

# Modern Desktop SecOps Consultancy Services

*Service Definition Document*

---

2026

Date  
January 2026

G-Cloud 15  
RM1557.15



# Contents

|                                                      |    |
|------------------------------------------------------|----|
| 1. Introduction.....                                 | 1  |
| 2. The Challenge .....                               | 2  |
| 3. Service Summary.....                              | 3  |
| 4. Key Service Capabilities .....                    | 4  |
| 5. Key Service Benefits .....                        | 5  |
| 6. Service Scope.....                                | 6  |
| 7. Service Transition .....                          | 7  |
| 8. Delivery Approach .....                           | 7  |
| 9. Prerequisites & Infrastructure Requirements ..... | 9  |
| 10. Customer Responsibilities .....                  | 10 |
| 11. Pricing Overview .....                           | 12 |
| 12. Service Levels & Performance.....                | 13 |
| 13. Quality and Service Assurance .....              | 14 |
| 14. Ordering and Invoicing .....                     | 15 |
| 15. Termination and Exit .....                       | 15 |
| 16. Further Information .....                        | 17 |
| 17. Additional Associated Services.....              | 17 |

# 1. Introduction

This service is provided by APPS DELIVERY, a specialist IT consultancy with experience supporting public sector organisations across Modern Desktop, Cloud, Security, and Digital Workplace environments. The consultancy works with organisations where desktop estates have evolved through multiple technologies, vendors, and operating models, resulting in complexity that is difficult to govern, modernise, or sustain.

Engagements are delivered as senior-led professional consultancy, combining technical expertise with operational insight to support clear, evidence-based decision-making.

The service focuses on reducing uncertainty and operational noise, enabling internal teams to concentrate on service delivery while desktop, endpoint, and application challenges are addressed through structured analysis and practical recommendations.

Delivery is aligned with recognised industry frameworks and applicable security and quality requirements, where required, providing consistency, assurance, and auditability. The consultancy acts as a bridge between architecture, security, operations, and delivery teams, aligning stakeholders around shared priorities and agreed next steps.

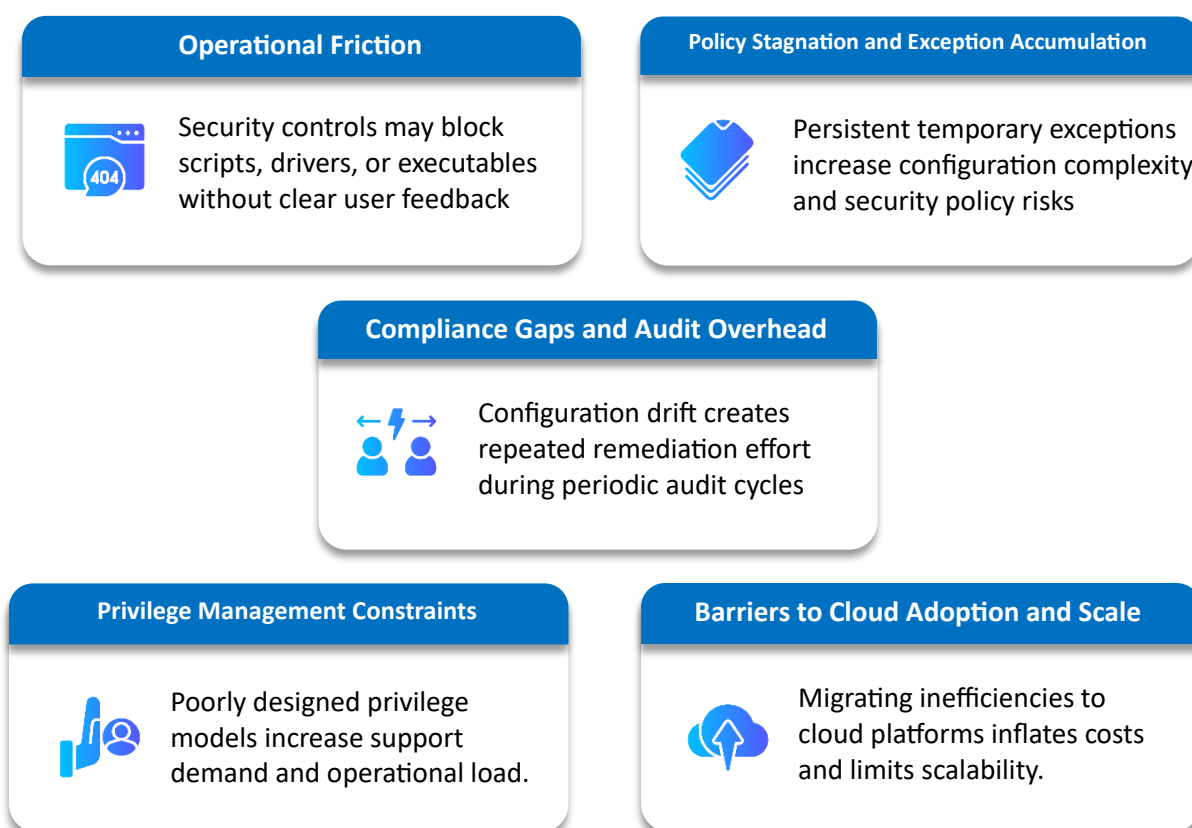
Scope, duration, and deliverables are agreed at call-off through the G-Cloud framework, ensuring services remain proportionate and aligned with organisational priorities and governance requirements.

This service provides advisory support to help organisations design, assess, and optimise endpoint security controls and operating models that balance protection, usability, and operational sustainability across modern desktop environments.

## 2. The Challenge

Public sector organisations are under sustained pressure to deliver a secure modern desktop that supports hybrid working while responding to an increasingly automated threat landscape. Endpoint security controls such as Ivanti Application Control, Windows App Control for Business, and Attack Surface Reduction are commonly used to support Zero Trust objectives. Over time, however, these controls can introduce operational friction and management complexity if not designed and maintained with day-to-day operations in mind.

Commonly observed challenges include:



**Operational friction and hidden productivity impact** - Security controls may block scripts, macros, drivers, or executables without clear user feedback. These behaviours can appear as application failures rather than security enforcement, increasing investigation effort for service desks and delaying routine user activity.

**Policy stagnation and exception accumulation** - As applications and user requirements change, security policies require ongoing review and tuning. Without a defined strategy, temporary exceptions such as elevated privileges or relaxed rules may persist, increasing configuration complexity and security risks.

**Compliance gaps and audit overhead** - Security frameworks and standards are often applied as point-in-time activities. In the absence of continuous evidence collection and monitoring, configuration drift can occur, leading to repeated remediation effort and increased demand on specialist resources during audit cycles.

**Privilege management constraints** - Applying least-privilege principles can create tension between security objectives and operational needs. Where privilege management is not well-designed, users may retain broad rights or require frequent manual intervention for routine tasks, increasing support demand and operational load.

**Barriers to cloud adoption and scale** - When organisations adopt platforms such as Windows 365, Azure Virtual Desktop or Citrix Cloud, existing security and configuration inefficiencies may be migrated unchanged. This can increase technical debt, inflate operating costs, and limit confidence in adopting native cloud security capabilities at scale.

### 3. Service Summary

The Modern Desktop SecOps Consultancy Services provide specialist professional support to public sector organisations seeking to design, refine, and operate endpoint security controls within modern desktop environments. The service focuses on aligning security policy intent with day-to-day operational requirements to support secure, usable, and supportable endpoints.

It covers consultancy activities relating to endpoint security controls such as application control, attack surface reduction, privilege management, and compliance baselines. Engagements may include assessment of existing configurations, security policy design, configuration rationalisation, and advisory support for integrating security controls within modern desktop platforms, subject to the scope agreed at call-off.

Services are delivered as consultancy engagements rather than managed operations. The service may be used to address security and operational challenges within existing environments or to support the adoption and scaling of cloud-based desktop platforms, where this forms part of the agreed scope.

## 4. Key Service Capabilities

The following capabilities describe the specialist consultancy activities that may be delivered under this service. The specific combination, depth, and application of these capabilities are determined by the buyer's requirements and are defined at call-off through the Statement of Work.

- **Telemetry-driven security assessment** - Assessment of existing endpoint security configurations using available telemetry and logging to understand policy behaviour, enforcement impact, and operational alignment.
- **Application control policy design** - Design and review of application control policies, including App Control for Business or Ivanti Application Control, to support secure execution while minimising operational disruption.
- **Attack surface reduction optimisation** - Advisory support for the design, tuning, and validation of ASR rules to balance security enforcement with application and user requirements.
- **Privilege management and EPM design** - Design of privilege management approaches that support least-privilege operation through role-based, contextual, or time-bound elevation models.
- **Security policy architecture and lifecycle support** - Consultancy support for structuring, documenting, and maintaining endpoint security policies to reduce exception sprawl and unmanaged configuration growth.
- **Compliance baseline advisory** - Advisory support for aligning endpoint configurations with recognised security baselines and standards.
- **Legacy configuration rationalisation** - Review and rationalisation of legacy endpoint security rules and policies to reduce technical debt and configuration complexity.
- **Cloud desktop security advisory** - Consultancy support for applying and adapting endpoint security controls within cloud-hosted desktop platforms.
- **Monitoring, audit, and evidence advisory** - Design support for the use of logging and security telemetry to assist with audit, assurance, and ongoing security review activities.
- **Documentation and knowledge transfer** - Provision of documentation and knowledge transfer to support internal teams in maintaining and evolving endpoint security controls.

## 5. Key Service Benefits

The service may provide the following benefits, subject to the agreed scope:

- **Reduced operational friction** - Better alignment between security controls and application behaviour can reduce unexpected enforcement outcomes and associated investigation effort.
- **Improved policy maintainability** - Policy design and lifecycle support can help limit exception sprawl and reduce the operational risk of security changes.
- **Lower audit overhead** - Improved visibility and evidence collection can reduce the effort required to demonstrate compliance during audit activities.
- **Balanced privilege management** - More targeted privilege management approaches can reduce reliance on broad administrative rights while supporting routine operational needs.
- **Improved support efficiency** - Clearer security enforcement behaviour can reduce misdiagnosis of security issues as application or platform faults.
- **Reduced technical debt** - Rationalisation of legacy security configurations can improve long-term maintainability of endpoint security controls.
- **Improved cloud security readiness** - Better-aligned security controls can support more predictable adoption and scaling of cloud-hosted desktop platforms.
- **Increased operational confidence** - Improved understanding of policy intent and behaviour can support more controlled security change and decision-making.
- **Knowledge retention** - Documentation and knowledge transfer can reduce reliance on individual expertise and support continuity within internal teams.

## 6. Service Scope

The scope of activities delivered under this service is defined by the buyer at call-off and documented within the Statement of Work.



### In-Scope – Consultancy Activities

**All in-scope activities below are consultancy-based and do not include operational ownership or ongoing management of customer environments. In-scope activities may include:**

- consultancy, assessment, and advisory services relating to endpoint security controls
- review, design, and rationalisation of application control, attack surface reduction, and privilege management configurations
- advisory support for security policy architecture, lifecycle management, and exception handling approaches
- consultancy support for aligning endpoint security controls with recognised security baselines and standards, where applicable
- advisory support for applying endpoint security controls within cloud-hosted desktop platforms
- documentation and knowledge transfer activities aligned to the agreed scope



### Out-of-Scope – Not included

**The following activities are explicitly out of scope unless separately agreed under another service or documented within a separate Statement of Work:**

- desktop build, configuration, or image engineering
- provision, hosting, or operation of customer infrastructure, platforms, or security services
- procurement, provisioning, or licensing of hardware, software, or cloud services
- ongoing managed security operations, monitoring, or service desk support
- direct end-user support or first- and second-line incident handling
- network, firewall, or perimeter security management
- penetration testing, red team exercises, or formal security assurance activities
- data migration activities unrelated to endpoint security configuration

## 7. Service Transition

Service transition covers the activities required to initiate and conclude an engagement in a controlled and proportionate manner. Transition activities are scaled to the scope, duration, and complexity of the engagement and are defined within the Statement of Work.



### On-boarding

**On-boarding activities are undertaken at the start of the engagement to enable delivery to commence effectively. These activities may include:**

- confirmation of the agreed scope, objectives, deliverables, and constraints
- confirmation of the agreed scope, objectives, deliverables, and constraints
- confirmation of roles, responsibilities, and points of contact
- agreement of delivery arrangements, governance, and reporting mechanisms
- confirmation of access, information, and prerequisite readiness

**The extent and format of on-boarding activities are proportionate to the engagement and are documented within the Statement of Work.**



### Off-boarding

**Off-boarding activities are undertaken at the conclusion of the engagement or upon early termination, where applicable. These activities are intended to support an orderly close-down of delivery and may include:**

- confirmation that agreed activities or deliverables have been completed
- handover of documentation or outputs produced as part of the service
- return or secure deletion of customer-provided information, where applicable
- confirmation that no ongoing service delivery or operational support is provided beyond the end of the engagement

**Any off-boarding support is limited to what is defined within the Statement of Work or agreed as part of termination arrangements.**

## 8. Delivery Approach

The service is provided as specialist professional support, scoped and governed through a clearly defined engagement agreed at call-off. Delivery is collaborative and proportionate to the size, complexity, and duration of the engagement.

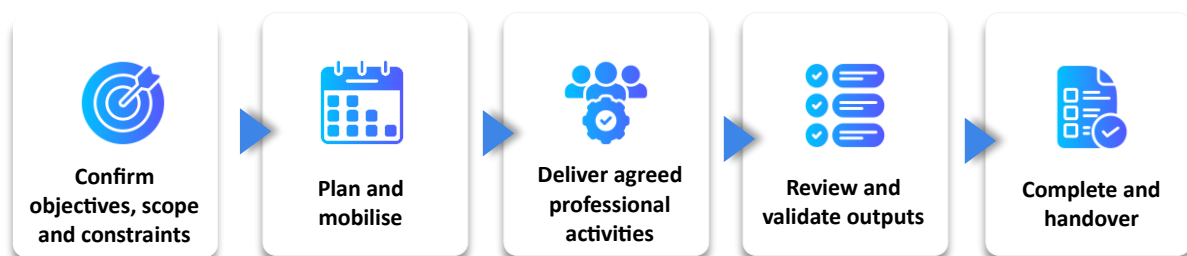
The delivery approach is designed to provide clarity, transparency, and control while avoiding unnecessary overhead. It does not imply managed service delivery, operational ownership, or ongoing responsibility for customer environments.

## Engagement Structure

Delivery follows a lifecycle appropriate to consultancy-based services, which may include:

- confirmation of objectives, scope, and constraints
- planning and mobilisation aligned to the agreed scope
- delivery of agreed professional activities
- review and validation of outputs against agreed objectives
- completion and handover of deliverables or outcomes, where applicable

The specific activities, sequence, and outputs are defined and documented within the Statement of Work.



## Collaboration and Governance

Delivery is based on collaboration between the customer and APPS DELIVERY, with defined points of contact on both sides. Governance arrangements are proportionate to the engagement and may include agreed review points, progress updates, and reporting mechanisms.

Decision-making authority remains with the customer at all times. Delivery is aligned with the customer's internal governance, assurance, and change control processes, where applicable and agreed.

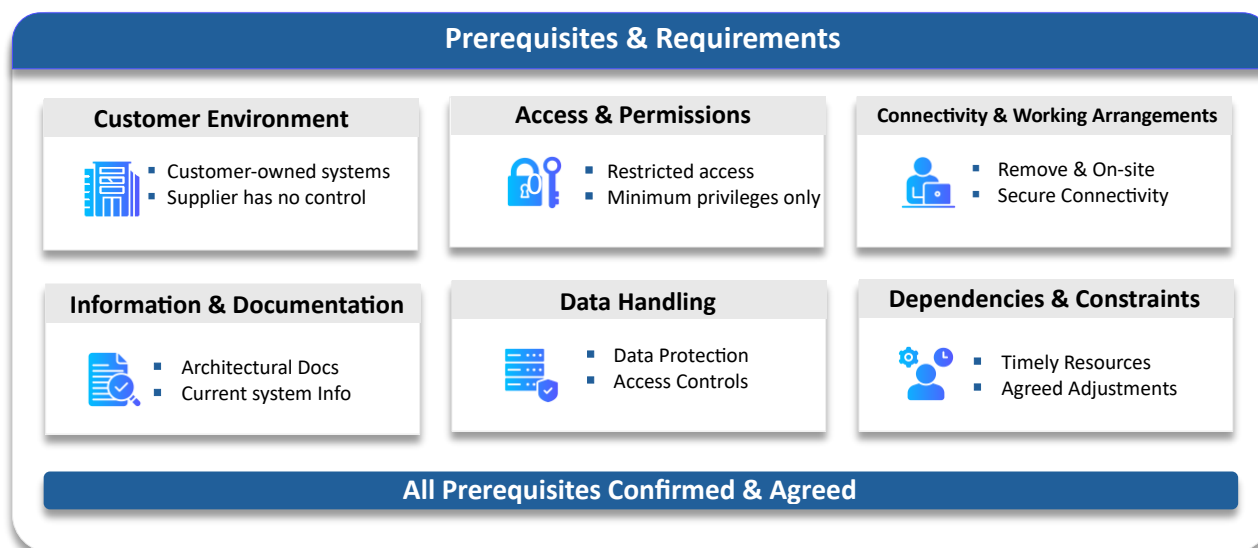
## Flexibility and Proportionality

The delivery approach is intentionally flexible and can be adapted to suit short, targeted engagements or longer-running pieces of work. The level of structure, interaction, and reporting is scaled to reflect the agreed scope and delivery model.

Any changes to scope, priorities, or delivery approach are subject to mutual agreement and managed in accordance with the arrangements set out in the Statement of Work.

## 9. Prerequisites & Infrastructure Requirements

The delivery of this service is subject to a number of organisational, technical, and access-related prerequisites being in place prior to commencement. These prerequisites define the conditions required to enable delivery and do not transfer ownership, operational responsibility, or control of customer environments to the supplier. All prerequisites are confirmed and agreed at call-off.



### Customer Environment

The service is delivered within environments agreed for the purposes of the engagement. APPS DELIVERY does not host, operate, or assume responsibility for customer infrastructure, platforms, or services as part of this service.

The specific environments, platforms, and technologies involved will depend on the scope of the engagement and will be documented within the Statement of Work.

### Access and Permissions

Where required to deliver the agreed scope, appropriate access must be provided to relevant systems, platforms, or information. Access levels are limited to the minimum privileges necessary to perform agreed activities and are granted in accordance with the customer's security, identity, and access management policies.

The method of access provisioning, approval processes, and security controls (including any requirements for authentication or privileged access) remain under the customer's control.



## Information and Documentation

To support delivery, relevant and current information may be required. This may include architectural documentation, configuration information, operational procedures, or other artefacts necessary to understand the existing environment, aligned to the agreed scope of work.

## Connectivity and Working Arrangements

Services are delivered primarily on a remote basis. Where on-site activity is required, this is agreed in advance. Secure connectivity to customer environments must be available for the duration of the engagement.

Any constraints relating to connectivity, network access, or working arrangements that may affect delivery are agreed and documented prior to commencement.

## Data Handling

Where access to configuration data, logs, or operational information is required, such access is limited to what is necessary to deliver the agreed scope. Data handling requirements are defined by the customer and are managed in accordance with applicable policies, contractual obligations, and relevant data protection requirements.

## Dependencies and Delivery Constraints

Delivery of the service is dependent on the timely availability of agreed prerequisites, including access, information, connectivity, and relevant customer resources. Where prerequisites are not met or constraints arise within the customer environment, the scope, timeline, or delivery approach may need to be adjusted by mutual agreement.

Any agreed adjustments are managed through the governance arrangements defined and documented within the Statement of Work.

# 10. Customer Responsibilities

The customer is responsible for meeting its obligations under the applicable G-Cloud terms and conditions, including (but not limited to) obligations relating to acceptable use, data protection, information security, confidentiality, intellectual property, and payment terms.

To enable effective delivery of the service, the customer is responsible for:

- Providing overall coordination and oversight for the engagement, including acting as the primary point of escalation for service-related matters.

- Ensuring that appropriate decision-making authority is available to support timely approvals, direction, and resolution of issues.
- Confirming scope, priorities, and constraints at call-off and approving any subsequent changes in accordance with agreed arrangements.
- Ensuring that required customer-owned environments, platforms, services, licences, and resources are available and in service, unless explicitly stated otherwise in the Statement of Work.
- Completing any agreed preparatory activities prior to the commencement of delivery
- providing timely physical and/or remote access to systems, locations, and information required to deliver the agreed scope.
- Ensuring that appropriate security access, credentials, and approvals are granted in line with internal policies.
- Making relevant personnel available, as reasonably required, to support delivery activities, including provision of information, clarification, and validation.
- Nominating primary and secondary contacts for technical, operational, and commercial matters.
- Managing internal communications and coordination with stakeholders impacted by delivery activities.
- Providing accurate, complete, and timely information required to support delivery
- informing APPS DELIVERY of any organisation-specific policies, standards, procedures, or constraints that may reasonably affect delivery.
- Raising and escalating concerns relating to scope, quality, or delivery impacts in a timely manner.

These responsibilities are intended to support effective collaboration and delivery.

## 11. Pricing Overview

Pricing for this service is based on the deployment of specialist professional resources using fixed daily rates, as published in the supplier's role-based pricing catalogue. All pricing is transparent and derived solely from the published rates.

Services are delivered on a time and materials basis. Where activities and deliverables are clearly defined and bounded, a fixed price may be agreed. Any fixed price is derived directly from the same published daily rates.

### Pricing Basis

- Pricing Model: Role-based daily rates
- Charging Method: Time and Materials
- Fixed Price: May be agreed at call-off where applicable, derived from published rates

The roles, number of days, and duration required to deliver the service are determined by the buyer.

### Pricing Assumptions

The following assumptions apply unless otherwise agreed:

- Working Day: A standard working day consists of 7.5 hours, exclusive of travel and lunch.
- Working Schedule: Monday to Friday, excluding UK public and national holidays, during standard UK business hours.
- Out-of-Hours Delivery: Delivery outside standard UK business hours, including evenings, weekends, or public holidays, is provided only where explicitly agreed.
- Delivery Location: Services are delivered primarily on a remote basis. Any on-site delivery must be agreed in advance.
- Travel and Expenses: Approved travel and subsistence costs may be charged at actual cost, with no uplift, where agreed in advance and approved by the buyer, in line with public sector guidance.
- VAT: All rates and charges are exclusive of VAT.

No discounts, bundled pricing, volume-based adjustments, or cross-service pricing arrangements apply.

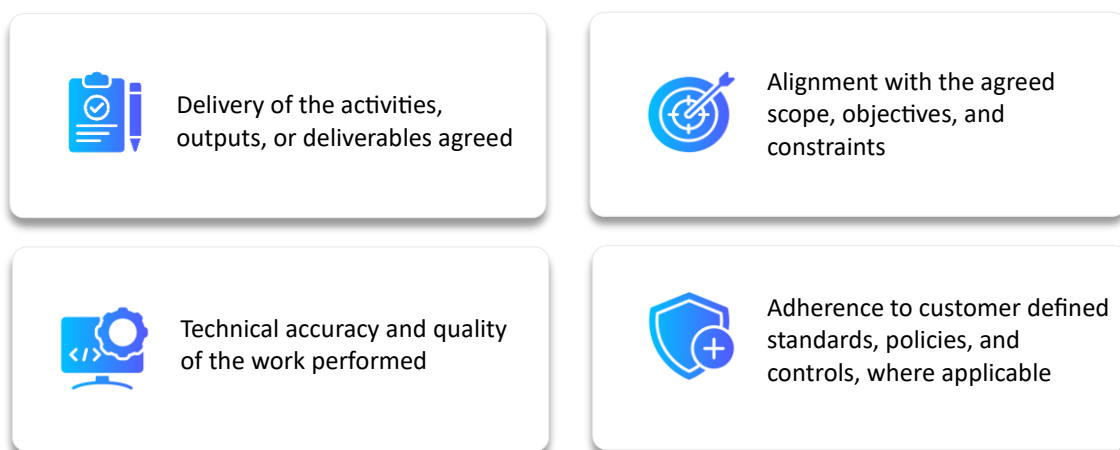
## 12. Service Levels & Performance

Service performance for this service is assessed against the delivery of agreed activities, outputs, or deliverables defined at call-off. Performance measurement is proportionate to the nature, scope, and duration of the engagement and does not imply managed service delivery or ongoing operational responsibility.

All performance measures are agreed in advance with the customer and documented within the Statement of Work.

### Performance Measurement Principles

Service performance is measured based on:



**No standard service levels, service credits, or availability guarantees apply unless explicitly agreed**

### Consultancy-Based Engagements

For consultancy-led engagements, performance is assessed against the completion of agreed activities and milestones. This may include:

- delivery of agreed professional services within the defined scope
- completion of activities or milestones as set out in the Statement of Work
- provision of outputs, advice, or recommendations aligned to the engagement objectives

### Deliverable-Based Engagements

Where the engagement includes defined deliverables, performance is assessed on a per-deliverable basis against acceptance criteria agreed in advance. Acceptance criteria may include confirmation that the deliverable:

- has been produced in accordance with the agreed scope
- meets the documented requirements or specifications
- is suitable for use within the customer's agreed environment

## Performance Reporting and Transparency

Performance reporting is proportionate to the engagement and may include progress updates, confirmation of completed activities or accepted deliverables, and identification of risks, dependencies, or decisions required.

## 13. Quality and Service Assurance

Quality and service assurance are applied to support the consistent and controlled delivery of professional services in line with the agreed scope. Assurance activities are proportionate to the nature and scale of the engagement and are defined at call-off.

This section describes the assurance controls that may be applied. It does not define service levels, performance targets, or operational guarantees.

### Assurance Controls

Quality assurance may include the application of one or more of the following controls, where appropriate to the engagement:

- internal peer review of technical outputs
- validation of deliverables or outputs against the agreed scope and requirements
- alignment checks against customer-defined standards, policies, and controls, where applicable
- review of documentation for completeness and clarity

### Governance and Oversight

Assurance activities are conducted within the governance arrangements agreed for the engagement. This may include periodic review points to confirm that delivery remains aligned to the agreed scope and objectives.

Any issues identified through assurance activities are raised with the customer and addressed in accordance with the agreed delivery and governance arrangements.

## Knowledge Transfer and Documentation

Where applicable to the scope, assurance activities may include confirmation that relevant documentation or knowledge transfer outputs have been produced in line with the agreed requirements.

## Security and Compliance Considerations

Where the service involves access to customer environments, data, or information, assurance activities may consider applicable customer security, information governance, and compliance requirements, as defined by the customer.

# 14. Ordering and Invoicing

## Ordering

This service is ordered by the buyer through a G-Cloud call-off agreement in accordance with the G-Cloud framework rules and associated contractual documentation.

The scope, duration, roles, volume of effort, delivery approach, and any service-specific requirements are agreed at call-off and documented within the Statement of Work.

No alternative procurement routes are supported.

## Invoicing

Invoicing is based on the pricing model and rates agreed at call-off and documented within the Statement of Work.

Invoices are raised in arrears in accordance with the agreed charging basis and are subject to buyer approval in line with the terms of the agreement.

The invoicing frequency, supporting information, and approval process are agreed at call-off.

# 15. Termination and Exit

Termination of this service is governed by the terms and conditions of the applicable G-Cloud call-off agreement.

The service may be terminated by the buyer in accordance with the call-off agreement, including where termination is required for convenience or as otherwise provided for under the contract.

## Exit Support

Upon termination or expiry of the service, we will provide reasonable exit support where required and agreed. Exit support is limited to activities necessary to support an orderly conclusion of the engagement and does not include ongoing service delivery beyond the end of the contract.

Where applicable to the scope, exit support may include:



Confirmation that agreed deliverables or outputs have been completed



Handover of documentation or materials produced as part of the service



Return or secure deletion of customer-provided information in accordance with contractual and data protection requirements

The scope and duration of any exit support are agreed at call-off or as part of the termination arrangements.

## No Lock-In

The service is delivered in a manner that avoids dependency on APPS DELIVERY beyond the term of the call-off agreement. No exclusivity, continuity, or ongoing engagement is implied beyond the agreed service period.



## 16. Further Information

Further information relating to this service, including contractual terms, service descriptions, and pricing, is provided through the supplier's G-Cloud 15 framework listing and associated framework documentation.

Buyers should refer to the relevant G-Cloud framework materials for details of call-off terms, buyer and supplier obligations, and applicable policies.

No additional information outside the G-Cloud framework documentation forms part of this service unless explicitly agreed at call-off.

## 17. Additional Associated Services

APPS DELIVERY offers other services that may be procured separately under the G-Cloud framework. These services are not included within the scope of this service and are not required for its delivery.

The availability, scope, pricing, and terms of any additional services are determined independently at call-off.

Additional associated services may include:

- Application Repackaging and Lifecycle Management Services
- Desktop Engineering Consultancy Services
- Ivanti User Workspace Consultancy Services
- Modern Desktop Consultancy Services

No dependency, delivery linkage, or preferential pricing applies between this service and any additional associated services.



## APPS DELIVERY | Confidence Through Engineering

**Tel:** +44 (0) 7391736261

**Email:** [GCloud@appsdelivery.co.uk](mailto:GCloud@appsdelivery.co.uk)

**Web:** [www.appsdelivery.co.uk](http://www.appsdelivery.co.uk)

