FluidOne

Managed Service Definition

G-Cloud 15

Company Name: FluidOne Ltd

Legal Entity: Private limited Company

Company Number: 05296759

Registered Address: 5 Hatfields, London, SE1 9PG

Contents

1.1 Managed Services 3

1.1.1 Service Desk Model & Hours 3
1.1.2 Onsite & Field Engineering 3
1.1.3 Operational Scope (Day-to-Day) 3
1.1.4 Tooling, Documentation & Knowledge 3
1.1.5 Governance & Roles 3
1.1.6 Operating Model Fit 4
1.1.7 Onboarding & Transition 4

1.2 Cloud Services – Fully Expanded Scope 4

1.2.1 Azure Infrastructure Management 4
1.2.2 Microsoft 365 Management & Compliance 4
1.2.3 Cloud Security & Zero-Trust Enforcement 5
1.2.4 Backup, Disaster Recovery & Continuity 5
1.2.5 Cloud Migration Services 5
1.2.6 Cloud Cost Management & Governance (FinOps) 5

1.3 Service Level Agreements (SLAs) 5

1.3.1 Hours of Operation & Coverage 5
1.3.2 Priority Definitions & Response SLAs 5
1.3.3 Proposed Resolution Targets (Confirm in Onboarding) 6
1.3.4 Major Incident & Communications 6
1.3.5 Availability & Service Credits (Optional Appendix) 6

1.4 Reporting, Governance & Continual Service Improvement (CSI) 6

1.5 Optional Add-On Services 7

FluidOne Managed Service Definition

This branded Service Definition provides an expanded, customer-facing overview of FluidOne's Managed Services for clients, including Service Desk model, onsite support, tooling, governance, onboarding, detailed Cloud Services, and Service Level Agreements (SLAs). It consolidates content reviewed across workshops, proposals, and collateral to form a single reference document.

1.1 Managed Services

FluidOne acts as your single partner and point of contact, operating a pod-based, multi-tier Service Desk and engineering capability aligned to ITIL v4. The service is designed to reduce incidents, improve stability and deliver a world-class user experience across office, site and home workers.

1.1.1 Service Desk Model & Hours

- **Pod-based, multi-tier support (Level 1–3)**
  - Providing triage, fix, and escalation, aligned to ITIL v4 principles.
- **Business-hours end-user support**
  - Complemented by Out-of-Hours (OOH) infrastructure support and monitoring including Saturday and Sunday.
- **Helpdesk coverage for:**
  - Office-based, site-based and home workers, with a dedicated Helpdesk Advisor for remote response and ticket management.

1.1.2 Onsite & Field Engineering

- **Site engineer attendance** for incident response, hands-on fixes, and equipment logistics when required.
- **Flexible onsite visits** during onboarding and BAU for knowledge transfer, audits and complex troubleshooting.

1.1.3 Operational Scope (Day-to-Day)

- **Incident Management and Service Requests** (*BAU changes such as starters and leavers*).
- **Problem Management** to remove root causes, supported by analytics in monthly reporting.
- **User Account Management** (*create/modify/deactivate*) with fair-usage model agreed during onboarding.
- **Third-party/vendor liaison** with shared workflows and SLA alignment captured during onboarding.
- **Proactive monitoring and alert handling** for critical services and infrastructure.

1.1.4 Tooling, Documentation & Knowledge

- **Halo ITSM workflows** for ticketing, approvals, automation, and multi-channel access *(email, portal, chat, phone)*.
- **IT Glue** for secure documentation of systems, runbooks, and configurations shared with agreed client roles.
- **Azure Monitor and Log Analytics** for telemetry, alerting, dashboards and trend analysis.

1.1.5 Governance & Roles

- **Service Delivery Manager (SDM)**
  - Accountable for SLA performance, monthly reporting, cadence reviews, escalations, and continuous improvement; acts as client's operational liaison.
- **Service Review Meetings**
  - With KPI/SLA packs, trend insights, risk & improvement tracking, and roadmap actions.
- **Monthly ticket reporting and analysis**
  - To reduce incidents and drive stability across servers, networks, and endpoints.

1.1.6 Operating Model Fit

- Single partner acting as SPOC, leading activities with third parties to conclusion.
- Senior consultancy available for future development needs and strategic planning.

1.1.7 Onboarding & Transition

- Discovery & assessment across Azure/M365, networks, devices, backup/DR posture, monitoring configuration and security baselines.
- Documentation consolidation into IT Glue: architecture diagrams, inventories, integrations, and runbooks.
- SLA & escalation design with communications plan and RACI alignment.
- Tooling enablement in Halo workflows, approvals, automation), monitoring setup (Log Analytics, Azure Monitor), and Defender policy baselining.
- Stabilisation and parallel operations: shadow support, backlog remediation, early-life improvements prior to full BAU transition.

1.2 Cloud Services – Fully Expanded Scope

1.2.1 Azure Infrastructure Management

- Azure VM lifecycle management, autoscaling, sizing recommendations and governance policies.
- Virtual network design, routing, NSGs, firewalls and hybrid connectivity (*VPN/ExpressRoute*).
- Azure Policy and tagging enforcement for compliance and cost governance.
- Update Management, patch orchestration, desired state baselines and OS hardening.
- Log Analytics workspace design, KQL alerting, dashboards, and alert routing to resolver groups.

1.2.2 Microsoft 365 Management & Compliance

- Lifecycle management and permissions governance of:
  - Exchange Online
  - SharePoint
  - OneDrive
  - Teams
- Compliance controls:
  - Retention policies
  - DLP
  - Communication compliance
  - Sensitivity labels

- Microsoft Defender
  - Deployment
  - Alert triage
  - Identity protection
  - Threat response playbooks
- License optimisation and usage analytics to reduce waste and uplift adoption across opcos.

1.2.3 Cloud Security & Zero-Trust Enforcement

- Identity design with Entra ID Conditional Access, MFA enforcement and device compliance.
- Defender XDR across identity, endpoint, cloud apps and email with automated investigations.
- Monthly Secure Score optimisation sprints and posture improvement activities.
- Incident response assistance including triage, investigation and containment with resolver playbooks.

1.2.4 Backup, Disaster Recovery & Continuity

- Azure Backup configuration, monitoring, alert response and retention governance.
- Azure Site Recovery design (*failover groups, runbooks, test cycles*) with documented outcomes.
- Annual DR simulation testing and remediation tracking for agreed RTO/RPO targets.

1.2.5 Cloud Migration Services

- Tenant-to-tenant migrations, AD/Entra consolidation, Exchange Online migrations.
- File server to SharePoint/OneDrive migrations with change management and adoption support.
- Azure infrastructure migrations covering rehost, re-platform and refactor approaches.

1.2.6 Cloud Cost Management & Governance (FinOps)

- Reserved instance planning, budget alerts, consumption dashboards, and anomaly detection.
- Cost governance including tagging standards, cleanup automation, and policy-based limits.
- Monthly cloud cost forecasting and CIO-level reporting across opcos and environments.

1.3 Service Level Agreements (SLAs)

1.3.1 Hours of Operation & Coverage

- **End-user support**: Business Hours (per client clarification).
- **Out-of-Hours**: Infrastructure support & monitoring including Saturday and Sunday.
- **Helpdesk servicing** for office-based staff, site-based users, and home workers; dedicated advisor for remote response & ticket management.

1.3.2 Priority Definitions & Response SLAs

Priority	Description	Response Times

P1 – Critical	Severe impact/total inability to operate; widespread business impact	30 Minutes
P2 – Major	Significant degradation, numerous users/major function impacted. Response target	1 Hour
P3 – User Blocking	Single user unable to work.	1 Hour
P4 - Minor	User can work but requires assistance.	1 Hour
Service Requests	e.g. BAU Change	24 Hours

Prioritisation based on impact and urgency; escalation paths led by SDM and resolver leads with governance oversight.

1.3.3 Proposed Resolution Targets (Confirm in Onboarding)

Priority	Description	Response Times
P1	Work to restore service or workaround	Within 4 Hours
	Post-incident review	Within 3 business days
P2	Resolution or workaround;	within 8 business hours
	Problem record raised if repeat incidents occur.	
P3	Resolution	within 2 business days
	Grouped trend analysis in monthly reporting.	
P4	Resolution	within 5 business days
	Batched for change windows where appropriate.	
Service Requests	Fulfilment per catalogue item (e.g., starters/leavers).	within 1 business day
	Standard access	within 2 business days

1.3.4 Major Incident & Communications

- Mandatory phone logging for P1 incidents; bridge opened with resolver groups and SDM.
- Hourly updates to stakeholders during MI; executive summary provided at closure including timeline, actions, and next steps.

1.3.5 Availability & Service Credits (Optional Appendix)

- FluidOne Core Network (Platform One) availability SLA at 99.99% with defined service credit tiers *(if client elects to include network SLAs in MS scope)*.
- Packet delivery, latency, jitter measured centrally; international sites may have unique terms depending on local carriers.

1.4 Reporting, Governance & Continual Service Improvement (CSI)

- **Monthly or Quarterly Service Reviews** includes:
  - SLA achievement
  - Breaches/root cause analysis
  - Improvement actions.
- **Comprehensive reporting pack**:
  - Incidents/requests
  - Capacity metrics
  - Cloud consumption
  - Secure Score

  - Defender alerts
  - Adoption trends.
  - Risk register, issue log, service improvement actions, and backlog review maintained by SDM with stakeholder sign-off.
- **Technology roadmap planning** covering:
  - Cloud uplift
  - Security enhancements
  - Lifecycle management
  - Cost optimisation

Structured CSI cycles identify recurring incidents, asset performance issues, weak security controls, adoption barriers, cost inefficiencies, and automation opportunities.

1.5 Optional Add-On Services

- vCIO/vCTO strategic advisory including budgets, IT strategy, and cloud maturity assessments.
- Advanced SOC & SIEM (e.g., Microsoft Sentinel) and threat hunting services.
- Network Managed Services including SD-WAN, LAN, WiFi, and Platform One connectivity.
- Professional Services for cloud architecture, cyber uplift, and infrastructure modernisation.