Service Definition Document

Managed Cloud Security Services

Rosebud Cloud Solutions
G-Cloud 15 – Lot 3: Cloud Support

## 1. Overview

Rosebud Cloud Solutions' *Managed Cloud Security Services* help public sector organisations strengthen their cloud security posture through strategic planning, risk management, secure design, and assurance activities. The service covers incident response planning, audit services, QA testing, and threat modelling to ensure resilient, compliant cloud environments aligned with UK public sector standards. It supports secure digital transformation by protecting sensitive data and enabling confident cloud adoption.

## 2. Service Summary

### Service Name

Managed Cloud Security Services

### Service Type

Lot 3 – Cloud Support

### Service Description

Rosebud's Cloud Support: Security Services provide strategic and operational support to enhance cloud security. The service includes security strategy development, risk management, secure architecture design, incident response planning, audit services, and quality assurance testing. It ensures public sector organisations maintain strong, compliant, and resilient cloud environments.

### Service Categories

- Security Services
- Security Strategy
- Security Risk Management
- Security Design
- Security Incident Management
- Security Audit Services

- Security Quality Assurance (QA) and Testing

## 3. Service Features and Benefits

### 3.1 Features

- Cloud security strategy development
- Risk identification and mitigation planning
- Secure architecture design
- Incident response planning
- Security audit services
- Quality assurance and penetration testing
- Compliance mapping and gap analysis
- Threat modelling and simulation
- Access control and identity review
- Security tooling recommendations

### 3.2 Benefits

- Strengthens cloud security posture
- Reduces risk of breaches
- Enhances incident response readiness
- Supports regulatory compliance
- Improves system resilience
- Identifies vulnerabilities early
- Builds stakeholder confidence
- Aligns security with business goals
- Enables proactive threat management
- Protects sensitive public sector data

## 4. Service Scope

### 4.1 Included

- Security strategy and roadmap development

- Cloud security risk assessments
- Secure architecture and design recommendations
- Incident response planning and playbook creation
- Security audits and compliance reviews
- Penetration testing and QA activities
- Threat modelling and simulation workshops
- Identity and access management reviews
- Security tooling and control recommendations
- Standard onboarding and documentation

### 4.2 Not Included

- Implementation of security tooling (available separately)
- Remediation of vulnerabilities (available separately)
- Onsite delivery (available at extra cost)
- Extended support packages (quoted separately)

## 5. Service Constraints

- Requires access to current system architecture, policies, and stakeholder input.
- Does not include implementation of security tooling unless separately contracted.
- Testing and audit activities may be limited by system availability or third-party restrictions.
- Recommendations may require further validation before execution.
- Deep customisation may require additional consultancy.
- Timelines depend on system complexity and stakeholder availability.

## 6. Reselling Information

### Supplier Type

Reseller providing additional features and support not available from the original supplier.

### Original Supplier

Microsoft

## 7. User Support

### 7.1 Support Channels

- Email or online ticketing: **Yes, at extra cost**
- Phone support: **No**
- Web chat support: **No**
- Onsite support: **Yes, at extra cost**

### 7.2 Support Response Times

- 1-hour initial response
- 2-day fix target
- 12-hour weekend response time (unless otherwise agreed)

### 7.3 Support Levels

- Standard support level (cost provided at discovery/quote stage)
- Dedicated technical account manager (qualified cloud engineer)

### 7.4 Support for Third Parties

Yes – support available to authorised third-party partners or managed service providers.

### 7.5 Accessibility

Compliant with EN 301 549.

## 8. How Users Access the Service

- Web browser interface: **No**
- Application installation: **No**
- Mobile-optimised interface: **No**
- Service interface: **No**
- API availability: **No**
- Customisation: **No**

## 9. Pricing

Pricing is provided during discovery and quotation, based on:

- Scope of security assessment and testing
- Number of systems and environments in scope
- Required depth of analysis and reporting
- Stakeholder engagement needs
- Optional onsite or extended support services

## 10. Onboarding and Offboarding

### 10.1 Onboarding

- Requirements and architecture review
- Stakeholder mapping and engagement planning
- Access and permissions setup
- Security assessment and testing schedule
- Governance and reporting structure definition

### 10.2 Offboarding

- Delivery of audit findings and security reports
- Removal of temporary access (if applicable)
- Optional follow-up review
- Optional transition to Managed Cloud Support Services

## 11. Security and Compliance

- Delivered using secure, approved cloud environments
- Aligns with UK public sector security and compliance frameworks
- Supports governance, risk management, and assurance requirements
- Reinforces secure-by-design principles

## 12. Service Management

Rosebud provides structured service management for security engagements, including:

- Risk and issue management
- Governance and reporting
- Stakeholder engagement
- Change and communication management
- Continuous improvement of security processes

## 13. Technical Roadmap

Rosebud continues to enhance the service through:

- Expanded threat modelling and simulation capabilities
- Enhanced automation for security assessments
- Additional sector-specific compliance templates
- Improved reporting and analytics tooling