IT Service Plans
Supplier	Renaissance Computer Services Ltd
Version	1.0
Last updated	[Insert Date]
Review cycle	Annual or upon material change