CIRRO

Service Description
Infrastructure as a Service – Azure Local HCI

Service Name

Infrastructure as a Service – Azure Local/HCI

Taxonomy	
A-201-301-401	IaaS General Purpose
A-201-301-402	IaaS Compute Optimised
A-201-301-403	IaaS Memory Optimised

Service Overview

The best of all worlds, combining Azure Local HCI Stack Infrastructure with Azure native Cloud. Either unmanaged, partly managed or fully managed, to your Info Security standards, DR and BC policies and Data Protection requirements.

Increasingly we are now building in cost effectiveness a budget predictability into the day-one architecture of our cloud solutions.

Whilst Hybrid-cloud is nothing new, the term has tended to refer to relatively static workload division between pubic cloud and traditionally hosted VMs – more a mixed estate than a true hybrid solution.

Cirro can offer solutions which combine the scalability, agility and security of public cloud but with costs and price predictability of private cloud or on premise solutions.

Working with our partner Innovate Ltd we design and deploy solutions using Azure Stack HCI.

Microsoft Azure HCI provides a privately hosted Azure environment with all its inherent benefits supporting Windows and Linux environments. It provides seamless management between privately hosted Azure and public Azure – workloads can be dynamically moved from private to public.

This provides a true hybrid cloud.

We have provided such services to range of customers both in the public and private sectors. Each customer has enjoyed a flexible scalable usage based platform at a fraction of the cost of pure public cloud.

General Purpose or Optimized for Memory or Compute

Azure Local (Azure Stack HCI / Azure Local) can be optimised for memory-intensive, compute-intensive, or balanced workloads. This flexibility is a key advantage of the platform and allows infrastructure to be tailored precisely to application and user requirements.

Compute-Optimised Configuration

Compute-optimised configurations are suited to CPU-intensive workloads such as application servers, web services, batch processing, and VDI session hosts.

Optimisation is achieved through higher core-count processors, faster CPU clock speeds, NUMA-aware VM placement, and appropriate vCPU allocation and reservations. This ensures high throughput and low latency for processor-bound workloads.

Memory-Optimised Configuration

Memory-optimised configurations are designed for workloads that require large memory footprints, such as databases, line-of-business systems, VDI/RDS environments, and in-memory analytics platforms.

This is achieved by deploying a high RAM-per-core ratio, avoiding memory overcommit, and aligning VM sizing to application working sets. The result is improved responsiveness and higher user density.

Balanced and Hybrid Optimisation

Azure Local also supports balanced and hybrid configurations, where some cluster nodes are optimised for compute and others for memory. Workloads can be placed accordingly, enabling efficient resource utilisation and cost optimisation.

Ongoing Optimisation and Evergreen Operation

Optimisation continues throughout the lifecycle of the platform. Performance monitoring, workload rebalancing, and incremental scale-out ensure Azure Local remains aligned to evolving business requirements without the need for disruptive refresh projects.

Cloud Deployment & Architecture

We provide a **UK-only private cloud platforms built on Azure Local HCI from Microsoft (formally Microsoft Azure Stack HCI)**, hosted across two secure and resilient Tier 3 UK data centres this Hyper Converged Infrastructure is a Local deployment of Microsoft Azure. Providing the **security and control of private hosting** with the **flexibility and familiarity of Azure-native tooling**, ensuring future hybrid cloud options are available whenever required.

Key architectural tiers:

- **Identity & Core Services**
  - Two Domain Controllers (split across racks/sites).
  - Services: AD DS, DNS, DHCP, Group Policy.
  - FSMO roles distributed; AD Recycle Bin enabled; secure delegation for service accounts.
- **Data Tier**
  - Dedicated SQL Server (SQL2019/2022) for MRI RAM and PIMMS.
  - SSD volumes split for Data, Log, TempDB, and Backups.
  - Backup strategy: nightly full, daily differential, 15-minute transaction log backups (RPO ≤ 60 mins).
  - SQL Query Store, index/statistics maintenance, and performance baselines built-in.
- **File & Print Tier**
  - Two clustered servers with DFS-N/DFS-R for seamless namespace and replication.
  - Print queues published via AD, resilient spooling, optional PaperCut integration.
- **Application Delivery**
  - Two Parallels RAS Gateways (TLS termination, DMZ deployed).
  - Two RAS Session Hosts in HA with load balancing and N+1 headroom.
  - Policies restrict clipboard/drive redirection; per-app MFA and conditional access available.
- **Integration & Transfer**
  - Hardened Secure FTP server (SFTP preferred, key-based auth, chrooted directories).
  - Inline DLP/malware scanning; full audit trails exported to SIEM.
- **Operations & Tooling**
  - Central management server (MGMT01): patch orchestration, backup console, monitoring dashboards, and secure jump host.
- **Networking & Segmentation**
  - VLANs for Users, SQL, Management, and DMZ.
  - East–west traffic restricted by policy; north–south flows logged.
  - Next-gen firewalls with IDS/IPS and micro-segmentation.

This architecture is **modular, scalable, and proven**, with 99% SLA adherence and over 20 years of uninterrupted service delivery in Innovate's UK platform.

Security & Compliance

Security is embedded into both the core **design** and **operations** of the solution, aligned to **ISO/IEC 27001**, **Cyber Essentials Plus**, and GDPR requirements. Services delivered within an ISMS (ISO27001) and ITSM (ISO20000, ITIL v4). Regular third-party audits and penetration testing provide independent validation. Assurance is delivered through:

Data Sovereignty & Assurance

- 100% UK hosting; no data leaves the UK (egress blocked at perimeter).
- Tier 3+ data centres with 2N power, multi-carrier connectivity, 24×7 security, ISO27001/22301.

Identity & Access

- AD-integrated authentication.
- MFA for privileged accounts.
- Admin tiering with jump host (MGMT01).
- Privileged Access Management (PAM) enforced for SQL and Windows admin groups.

Encryption & Hardening

- TLS 1.2+ enforced, SMB signing, IPSec where appropriate.
- BitLocker/SQL TDE for all at-rest data.
- CIS/SCA baselines applied; legacy protocols (SMBv1, TLS1.0/1.1) disabled.
- LAPS/Windows LAPS for local admin accounts.

Monitoring & Logging

- Real-time monitoring of OS, SQL waits/blocking, I/O latency, AD replication, RAS session health, AD replication and authentication failures.
- Logs (Windows, SQL Agent, RAS, SFTP) forwarded to SIEM.
- Alerting integrated with Innovate SOC.

Vulnerability & Patch Management

- Monthly cumulative updates for OS/SQL.
- Emergency patch window ≤72 hours.
- Regular vulnerability scans with tracked remediation.

Backup Security

- Immutable/offline backup copies.
- MFA and four-eyes role separation for backup operators.
- Monthly test restores with documented evidence.

These measures provide you with **defence-in-depth** and auditable compliance with GDPR, industry best practice and cyber security standards. Furthermore, we provide services to UK National Critical Infrastructure organisations and to the UK Governments Official (Sensitive) standard. With no variation between a 'regular' customers and a Government one when it comes to the design, security or resiliency of the services.

Resilience

Resilience is built into the core fabric of our operations and cloud compute platforms, we build resilience in customer deployments against requirements. This approach ensures that as a business, we are highly resilient, and as a customer, you have the flexibility to have the right level of resilience based on required update, data loss sensitivity, risk and cost.

Everyday resilience:

- N+1 compute and storage design; dual PSUs, redundant networking.
- Dual PSUs and redundant network paths.
- HA clustering for Domain Controllers, File & Print, RAS Gateways/Hosts.
- SQL log backups every 15 minutes.

Protecting against Short-term outages (minutes–hours):

- **Power dips/UPS events**: Online UPS with generator-backed supply ensures no service interruption. Failover procedures are automated and tested.
- **Network or carrier blips**: Dual-carrier WAN links with automatic failover. User sessions preserved via HA Parallels RAS gateways.
- **Host hardware failures**: VMs restart automatically on surviving hosts within the cluster. RAS session hosts drain sessions before planned maintenance.

Dealing with Prolonged failures (hours–days):

- **Data centre power loss**: Both Manchester and Fareham DCs have 2N power and generator backup. Fuel contracts guarantee prolonged runtime.
- **WAN provider outage**: Automatic carrier failover, with escalation to Innovate's NOC for supplier management. Remote access preserved via alternative circuits.
- **Site loss / major incident**: Services failover to secondary site (Manchester ↔ Fareham). RPO ≤ 60 mins, RTO ≤ 60 mins proven in annual DR tests.

Support Model

We will deliver a UK-based, ITIL-aligned Service Desk service that supports a resilient, transparent, and high-quality service model. Based in Bournemouth and backed by hybrid engineers across the UK, our Service Desk offers direct access to skilled second- and third-line engineers, supported by the HaloPSA platform for real-time ticketing, tracking, and reporting. A dedicated Service Delivery Manager will ensure governance, continuity, and strategic alignment, while our focus on continuous improvement, strong SLAs, and proactive monitoring guarantees that your ICT services remain secure, reliable, and continually optimised.

Our service desk has a call pick up time of less than 6 seconds and we typically resolve 85% of incidents on first contact. As a policy we also look to drive down call volume through Problem Management and using reporting data in HaloPSA to identify trends and put forward improvement projects. On taking on new customers, we have typically reduced call volumes by 40% to 50% over the first two years.

Staffed Hours and Access

You will have access to the Service Desk during core business hours of 08:00–18:00, Monday to Friday, with full 24×7 coverage for Priority 1 and Priority 2 incidents.

Calls can be logged using a standard-rate UK telephone number, and all incidents and requests can also be submitted through the HaloPSA self-service portal, which is available 24×7 for reporting and tracking. The portal provides full visibility of SLA timers, ticket ownership, and progress updates.

Staffing and Knowledge

At any one time, there are typically 20 support engineers available to take calls, covering disciplines such as networking, cloud platforms, security, end-user computing, and line-of-business applications. Each engineer supports a carefully limited number of customers to ensure familiarity with the business and the supporting environments.

Major incidents are managed through a structured process that aligns with ITIL and our ISO9001 and ISO2000 standards. On declaration of a P1 or P2, a Major Incident Manager is assigned, and communications are initiated within 30 minutes. Updates are provided at agreed intervals until resolution. Following closure, a full post-incident review with root cause analysis is delivered within 5 working days.

Escalation paths begin with the Service Desk Team Leader, progressing through the Service Desk Manager, then to the SDM, and ultimately to our Operations Director. you will always have visibility of escalation status and named contacts at every stage.

Onboarding & Offboarding (Exit)

Cirro – Cloud Migration Best Practice Standards

Cirro follows recognised, industry-standard cloud migration best practices, centred on the Microsoft Cloud Adoption Framework (CAF). This framework provides a structured and proven approach to planning, migrating, and optimising cloud environments.

Core Best Practice Framework

Cirro aligns its cloud migrations to the Microsoft Cloud Adoption Framework, which is widely adopted as best practice for Azure migrations.

Migration Lifecycle Adopted by Cirro

- Analyse – Assessment of the existing environment, dependencies, risks, security and compliance requirements.
- Plan – Definition of migration strategy, workload prioritisation, timelines, rollback planning, and risk management.
- Transition – Phased migration using Azure-native tools to minimise downtime and disruption.
- Operate – Ongoing operational management, monitoring, security and cost optimisation.
- Transform – Adoption of cloud-native services and modern workplace technologies to improve performance and scalability.
- Continual Improvement – Continuous optimisation using lessons learned, service reviews and performance reporting.

Supporting Standards and Governance

Cirro underpins the Cloud Adoption Framework with recognised governance, security and service management standards including:
- ISO 27001 – Information Security Management
- ISO 22301 – Business Continuity Management
- ISO 9001 – Quality Management
- ITIL – IT Service Management best practices
- PRINCE2 – Structured project management methodology
- Cyber Essentials / Cyber Essentials Plus

Summary

In summary, Cirro delivers cloud migrations using the Microsoft Cloud Adoption Framework, supported by ISO-accredited quality, security and continuity standards. This ensures migrations are secure, low-risk, well-governed, and continuously optimised after go-live.

At exit, we will deliver a **structured, time-boxed handover** ensuring you or your successor MSP receives all data in open formats:

- **Databases**: Native SQL .bak files (full/differential/log chain), CSV exports, schema documentation.
- **File Shares**: Robocopy with ACL preservation, or packaged archive (ZIP/TAR).
- **SFTP Zones**: Structured export including logs.

- **Configurations**: AD, GPOs, RAS farm exports, SFTP configs, certificates (via escrow).
- **Verification & Handover**: Data integrity checked via checksums, with joint sign-off.
- **Secure Destruction**: Certified wiping of residual data post-handover.

This guarantees **no vendor lock-in**, UK-only handling, and a **risk-free transition**.

Shared Responsibility Model

The following RACI Model defines the shared responsibility model.

Activity	Exec Sponsor	Client IT	PM	Architect	Engineers	Security
Strategy & scope definition	A	C	R	C	I	C
Discovery & assessment	I	C	R	A	R	C
Target architecture design	I	C	R	A	C	C
Migration planning	I	C	A	R	C	I
Security & compliance design	I	C	R	C	I	A
Cloud build & configuration	I	I	R	C	A	C
Data replication & testing	I	C	R	C	A	I
Go-live approval	A	C	R	I	I	I

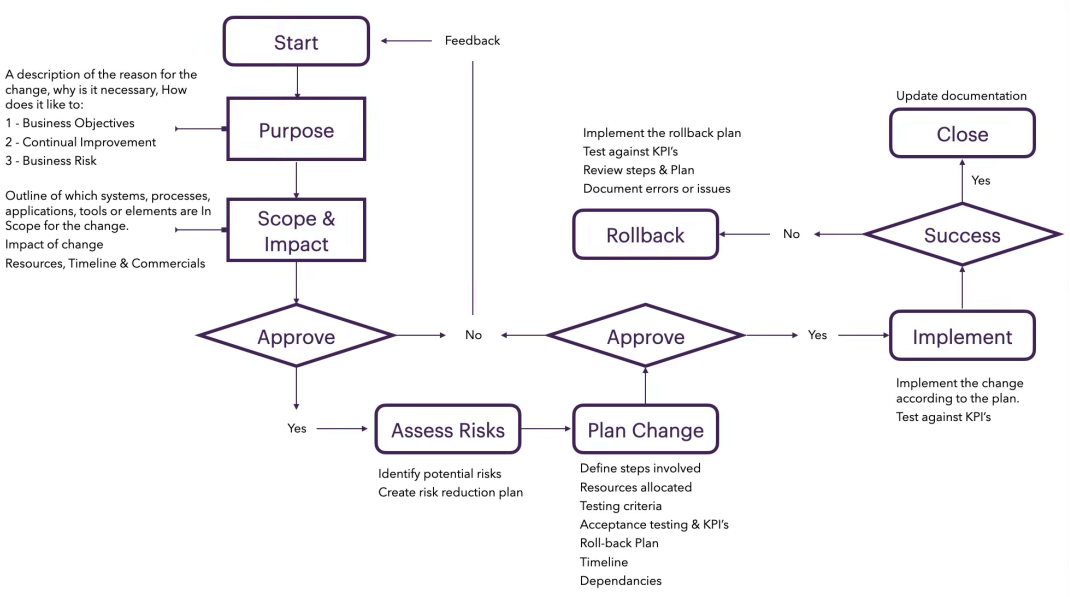
Pro-duction cutover	I	C	A	C	R	I
Hando-ver to BAU sup-port	I	C	A	I	R	I
Opera-tional moni-toring	I	I	C	I	A	C
Cost optimi-sation	I	C	R	A	C	I
Contin-ual im-prove-ment	I	C	R	A	C	C

Service Change & Evergreen Commitment

Change Control

Our change control process is ITIL-aligned and operated within HaloPSA. All changes are categorised as standard, normal, or emergency. Each non-standard change includes an assessment of business impact, risk, back-out plan, and test plan, and must be approved by the Change Advisory Board (CAB). Emergency changes follow an expedited approval route but are always documented and reviewed retrospectively. A sample Change Control Form is provided as part of the tender submission.

A typical change control process flow:



Commitment to an Evergreen Azure Local Platform

We are committed to maintaining the Azure Local platform as an evergreen environment throughout the contract term. This is achieved through proactive lifecycle management, including regular platform updates, security patching, and controlled version upgrades aligned to Microsoft's Azure and Azure Local release cadence. We continuously monitor platform health, performance, and compatibility, ensuring updates are tested and deployed in a structured, non-disruptive manner. This approach removes the risk of end-of-life infrastructure, maintains ongoing security and compliance, and ensures customers consistently benefit from the latest Azure capabilities without the need for major refresh projects.