mvw CONSULTANCY SERVICES

SERVICE DEFINITION

CLOUD CONSULTANCY

JANUARY 2026

Prepared for:

mvw CONSULTANCY SERVICES

TABLE OF CONTENTS

1. THIS DOCUMENT

This document is the MVW Service Definition for Cloud Support version January 2026.

This document defines MVW Cloud Consultancy for G-Cloud Lot 3 (Cloud Support), using the service structure Cloud Migration Planning. It describes how the service is delivered, what is included, and the service boundaries. Client-specific scope, deliverables, and commercial terms are agreed in a statement of work (SoW).

Prepared by Alistair Ross on January 2026.

1.1 ABOUT MVW TECHNOLOGY LIMITED

MVW Technology Limited are a technology consultancy and managed service provider who specialise in delivering a Modern Workplace and IT Infrastructure services.

Our focus in this field enables us to remain in touch with the evolution of end-user and infrastructure technologies and apply innovative and effective solutions to meet business needs, whilst aligning to operational, security and regulatory requirements.

Our senior consultants each have over 25 years of experience each in top tier organisations including leading investment and retail banks.

1.2 VERSION HISTORY

VERSION	DATE	AUTHOR	UPDATES
2601	09 Jan 2026	Alistair Ross	Updated document to support G-Cloud

1.3 TERMS USED

The following terms may be used throughout this document:

- Client: the buying organisation receiving consultancy services.
- SoW: statement of work defining deliverables, timescales, and commercial terms.
- Architecture forum: a governance group that reviews options and approves target designs.
- Workload: an application, service, database, server, platform component, or data set in scope for migration planning.

2. SERVICE DESCRIPTION (CLOUD MIGRATION PLANNING)

MVW's specialist cloud advisory service, helping public-sector organisations define cloud strategy, assess readiness, and build business cases aligned to government standards. The service includes cloud migration planning and architecture advisory across multi-cloud environments. The primary focus is Microsoft cloud, including Microsoft Azure, Microsoft 365 and Amazon Web Services (AWS).

The service produces a migration plan, roadmap, and design decisions suitable for delivery by the client, MVW delivery teams, or a third party.

Delivery is primarily remote. On-site workshops and design sessions can be provided where required. The service is designed for medium sized organisations.

2.1 WHAT THE SERVICE DOES

The service helps clients plan a controlled migration to cloud services, aligned to operational needs, security requirements, and compliance obligations.

Core activities include:

- Cloud migration planning and wave design
- Capability analysis
- Cloud readiness assessment
- Enterprise architecture inputs and target state definition
- Cloud gap assessment and remediation backlog creation
- Architecture options analysis (risk, cost, complexity, operational impact)
- Delivery road-mapping and prioritised work packages

2.2 WHAT THE SERVICE IS COMPRISED OF

The service structure is Cloud Migration Planning. It is delivered through the phases below. Each phase can be delivered as a single engagement or as staged work packages.

1. **Mobilise and scope:** confirm objectives, success criteria, stakeholders, and the workload list in scope.

2. **Discover:** collect current state information, dependencies, and constraints using workshops and evidence review.
3. **Assess and classify:** assess workloads, group them into migration paths, and identify prerequisites and risks.
4. **Design and decide:** produce options and recommendations, then capture decisions through an architecture forum (where used).
5. **Plan and roadmap:** create the migration wave plan, runbook approach, and delivery roadmap with priorities and dependencies.
6. **Handover and knowledge transfer:** provide the deliverables pack, walkthrough sessions, and close-out actions.

2.3 DELIVERABLES AND OUTPUTS

Deliverables are confirmed in the Statement of Work (SoW). Typical deliverables for Cloud Migration Planning include:

- Cloud readiness and capability assessment (people, process, technology, governance).
- Workload inventory and dependency mapping summary.
- Per-workload assessment outputs, for example a one-to-three-page Definition of Work (DOW) per workload.
- Migration path classification (for example rehost, re-platform, refactor, replace, retire, retain).
- Target architecture pack covering landing zone, identity, networking, security controls, governance, and operations.
- Migration wave plan with sequencing, dependencies, and cutover approach.
- Migration runbook outline per wave, including roles, steps, checks, and rollback approach.
- Risk, assumptions, issues, and dependencies (RAID) log and mitigation actions.
- Roadmap and prioritised backlog of work packages for delivery.

2.4 SERVICE SCOPE AND BOUNDARIES

Baseline scope is advisory and architecture for migration planning. Hands-on delivery activity is only included where explicitly authorised in the SoW.

In scope (typical):

- Workshops, interviews, and evidence collection.
- Review of existing documentation and technical artefacts.
- Design of target state and migration approach, including standards and decision records.
- Advisory input on tooling choices for migration planning (for example assessment tools, dependency mapping, and runbook approaches).
- Support to client delivery teams through design clarification and design assurance where included.

Out of scope by default:

- Execution of migrations and cutovers (delivery), unless included in a separate SoW.
- 24x7 operational monitoring and incident response (managed service).
- End user service desk support.
- Software licensing resale or procurement on behalf of the client.
- Formal audit sign-off or legal representation.

2.5 LIMITATIONS AND EXCLUSIONS

Outputs depend on the accuracy and completeness of information provided by the client and the availability of client stakeholders.

Where the client requires detailed low-level designs (LLD's) or build artefacts, this is treated as additional scope and agreed in the SoW.

2.6 CLOUD MIGRATION PLANNING

Purpose:

- Create a structured migration plan that sequences workloads into waves and defines the approach to assessment, design, testing, cutover, and handover.

Activities:

- Confirm the workload list and ownership. Create a baseline inventory and classify workloads.
- Perform dependency mapping and identify shared services that gate migration waves.
- Classify each workload into a migration path (for example rehost, replatform, refactor, replace, retire, retain).
- Define wave plan sequencing with prerequisites, testing, and cutover approach.
- Define runbook structure, roles, checks, and rollback approach per wave.
- Define communications approach and governance for go or no-go decisions.

Inputs required:

- Workload inventory, service ownership, and technical contacts.
- Current state architecture and constraints (network, identity, security, operations).
- Known business events and blackout periods.
- Client risk appetite and change control constraints.

Outputs:

- Workload list and dependency mapping summary.
- Per-workload definition of work (DOW) where required.

- Migration wave plan with sequencing, assumptions, and dependencies.
- Runbook outline per wave and cutover governance approach.

Acceptance criteria (typical):

- Workload list is agreed with named owners.
- Each workload has a documented migration path and key dependencies.
- Wave plan has clear prerequisites and go or no-go checkpoints.
- Risks and assumptions are recorded and owned.

Service boundary:

- This component produces the plan and supporting artefacts. Execution of migrations is separate unless agreed in the SoW.

2.7 CAPABILITY ANALYSIS

Purpose:

- Assess organisational capability to deliver and operate cloud services. Identify skills gaps, process gaps, and governance gaps that affect migration delivery and live operations.

Activities:

- Run stakeholder interviews and workshops across technology, security, operations, and business owners.
- Assess current processes and tools against the target operating approach.
- Identify capability gaps that create delivery risk or operational risk.
- Create a capability improvement plan aligned to the migration roadmap.

Inputs required:

- Organisation structure and role ownership information.
- Existing operational process documentation (change, incident, problem, release).
- Current tooling list (monitoring, backup, security, ITSM).

Outputs:

- Capability assessment report with prioritised recommendations.
- Roles and responsibility gaps list with proposed owners.
- Inputs to the remediation backlog and delivery roadmap.

Acceptance criteria (typical):

- Key capability gaps are mapped to specific migration and operational risks.
- Recommendations include ownership and suggested sequencing.

2.8 CLOUD READINESS ASSESSMENT

Purpose:

- Assess readiness for cloud migration and cloud operations, and identify prerequisites required before migrations begin.

Activities:

- Assess platform readiness: tenancy, subscriptions, identity integration, connectivity, and baseline governance.
- Assess security readiness: access control, logging, encryption approach, and compliance obligations.
- Assess operations readiness: monitoring, backup, patching, change control, and incident management.
- Assess workload readiness: dependency health, version compatibility, and technical debt drivers.
- Produce readiness findings with priority actions and ownership.

Inputs required:

- Current state architecture artefacts and inventories.
- Access to relevant administration portals for evidence gathering, where permitted.
- Client security and compliance requirements.

Outputs:

- Readiness assessment report with prioritised actions.
- Prerequisite checklist for migration waves.
- Input to the remediation backlog and roadmap.

Dependencies:

- Readiness outcomes depend on access to accurate inventories, current documentation, and availability of technical owners.

2.9 ENTERPRISE ARCHITECTURE INPUTS AND TARGET STATE DEFINITION

Purpose:

- Define a target cloud architecture that aligns to business objectives and operational constraints, and supports safe migration execution.

Activities:

- Confirm enterprise principles and guardrails (security, data handling, resilience, operational model).
- Define target state architecture for identity, networking, security, governance, and operations.
- Define reference patterns for common workload types (IaaS, PaaS, SaaS, Microsoft 365 workloads).
- Produce architecture artefacts for approval (HLD and, where required, LLD).
- Capture decisions and exceptions through an agreed governance process.

Inputs required:

- Business objectives and service criticality requirements.
- Operational constraints and support model.
- Security and compliance requirements.

Outputs:

- Target architecture pack (diagrams, standards, and decision records).
- Landing zone design summary and operating model considerations.
- Standards catalogue and reference patterns (amendable).

Service boundary:

- Architecture definition includes design and documentation. Detailed engineering build tasks are not included unless stated in the SoW.

Examples that can be amended:

- Target state: Azure landing zone with management groups, subscription segregation, policy baseline, and central logging.
- Target state: Microsoft 365 tenant baseline for identity governance, device management approach, and information protection.
- Connectivity option set: site-to-site VPN versus ExpressRoute, depending on bandwidth and resilience requirements.

2.10 CLOUD GAP ASSESSMENT AND REMEDIATION BACKLOG CREATION

Purpose:

- Identify gaps between current state and target state, then convert gaps into a remediation backlog suitable for delivery planning.

Activities:

- Define target state controls and patterns (identity, network, security, governance, operations).
- Assess current state against target, using evidence and agreed standards.
- Log gaps with impact, priority, and dependency mapping.
- Convert gaps into remediation items with owners, acceptance criteria, and suggested implementation approach.

Inputs required:

- Target state architecture and standards.
- Current state evidence and inventories.
- Agreed prioritisation approach (risk-based, criticality-based, or time-based).

Outputs:

- Gap assessment report with prioritised findings.
- Remediation backlog with acceptance criteria and dependencies.
- Roadmap inputs for sequencing remediation ahead of migrations.

Service boundary:

- This component identifies and plans remediation. Implementation of remediation items is included only where authorised in the SoW.

Examples that can be amended:

- Landing zone governance: management groups, policy baseline, tagging, and subscription model.
- Identity controls: MFA enforcement, conditional access baseline, privileged access process.
- Network controls: segmentation, routing, private endpoints, DNS design, and connectivity resilience.
- Security controls: logging, key management, secure configuration baselines, and vulnerability management approach.
- Operations: monitoring, backup design, patching approach, and incident management process.

2.11 ARCHITECTURE OPTIONS ANALYSIS (RISK, COST, COMPLEXITY, OPERATIONAL IMPACT)

Purpose:

- Provide decision-ready options with clear trade-offs so the client can approve target patterns and migration paths.

Activities:

- Define option set per workload or capability area (for example identity integration, network connectivity, backup, firewalling, monitoring, and landing zone design).
- Assess each option against risk, cost drivers, delivery complexity, operational impact, and compliance fit.
- Document assumptions and constraints that materially change the recommendation.
- Produce an options paper and present through the agreed governance route.
- Record decisions and actions as architecture decision records (ADRs).

Inputs required:

- Current state evidence and target state requirements.
- Commercial constraints and known supplier commitments.
- Operational constraints and skills considerations.

Outputs:

- Options analysis document with recommendation and rationale.
- Decision log and ADRs for approved choices.
- Identified prerequisites and risks per chosen option.

Acceptance criteria (typical):

- Each option includes a clear statement of risk and operational impact.
- Costs are described using drivers and assumptions where exact values are not available.
- Recommendation is linked to documented constraints and acceptance criteria.

Service boundary:

- Options analysis provides recommendations and documented decisions. Procurement decisions and supplier selection remain client responsibilities unless explicitly included in scope.

2.12 DELIVERY ROAD-MAPPING AND PRIORITISED WORK PACKAGES

Purpose:

- Produce a delivery-ready roadmap that sequences work into prioritised work packages, aligned to dependencies, risk, and operational readiness.

Activities:

- Confirm delivery objectives, constraints, and key dates (for example contract milestones, lease exits, renewal points, or data centre closure dates).
- Group workloads and prerequisites into waves and workstreams (platform, identity, network, security, data, applications).
- Define work packages with clear scope, acceptance criteria, and entry and exit conditions.
- Identify dependencies, critical path items, and gating decisions.
- Define testing and validation approach per wave, including rollback planning and cutover governance.
- Produce a RAID log and maintain it through governance checkpoints.

Inputs required:

- Workload list and proposed migration paths.
- Target architecture and landing zone approach.
- Client change process and release windows.
- Operational model and support constraints (support hours, on-call, third-party dependencies).

Outputs:

- Roadmap covering 90-day plan and medium-term horizon (commonly 6 to 18 months, adjusted to client need).
- Prioritised backlog of work packages, each with scope, effort drivers, and acceptance criteria.
- Wave plan and high-level cutover schedule.
- RAID log with owners and review cadence.

Service boundary:

- Roadmaps are planning artefacts. Execution and delivery management are included only where explicitly agreed in the SoW.

Examples that can be amended:

- Work package: Establish landing zone management groups, subscriptions, policy baseline, and logging.
- Work package: Configure identity prerequisites, conditional access baseline, and privileged access approach.
- Work package: Enable migration tooling and run pilot migrations for a low-risk wave.

3. PRICING OVERVIEW, VOLUME DISCOUNTS AND DATA EXTRACTION COSTS

Pricing is provided in the separate G-Cloud pricing document for this service.

Typical charging models for Cloud Migration Planning include fixed-price work packages, time and materials, or a blended approach, depending on scope and deliverables.

Volume discounts apply where multiple workloads, sites, or business units are assessed under a single engagement, subject to the commercial model agreed.

Data extraction costs: this service does not charge for data extraction from an MVW-hosted platform because the service does not host client workloads. Any costs related to client tooling, third-party discovery tools, or specialist assessments are agreed in advance.

4. SERVICE CONSTRAINTS, MAINTENANCE WINDOWS AND CUSTOMISATION OPTIONS

Constraints are used to ensure controlled delivery and safe access to client environments.

- Access is least privilege. Elevated access is time-bound and requires client approval.
- Work is limited to the scope and deliverables in the SoW. Change requests follow formal scope control.
- Timescales depend on client approval cycles and governance cadence.
- Assessments depend on access to accurate inventories and technical owners.
- Customisation is limited to the agreed deliverables. Bespoke templates or additional artefacts are treated as additional scope.
- Maintenance windows: where any hands-on work is authorised, activity is scheduled within client change windows and follows client change control.

5. SERVICE LEVELS, PERFORMANCE, COMPENSATION AND SUPPORT HOURS

This is a consultancy service delivered against milestones and deliverables. Service levels relate to responsiveness and delivery governance, not platform uptime.

6. SUPPORT HOURS

Standard working hours are Monday to Friday, 08:30 to 17:30 UK time, excluding UK public holidays, unless otherwise agreed in the SoW.

7. TARGET RESPONSE TIMES (EXAMPLE)

ITEM	DESCRIPTION	TARGET
Client query acknowledgement	Acknowledge a request received during working hours	Within 4 working hours
Meeting scheduling request	Propose times for workshops or governance sessions	Within 1 working day
Document review turnaround	Review of a client artefact up to 20 pages	Within 5 working days
Critical delivery blocker	Response to an issue that blocks agreed migration planning outputs	Same working day

8. COMPENSATION

Service credits are not typically applied to consultancy services. Any contractual remedies are defined in the call-off contract and the SoW.

9. ORDERING AND INVOICING PROCESS

Orders are placed through a G-Cloud call-off contract and an SoW that defines scope, deliverables, timeline, and commercial terms.

Invoicing is aligned to the SoW, typically monthly in arrears for time and materials engagements, or to milestones for fixed-price engagements.

10. TERMINATION OF CONTRACT

Termination terms are set out in the G-Cloud call-off contract. On termination, MVW will provide a handover of completed deliverables and revoke access to client environments.

If termination occurs mid-engagement, MVW will provide:

- All deliverables completed up to the termination date.
- An up-to-date RAID log and action list.
- A summary of work completed and remaining work required to finish the migration planning outputs.

11. AFTER-SALES SUPPORT

After-sales support covers governance during the engagement and any post-engagement support period defined in the SoW.

- Weekly or fortnightly checkpoint meeting (progress, risks, actions).
- Architecture forum or design review cadence (where applicable).
- Close-out knowledge transfer sessions for client engineers and operations teams.

12. TECHNICAL REQUIREMENTS

Technical requirements depend on scope. Baseline requirements include:

- Access to current architecture diagrams, inventories, and service ownership information.
- Read-only access to relevant cloud portals for assessment where permitted.
- Ability to run workshops with business, security, networking, identity, application, and operations owners.
- Agreement on tooling used for documentation, work tracking, and approvals.

Where assessment tooling is used, the client may need to deploy discovery components and provide permissions for data collection, depending on the tool and environment.

ANNEX A: DELIVERABLES CATALOGUE (TEMPLATE)

Use this annex to agree deliverables for an SoW. Add, remove, and tailor entries to the engagement.

DELIVERABLE	DESCRIPTION	FORMAT	ACCEPTANCE CRITERIA	DUE DATE
[Deliverable name]	[Short description]	[Word/Excel/Visio/PDF]	[Acceptance criteria]	[Date]
[Deliverable name]	[Short description]	[Word/Excel/Visio/PDF]	[Acceptance criteria]	[Date]
[Deliverable name]	[Short description]	[Word/Excel/Visio/PDF]	[Acceptance criteria]	[Date]
[Deliverable name]	[Short description]	[Word/Excel/Visio/PDF]	[Acceptance criteria]	[Date]
[Deliverable name]	[Short description]	[Word/Excel/Visio/PDF]	[Acceptance criteria]	[Date]
[Deliverable name]	[Short description]	[Word/Excel/Visio/PDF]	[Acceptance criteria]	[Date]
[Deliverable name]	[Short description]	[Word/Excel/Visio/PDF]	[Acceptance criteria]	[Date]
[Deliverable name]	[Short description]	[Word/Excel/Visio/PDF]	[Acceptance criteria]	[Date]

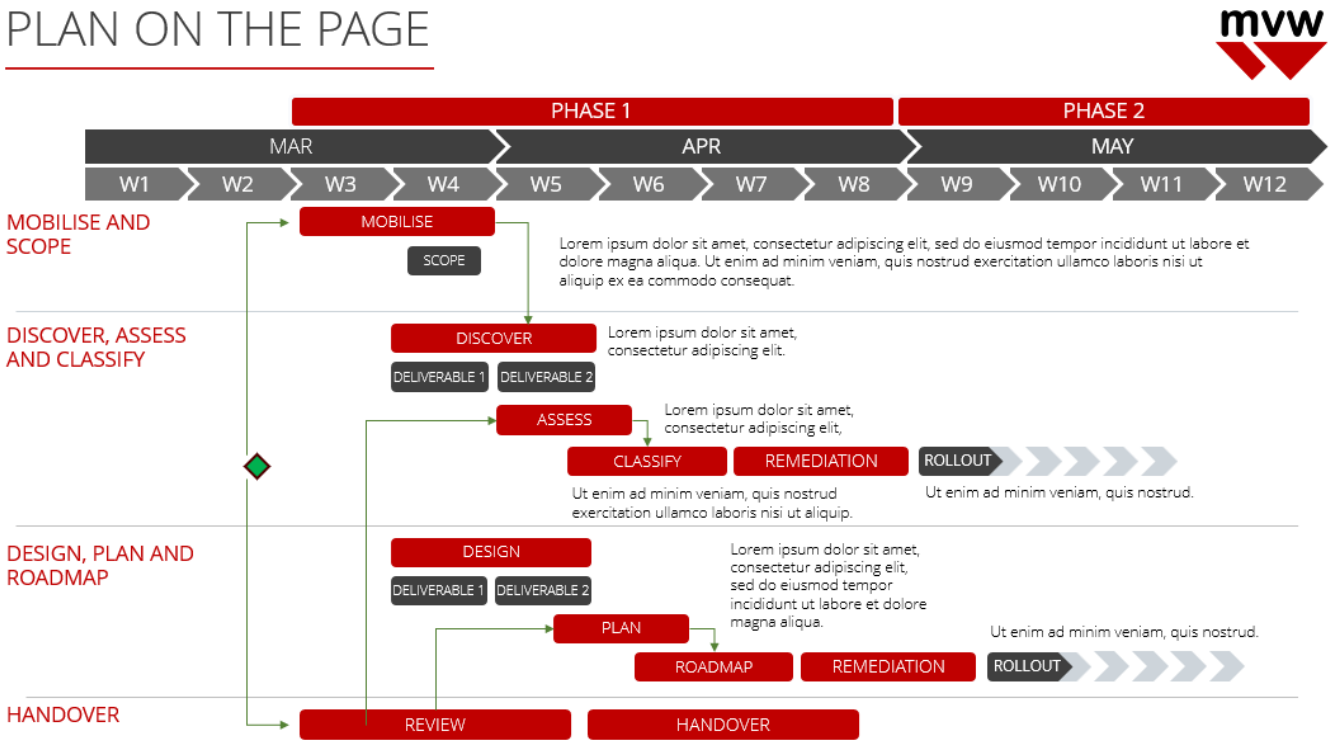
ANNEX B: SERVICE STRUCTURE SUMMARY (ONE-PAGE VIEW)

Service structure: Cloud Migration Planning.

Phases: mobilise and scope, discover, assess and classify, design and decide, plan and roadmap, handover and knowledge transfer.

Core components: migration planning, capability analysis, readiness assessment, target architecture definition, gap assessment and backlog, options analysis, delivery road-mapping.

A typical plan for migration planning phases looks like this:



APPENDIX A – TEAM ROLES AND CREDENTIALS (EXAMPLE)

The team is agreed per engagement. Example roles:

- Engagement Lead: delivery governance, stakeholder management, and quality control.
- Cloud Architect: target architecture, standards, and options analysis.
- Security Architect: security controls, compliance mapping, and risk input.
- Network and Connectivity Specialist: hybrid connectivity and segmentation patterns.
- Microsoft 365 Architect: tenant and identity considerations that affect migration outcomes.
- Project or Delivery Manager (optional): plan management, RAID management, and reporting.

Example certification areas (non-exhaustive):

- Microsoft Certified: Azure Solutions Architect Expert
- Microsoft Certified: Azure Security Engineer Associate
- Microsoft Certified: Identity and Access Administrator Associate
- Microsoft Certified: Microsoft 365 Administrator Expert

APPENDIX B – EXAMPLE TECHNOLOGY PATTERNS (AMENDABLE EXAMPLES)

The technology stack varies by client. Examples below are amendable.

B.1 MICROSOFT CLOUD (COMMON BASELINE)

- Microsoft Azure: landing zone, management groups, subscriptions, policy, networking, identity integration.
- Microsoft 365: tenant configuration, identity governance, device management approach, information protection.
- Microsoft Entra ID: conditional access, role-based access control, and privileged access processes.

B.2 MIGRATION ASSESSMENT AND PLANNING TOOLING (EXAMPLES)

- Azure Migrate for discovery, assessment, and planning for Azure target workloads.
- Dependency mapping approaches aligned to client constraints and security policy.
- Runbook templates for waves and cutovers, including pre-checks and rollback steps.

B.3 BACKUP SOLUTIONS (EXAMPLES)

- Azure Backup and Azure Site Recovery for Azure workloads, where selected by the client.
- Veeam Backup for Microsoft 365 for Microsoft 365 data protection, where selected by the client.
- Rubrik or Cohesity for enterprise backup, depending on client preference and existing contracts.

B.4 FIREWALL AND PERIMETER CONTROLS (EXAMPLES)

- Azure Firewall for cloud-native firewalling, where selected by the client.
- Palo Alto Networks or Fortinet virtual appliances where adopted by the client.
- Secure web gateway patterns such as Zscaler where adopted by the client.

B.5 NOTES ON EXAMPLES

- Examples are not commitments to specific products.
- Final choices are made through options analysis and client approvals.
- Licensing and procurement are managed by the client unless contracted separately.

END OF DOCUMENT