

Renaissance Computer Services Ltd

Service Definition Document (SDD)

Managed Penetration Testing & Remediation Support – G-Cloud Lot 3 (Cloud Support)

Supplier: Renaissance Computer Services Ltd

Service: Managed Penetration Testing & Remediation Support

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

Version: 2.0

Last Updated: 30 Jan 2026

Document Owner: Managing Director

Contents

1. Service Overview
2. Service Description
3. Intended Users
4. Service Scope and Responsibilities
5. Testing Approach and Methodology
6. Service Features
7. Benefits
8. Engagement Model and Deliverables
9. Service Management and Support
10. Security, Assurance and Ethics
11. Availability and Scheduling
12. Exit and Retention of Materials
13. Assumptions and Constraints
14. Document Control

1. Service Overview

Managed Penetration Testing & Remediation Support is a cloud support security service delivered by Renaissance Computer Services Ltd (“Renaissance”) as the prime

contractor. Renaissance manages the engagement end-to-end, including scoping, rules of engagement, coordination, and findings triage. Technical testing and certified assessor review are delivered by an approved specialist testing partner. Renaissance remains accountable for service delivery and outcomes.

The service supports organisations seeking assurance over the security posture of cloud infrastructure, applications, and configurations, and is suitable for audit preparation, risk management, and ongoing security assurance activities.

2. Service Description

Renaissance provides a managed penetration testing service delivered as a scoped, authorised engagement. Renaissance manages planning, scope definition, rules of engagement, access coordination, scheduling, and stakeholder communication. Technical testing activities and certified assessor review are delivered by an approved specialist testing partner using recognised techniques and tooling. Findings are triaged, risk-rated, and presented with clear remediation guidance. Optional remediation validation / retesting can be coordinated to confirm that fixes have been successfully implemented. Where buyers require a specific accreditation (e.g., CREST), this can be delivered via an appropriately accredited testing partner and confirmed at call-off (and may be priced separately).

3. Intended Users

The service is suitable for:

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

The service is appropriate for organisations operating cloud-hosted or internet-facing systems that require independent security assurance.

4. Service Scope and Responsibilities

4.1 Included in the Service

Renaissance provides:

- Scoping and rules of engagement definition
- Engagement management and delivery coordination
- Access coordination, scheduling and safe testing controls
- Technical testing of agreed targets delivered by an approved specialist testing partner
- Technical evidence capture and analysis (testing party), with findings triage and remediation prioritisation (Renaissance)
- Penetration testing report provided as part of the assurance pack (Renaissance-branded unless CREST is required)
- Renaissance assurance pack: remediation guidance and prioritised action plan
- Optional remediation validation / retest coordination (where agreed)

4.2 Buyer Responsibilities

The Buyer is responsible for:

- Providing written authorisation for testing
- Defining and approving the testing scope
- Ensuring relevant system owners and stakeholders are informed
- Providing access details and test accounts where required
- Implementing remediation actions following testing

4.3 Specialist Testing Partner Responsibilities

The specialist testing partner delivers the technical testing activities and certified assessor review in line with the agreed scope and rules of engagement. For CREST-accredited engagements, the partner issues and brands the final CREST report. For non-CREST engagements, the report is provided within the Renaissance assurance pack. Renaissance coordinates delivery, provides governance and communication, and remains accountable to the Buyer for overall service delivery. Where a Buyer requires a specific accreditation/format (e.g., CREST), this is delivered via an appropriately accredited testing partner and confirmed at call-off.

5. Testing Approach and Methodology

Technical testing is delivered by the approved specialist testing partner in line with recognised industry best practice and ethical standards. Renaissance manages planning, governance, coordination, and findings triage to minimise operational risk and avoid unnecessary disruption to live services.

The approach typically includes:

1. Planning and scoping
2. Rules of engagement and safety controls
3. Reconnaissance and discovery
4. Vulnerability identification
5. Exploit validation and impact assessment
6. Reporting and remediation guidance
7. Remediation validation / retest (where agreed)

6. Service Features

- Scoping and Rules of Engagement (RoE) pack
- Engagement management, access coordination and scheduling
- Technical testing delivered by an approved specialist testing partner with certified assessor review
- Findings triage, risk rating and remediation prioritisation
- Evidence pack and report provided within our assurance pack
- Optional remediation planning workshop and retest coordination
- Ongoing / periodic validation option (agreed cadence)
- Safe testing controls and escalation routes for critical findings

7. Benefits

- Faster testing cycles without sacrificing coverage
- Improved visibility of testing progress and findings
- Early identification of new risks as environments change
- Identification of exploitable weaknesses before malicious actors
- Validation of real-world impact rather than theoretical issues
- Assurance that data exfiltration controls function as intended
- Clear prioritisation and evidence for remediation decisions
- Support for audit and regulatory assurance requirements
- Reduced false positives through validation of findings and impact assessment
- Safe testing aligned to agreed boundaries

8. Engagement Model and Deliverables

Each engagement is delivered as a defined piece of work agreed at call-off, with Renaissance acting as prime contractor. Technical testing and certified assessor review are delivered by the approved specialist testing partner.

Deliverables typically include:

- Penetration testing report provided within the assurance pack
- Risk-rated findings and severity assessment
- Technical evidence and reproduction steps (as applicable)
- Executive summary suitable for senior stakeholders
- Remediation guidance and prioritised action plan (Renaissance assurance pack)
- Optional remediation validation / retesting confirmation (where agreed)

9. Service Management and Support

9.1 Support Channels

- Email or online ticketing
- Telephone support

9.2 Support Hours

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

9.3 Response Times

- Telephone calls responded to within one business hour
- Email or ticketing responses within 60 minutes during service hours

9.4 Support Levels

- 1st, 2nd and 3rd line support
- Named Technical Account Manager (TAM) for engagement coordination

10. Security, Assurance and Ethics

Technical testing is conducted only with explicit written authorisation and agreed scope, and is delivered by the approved specialist testing partner. Testing adheres to ethical standards and safe testing practices, including:

- Defined rules of engagement

- Exclusion of out-of-scope targets
- Controlled exploitation within agreed boundaries to avoid unnecessary service impact
- Clear escalation routes for critical findings

Testing does not include social engineering or physical security testing unless explicitly agreed.

11. Availability and Scheduling

Testing is scheduled by agreement. For production systems, testing windows may be required to manage operational risk. Scheduling is coordinated with the Buyer to minimise disruption.

12. Exit and Retention of Materials

At the conclusion of an engagement, reports and evidence are provided to the Buyer. Testing data and artefacts produced during delivery (including those produced by the specialist testing partner) are retained or deleted/returned as agreed at call-off, in accordance with contractual terms and applicable data protection requirements.

13. Assumptions and Constraints

Testing is performed only with written authorisation and agreed scope. Out-of-scope targets and social engineering activities are excluded unless explicitly agreed. Testing windows may be required for production systems. CREST-accredited reports are issued by the accredited testing partner where required.

14. Document Control

Item	Value
Document title	Service Definition Document – Managed Penetration Testing & Remediation Support
Supplier	Renaissance Computer Services Ltd
Version	2.0
Last updated	30 Jan 2026

Item	Value
Review cycle	Annual or upon material change